MATH 228: COMMUTATIVE RING THEORY

James D. Lewis

TABLE OF CONTENTS

Cover page computer artistic work courtesy of Dale R. Lewis.

MATH 228

A Course on Commutative Rings

James D. Lewis

$\mathbf{R} =$ Real numbers. Picture : $\overset{-}{\longleftarrow} \circ \overset{+}{\longrightarrow}$

$\mathbf{Z} =$ Integers $= \{0, \pm 1, \pm 2, \ldots\}$

$$\mathbf{Q} = \text{ Rational numbers} = \left\{ \frac{a}{b} \Big| \; a, b \in \mathbf{Z}, b \neq 0 \;\&\; \frac{a_1}{b_1} = \frac{a_2}{b_2} \Leftrightarrow a_1 b_2 = b_1 a_2 \right\}$$

There are inclusions

$$\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R},$$

where the inclusion $\mathbf{Z} \subset \mathbf{Q}$ is given by $n \in \mathbf{Z} \mapsto \frac{n}{1} \in \mathbf{Q}$.

Description of the Real Numbers

(Note: $\coprod$ = disjoint union)

$$\mathbf{R} \;=\; \mathbf{Q} \;\coprod\; \{\text{Irrational numbers}\}$$

$$\| \qquad\qquad\qquad \|$$

repeating decimals e.g. $0.2\overline{35}$

non − repeating decimals

$$\swarrow \quad \searrow$$

algebraic irrationals e.g. $\sqrt{2}, \sqrt[3]{5}$

transcendental irrationals e.g. e, π

The algebraic irrational numbers are solutions of equations of the form:

$$x^2 - 2 = 0 \qquad ; \qquad 3x^3 - \frac{1}{2} = 0,$$

i.e. single variable polynomial equations with $\mathbf{Q}$-coefficients.

Notation: $\mathbf{N} = \{1, 2, 3, \ldots\} =$ Natural numbers.

Axiomatic Properties of the Real Numbers

$\mathbf{R}$ (as well as $\mathbf{Z}$, $\mathbf{Q}$) has two (binary) operations $+$, $\bullet$:

$$\begin{array}{ccc} \mathbf{R}\times\mathbf{R} & \stackrel{+}{\to} & \mathbf{R} \\ (a,b) & \mapsto & a+b \end{array}$$

$$\begin{array}{ccc} \mathbf{R}\times\mathbf{R} & \stackrel{\bullet}{\to} & \mathbf{R} \\ (a,b) & \mapsto & ab \end{array}$$

Properties of $[\mathbf{R};+,\bullet]$

(1) $\mathbf{R}$ is closed under $+,\bullet$, i.e. $a,b\in\mathbf{R}\Rightarrow a+b,\ ab\in\mathbf{R}$. [Analogous notion: $\mathbf{R}$ is not closed under $\sqrt{\ }$'s. E.g. $-1\in\mathbf{R}$, but $\sqrt{-1}\notin\mathbf{R}$.]

(2) Associativity.

$$(a+b)+c=a+(b+c)$$

$$(ab)c=a(bc)$$

[Hence can write $a+b+c$, abc.] For example, if we denote by $f_+:\mathbf{R}\times\mathbf{R}\to\mathbf{R}$ the $+$ map, i.e., $f_+(a,b)=a+b$, then associativity implies that $f_+(f_+(a,b),c)=f_+(a,f_+(b,c))$.

(3) Commutivity.

$$a+b=b+a$$

$$ab=ba$$

[I.e. $f_+(a,b)=f_+(b,a)$ and similarly $f_\bullet(a,b)=f_\bullet(b,a)$, where $f_\bullet(a,b):=ab$ is the corresponding multiplication map.]

(4) Zero element. There exists an element labeled $0\in\mathbf{R}$ such that $a+0=a$ for all $a\in\mathbf{R}$. [Note: It will be proven that 0 is unique.]

(5) Identity element (or Unity). There exists an element labelled $1\in\mathbf{R}$ such that $1\cdot a=a$ for all $a\in\mathbf{R}$. [Note: It will be proven that 1 is unique.]

(6) Additive Inverse. For any $a\in\mathbf{R}$, there exists an element labelled $-a\in\mathbf{R}$ such that $a+(-a)=0$. [Note: It will be proven that additive inverses are unique.]

(7) Multiplicative Inverse. For any $a\in\mathbf{R}$, $a\neq 0$, there exists an element labelled $a^{-1}\in\mathbf{R}$ such that $a\cdot a^{-1}=1$. [Note: It will be proven that multiplicative inverses are unique.]

(8) Distributive. [Interaction of $+$, $\bullet$.]

$$a(b+c) = ab + ac$$

(9) $1 \neq 0$.

Remarks 1. If $a = b$ & $c = d$, then $a + c = b + d$ and $ac = bd$, i.e. the operations $+, \bullet$ are well-defined.

2. Given $a, b \in \mathbf{R}$, we write

$$a - b := a + (-b)$$

and if $b \neq 0$, then

$$\frac{a}{b} := a \cdot b^{-1}$$

3. $[\mathbf{R}; +, \bullet]$ is an example of a field, i.e. satisfies axiomatic properties (1) -(9) above. [We only require axiomatic properties (1)-(4), (6), (8) to define a ring. Roughly then, a "ring including division" amounts to a field.]

Some Consequences of the 9 Axiomatic Properties of $[\mathbf{R}; +, \bullet]$

(i) 0 is unique, i.e. there is only 1 zero.

Restatement: If $\tilde{0}$ also satisfies the property that $\tilde{0} + a = a$, for all $a \in \mathbf{R}$, then $\tilde{0} = 0$.

Reason :

$$\begin{array}{ccccc} \tilde{0} & = & \tilde{0} + 0 & = & 0 \\ & \uparrow & & \uparrow & \\ & \text{def'n of} & & \text{def'n of} & \\ & \text{zero } 0 & & \text{zero } \tilde{0} & \end{array}$$

(ii) 1 is unique, i.e. there is only 1 unity. [Reason: Similar to (i) above.]

(iii) $a \cdot 0 = 0$ for any $a \in \mathbf{R}$.

Reason: We refer to the axiomatic properties (1)-(9) above. Then

$$a \cdot 0 \overset{(4)}{=} a \cdot (0 + 0) \overset{(8)}{=} a \cdot 0 + a \cdot 0$$

Next, add $-(a \cdot 0)$ to both sides. Thus

$$0 \overset{(6)}{=} (a \cdot 0) + (-(a \cdot 0)) = (a \cdot 0 + a \cdot 0) + (-(a \cdot 0)) \overset{(2)}{=} a \cdot 0 + (a \cdot 0 + (-a \cdot 0)) \overset{(6)}{=} a \cdot 0 + 0 \overset{(4)}{=} a \cdot 0$$

Therefore $a \cdot 0 = 0$.

(iv) $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$. Reason: If $a = 0$, then we're done. Therefore assume $a \neq 0$, hence $a^{-1} \in \mathbf{R}$ exists. We must then show that $b = 0$. But

$$0 \overset{\text{(iii)}}{=} a^{-1} \cdot 0 = a^{-1}(a \cdot b) \overset{(2)}{=} (a^{-1} \cdot a)b = 1 \cdot b \overset{(5)}{=} b$$

Hence $b = 0$.

(v) [Cancellation Law for Multiplication] If $ac = bc$ and if $c \neq 0$, then $a = b$. Reason: One shows that $ac = bc \Leftrightarrow (a - b)c = 0$, and then apply (iv) above. In showing that $ac = bc \Leftrightarrow (a - b)c = 0$, one first shows that $-(bc) = (-b)c$. This is an exercise left to the reader.

(vi) [Cancellation Law for Addition] If $a + c = b + c$ then $a = b$. Reason: Add "$-c$" to both sides of "$a + c = b + c$ ".

(vii) There is no $0^{-1} \in \mathbf{R}$, i.e. there is no multiplicative inverse to 0. Restatement: There is no number $y \in \mathbf{R}$ such that $y \cdot 0 = 1$. Reason: Otherwise

$$0 \overset{\text{(iii)}}{=} y \cdot 0 = 1,$$

i.e. $0 = 1$, which violates axiomatic property (9).

(viii) [Uniqueness of Additive Inverse] Let $a \in \mathbf{R}$. Then there is only one $-a \in \mathbf{R}$. Restatement: If $a + x = 0$ and $a + y = 0$, then $x = y$. Reason: $a + x = 0$ and $a + y = 0$ $\Rightarrow a + x = a + y$, hence by (vi) above, $x = y$.

(ix) [Uniqueness of Multiplicative Inverse] Let $a \in \mathbf{R}$ with $a \neq 0$. Then there is only one $a^{-1} \in \mathbf{R}$. Restatement: If $xa = 1$ and $ya = 1$ with $a \neq 0$, then $x = y$. Reason: $xa = 1$ and $ya = 1 \Rightarrow xa = ya$, hence $x = y$ by (v) above.

(x) $-(-a) = a$. Reason: $(-a) + (-(-a)) = 0$ and $-a + a = 0$. Hence $-(-a) = a$ by (viii) above.

(xi) Suppose $a, b \in \mathbf{R}$. Note that $a, b \neq 0 \Leftrightarrow ab \neq 0$ by (iii) & (iv) above. Then if $ab \neq 0$, $(ab)^{-1} = a^{-1}b^{-1}$. Reason: It is easy to see that $(ab)(a^{-1}b^{-1}) = 1$; moreover $(ab)(ab)^{-1} = 1$. Thus $(ab)^{-1} = (a^{-1}b^{-1})$ by (ix) above.

(xi) $-(a+b) = (-a)+(-b)$. Reason: It is easy to see that $(a+b)+((-a)+(-b)) = 0$; moreover $(a + b) + (-(a + b)) = 0$. Hence $-(a + b) = (-a) + (-b)$ by (viii) above.

(xii) Exercise: Show the following

1.) $(-a)b = a(-b) = -(ab)$

2.) $(-a)(-b) = ab$

3.) $(a+b)(a-b) = a^2 - b^2$

Useful Notation: Let $a \in \mathbf{R}$, $a \neq 0$ be given, and $n \in \mathbf{N}$. Set $a^0 = 1$, $a^1 = a$, $a^2 = a \cdot a, \ldots, a^n = \underbrace{a \cdots a}_{n \text{ times}}$. Finally, set $a^{-n} := (a^{-1})^n$.

Summary

Assume given a set $\mathbf{A}$ with 2 binary operations

$$\mathbf{A} \times \mathbf{A} \stackrel{\{+,\bullet\}}{\longrightarrow} \mathbf{A}$$

Consider these properties:

1. *(Closure)*

$$a,\ b \in \mathbf{A} \Rightarrow \begin{cases} a+b \\ ab \end{cases} \in \mathbf{A}$$

2. *(Associativity)*

$$a + (b + c) = (a + b) + c$$

$$a(bc) = (ab)c$$

3. *(Commutativity)*

$$a + b = b + a$$

$$ab = ba$$

4. *(Zero element)* There exists a (unique) element $0 \in \mathbf{A}$ such that $a + 0 = a$ for all $a \in \mathbf{A}$.

5. *(Identity element = unity)* There exists a (unique) element $1 \in \mathbf{A}$ such that $1 \cdot a = a$ for all $a \in \mathbf{A}$.

6. *(Additive inverse)* For any $a \in \mathbf{A}$, there exists a (unique) $-a \in \mathbf{A}$ such that $a + (-a) = 0$.

7. *(Multiplicative inverse)* For any non-zero $a \in \mathbf{A}$, there exists a (unique) $a^{-1} \in \mathbf{A}$ such that $a \cdot a^{-1} = 1$.

8. *(Distributive law)*

$$a(b + c) = ab + ac$$

9. $1 \neq 0$.

Note: 1. The uniqueness parts of properties 4, 5, 6, 7 can be proven as in the case of $[\mathbf{R}; +, \bullet]$.

2. As a blanket statement, all the consequences (i)-(xii) for $[\mathbf{R}, +, \bullet]$, likewise hold for $[\mathbf{A}; +, \bullet]$.

Definitions (i) $[\mathbf{A}, +, \bullet]$ is called a <u>field</u> if it satisfies properties $1 \rightarrow 9$.

(ii) $[\mathbf{A}, +, \bullet]$ is called a [commutative] <u>ring</u> if it satisfies properties 1, 2, 3, 4, 6, 8.

(iii) $[\mathbf{A}, +, \bullet]$ is called a ring with identity (or unity), if it is a [commutative] ring that also satisfies 5.

Note that any field is a ring, but not the other way around! For example, $\mathbf{Z}$ is a ring with unity, but not a field, since $2 \in \mathbf{Z}$, $2 \neq 0$, and yet $2^{-1} = \frac{1}{2} \notin \mathbf{Z}$. If we consider the natural numbers $\mathbf{N}$ with addition induced from $\mathbf{Z}$, then it is clear that $\mathbf{N}$ has no additive inverses, and no zero element. Thus clearly $\mathbf{N}$ is <u>not</u> a ring.

<u>Some Examples of Fields</u>

Ex. 1: The rational numbers $[\mathbf{Q}; +, \bullet]$. Recall the rational numbers

$$\mathbf{Q} = \left\{ \frac{a}{b} \middle| \ a, b \in \mathbf{Z}, b \neq 0 \ \& \ \frac{a_1}{b_1} = \frac{a_2}{b_2} \Leftrightarrow a_1 b_2 = b_1 a_2 \right\}$$

Define $\bullet$:

$$\frac{a_1}{b_1} \bullet \frac{a_2}{b_2} \stackrel{\text{def}}{=} \frac{a_1 a_2}{b_1 b_2} \in \mathbf{Q}$$

Define $+$:

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} \stackrel{\text{def}}{=} \frac{a_1 b_2 + b_1 a_2}{b_1 b_2} \in \mathbf{Q}$$

This gives closure, i.e.

$$\mathbf{Q} \times \mathbf{Q} \stackrel{+,\bullet}{\rightarrow} \mathbf{Q}$$

One must check well-definedness of $+, \bullet$. If

$$\frac{a_1}{b_1} = \frac{a_1'}{b_1'}, \text{ viz., } a_1 b_1' = a_1' b_1, \ \& \ \frac{a_2}{b_2} = \frac{a_2'}{b_2'}, \text{ viz., } a_2 b_2' = a_2' b_2,$$

then we must verify that

$$\frac{a_1 a_2}{b_1 b_2} = \frac{a_1' a_2'}{b_1' b_2'}, \text{ viz., } a_1 a_2 b_1' b_2' = a_1' a_2' b_1 b_2,$$

and

$$\frac{a_1 b_2 + b_1 a_2}{b_1 b_2} = \frac{a_1' b_2' + b_1' a_2'}{b_1' b_2'}, \text{ viz., } (a_1 b_2 + b_1 a_2)(b_1' b_2') = (a_1' b_2' + b_1' a_2')(b_1 b_2)$$

This is left as an exercise for the reader.

WARNING: Suppose we defined on $\tilde{+}$ on $\mathbf{Q}$ by the formula

$$\frac{a_1}{b_1}\tilde{+}\frac{a_2}{b_2} = \frac{a_1+a_2}{b_1+b_2}.$$

Then the operation $\tilde{+}$ is <u>not</u> well-defined on $\mathbf{Q}$. The reason is as follows: $\frac{1}{2} = \frac{2}{4}$. Thus for example, we must require that

$$\frac{1}{2}\tilde{+}\frac{1}{3} = \frac{2}{4}\tilde{+}\frac{1}{3},$$

i.e.

$$\frac{2}{5} = \frac{1+1}{2+3} = \frac{2+1}{4+3} = \frac{3}{7},$$

i.e.

$$14 = 2\cdot 7 = 5\cdot 3 = 15,$$

which is absurd!

Ex. 2. Consider the 2 element set $\mathbf{F}_2 = \{\overline{0}, \overline{1}\}$ with binary operations $+$, $\bullet$ given by the tables below.

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\bullet$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Then it is easy to verify that $[\mathbf{F}_2, +, \bullet]$ is a field. [For example, symmetry about the diagonal implies commutivity; moreover "$-\overline{1}$" $= \overline{1}$.]

Ex. 3. Consider the 3 element set $\mathbf{F}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ with binary operations $+$, $\bullet$ given by the tables below.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Note that "$-\overline{1}$" $= \overline{2}$ and "$-\overline{2}$" $= \overline{1}$. Further, $\overline{2}^{-1} = \overline{2}$. One can easily verify that $[\mathbf{F}_3, +, \bullet]$ is a field.

Ex. 4. Ex. 2. Consider the 2 element set $\mathbf{F} = \{\overline{0}, \overline{5}\}$ with binary operations $+$, $\bullet$ given by the tables below.

$+$	$\overline{0}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{0}$

$\bullet$	$\overline{0}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{5}$	$\overline{0}$	$\overline{5}$

This is a field, with unity $\overline{5}$. It is a carbon copy of Ex. 2. The point here is to not get too attached to "labels".

We want to revisit the situation of the inclusions

$$\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R}.$$

It is a fact that $+, \bullet$ on $\mathbf{Z}$ and $\mathbf{Q}$ come from $+, \bullet$ on $\mathbf{R}$.

Definition. Let $[\mathbf{A}; +, \bullet]$ be a ring [resp. field]. Suppose $\mathbf{B} \subset \mathbf{A}$ is a subset that is closed under $+, \bullet$ from $\mathbf{A}$, in such a way that $[\mathbf{B}; +, \bullet]$ is a ring [resp. field]. Then $[\mathbf{B}; +, \bullet]$ is called a subring [resp. subfield] of $\mathbf{A}$.

Picture :

$$\begin{array}{ccc} \mathbf{A} \times \mathbf{A} & \overset{+,\bullet}{\rightarrow} & \mathbf{A} \\ \bigcup & \overset{+,\bullet}{\nearrow} & \bigcup \\ \mathbf{B} \times \mathbf{B} & \overset{+,\bullet}{\rightarrow} & \mathbf{B} \end{array}$$

Note that any subring (resp. subfield) is itself a ring (resp. field).

Examples. 1. $\mathbf{Z} \subset \mathbf{Q}$ is a subring.

2. $\mathbf{Q} \subset \mathbf{R}$ is a subfield.

3. $2\mathbf{Z} := \{0, \pm 2, \pm 4, \pm 6, \pm 8, \ldots\} \subset \mathbf{Z}$ is a subring. [Note that $[2\mathbf{Z}; +, \bullet]$ is a ring without unit.]

4. The odd integers $\{\pm 1, \pm 3, \pm 5, \ldots\}$ with $+, \bullet$ induced from $\mathbf{Z}$, do not form a ring. [No zero element, and not closed under addition.]

WARNING Keep in mind the following:

1. $[\mathbf{F}_2; +, \bullet] \not\subset [\mathbf{F}_3; +, \bullet]$

2. $[\mathbf{F}_2; +, \bullet] \not\subset [\mathbf{R}; +, \bullet]$

3. $[\mathbf{F}_3; +, \bullet] \not\subset [\mathbf{R}; +, \bullet]$.

4. $[\mathbf{N}; +, \bullet] \subset [\mathbf{Z}; +, \bullet]$ is not a subring.

Example. Let

$$\mathbf{A} = \left\{ \frac{p}{2^q} \;\middle|\; p, q \in \mathbf{Z} \;\&\; q \geq 0 \right\} \subset \mathbf{Q}$$

Claim 1) $\mathbf{A}$ is a subring (with unit) of $[\mathbf{Q}; +, \bullet]$.

2) $\mathbf{A}$ is *not* a subfield of $[\mathbf{Q}; +, \bullet]$.

Reason for 1): Let $\frac{p_1}{2^{q_1}}$, $\frac{p_2}{2^{q_2}} \in \mathbf{A}$ be given. Then

$$\frac{p_1}{2^{q_1}} \cdot \frac{p_2}{2^{q_2}} = \frac{p_1 p_2}{2^{q_1+q_2}} \in \mathbf{A}$$

$$\frac{p_1}{2^{q_1}} + \frac{p_2}{2^{q_2}} = \frac{(p_1 2^{q_2} + p_2 2^{q_1})}{2^{q_1+q_2}} \in \mathbf{A}$$

Thus $\mathbf{A}$ is closed under $+, \bullet$ from $\mathbf{Q}$. Next, we must show that $[\mathbf{A}; +, \bullet]$ is a ring (with unity). But we know that $[\mathbf{Q}; +, \bullet]$ satisfies the associative, commutative and distributive laws, and that $\mathbf{A}$ being closed under $+, \bullet$ from $\mathbf{Q}$ implies that the corresponding laws must hold for $\mathbf{A}$. Further, $\frac{p}{2^q} \in \mathbf{A} \Rightarrow -\frac{p}{2^q} = \frac{(-p)}{2^q} \in \mathbf{A}$, i.e. one has additive inverses. Also $0 = \frac{0}{2^1} \in \mathbf{A}$ and $1 = \frac{1}{2^0} \in \mathbf{A}$. Thus $[\mathbf{A}; +, \bullet]$ must be a ring with unity. This implies part 1) of the claim.

Reason for 2): It suffices to find a non-zero element of $\mathbf{A}$ with no multiplicative inverse in $\mathbf{A}$. Note that such an inverse can be found in $\mathbf{Q}$. Consider $3 = \frac{3}{2^0} \in \mathbf{A}$. If $3^{-1} \in \mathbf{A}$, then we would have, for some $p, q \in \mathbf{Z},\ q \geq 0$

$$\frac{1}{3} = \frac{p}{2^q}, \quad \text{i.e.,} \quad 2^q = 3p$$

There are two reasons why this cannot happen:

Reason (i): The Fundamental Theorem of Arithmetic (to be discussed later) implies that integer $2^q = 3p$ has a unique decomposition into primes. But 2^q is already a prime decomposition, which doesn't contain the prime number 3, violating uniqueness!

Reason (ii): We must have $q \geq 1$, hence 2^q is even, hence $3p$ is even. Thus $p = 2p_1$ is even ($p_1 \geq 1$). And so $2^{q-1} = 3p_1$. Therefore $q - 1 \geq 1$, hence $p_1 = 2p_2$ ($p_2 \geq 1$) for the same reason, and hence $2^{q-2} = 3p_2$, and so on. Clearly this process must end, after say m steps, with $1 = 2^0 = 3p_m$, for some $p_m \geq 1$, which is absurd!

In summary, $3 \in \mathbf{A},\ 3 \neq 0$ and yet $3^{-1} \notin \mathbf{A}$. I.e. $\mathbf{A}$ is not a subfield of $\mathbf{Q}$, hence part 2) of the claim follows.

Example. The Complex Numbers $\mathbf{C}$.

Motivation. The equation $x + 1 = 0$ has no solution in $\mathbf{N}$. The invented solution $x =$ "-1" leads to an enlargement of $\mathbf{N}$ to $\mathbf{Z}$. In a similar vein, the quadratic equation

$x^2+1=0$ has no solution in $\mathbf{R}$. An invented solution $x=$ "$\sqrt{-1}$" will lead to an extention of $\mathbf{R}$ to the Complex Numbers $\mathbf{C}$. Of course, $(\sqrt{-1})^2=(-\sqrt{-1})^2=-1$. We fix a choice of $\sqrt{-1}$.

Definition. The Complex Numbers are given by

$$\mathbf{C}:=\left\{z=x+\sqrt{-1}y \;\middle|\; x,y\in\mathbf{R}\right\}.$$

The Complex Numbers can be identified with the $xy-$plane $\mathbf{R}^2$ by the dictionary $z=x+\sqrt{-1}y\in\mathbf{C}\leftrightarrow(x,y)\in\mathbf{R}^2$. Further, $z=x+\sqrt{-1}y=0\Leftrightarrow(x,y)=(0,0)$, (otherwise one would end up with $\sqrt{-1}\in\mathbf{R}$, which is not the case since $(\sqrt{-1})^2=-1<0$). We define $+,\bullet$ on $\mathbf{C}$ as follows. Let $z_1=x_1+\sqrt{-1}y_1,\ z_2=x_2+\sqrt{-1}y_2\in\mathbf{C}$.

$$z_1+z_2=(x_1+x_2)+\sqrt{-1}(y_1+y_2)\in\mathbf{C}$$

$$z_1\bullet z_2\overset{(\sqrt{-1})^2=-1}{=}(x_1x_2-y_1y_2)+\sqrt{-1}(x_1y_2+x_2y_1)\in\mathbf{C}$$

It is obvious that $\mathbf{C}$ is closed under $+,\bullet$. Further $\mathbf{R}\subset\mathbf{C}$, where $x\in\mathbf{R}\mapsto z=x+0\sqrt{-1}\in\mathbf{C}$. [Note that $z_1=z_2\Leftrightarrow x_1=x_2\ \&\ y_1=y_2$. This is because $z_1=z_2\Leftrightarrow z_1-z_2=0\Leftrightarrow(x_1-x_2)+\sqrt{-1}(y_1-y_2)=0\Leftrightarrow(x_1-x_2)=0\ \&\ (y_1-y_2)=0$.]

Example Calculations: (i) $(2+4\sqrt{-1})+(-5+\sqrt{-1})=-3+5\sqrt{-1}$

(ii) $(2-4\sqrt{-1})\cdot(-5+\sqrt{-1})=(-10+4)+\sqrt{-1}(20+2)=-6+22\sqrt{-1}$

Claim 1) $[\mathbf{C};+,\bullet]$ is a field.

2) $[\mathbf{R};+,\bullet]\subset[\mathbf{C};+,\bullet]$ is a subfield. [We leave this part as an exercise for the reader.]

Reason for 1) (Outline only): The reader can easily check that associativity, commutivity, and the distributive laws hold for $[\mathbf{C};+,\bullet]$. Since $\mathbf{R}\subset\mathbf{C}$, it follows that $0,\ 1\in\mathbf{C}$ and that $1\neq0$. Also $z=x+\sqrt{-1}y\in\mathbf{C}\Rightarrow-z:=(-x)+\sqrt{-1}(-y)\in\mathbf{C}$. Next, suppose $z=x+\sqrt{-1}y\in\mathbf{C}$, with $z\neq0$ (hence $(x,y)\neq(0,0)$, or $x^2+y^2\neq0$). Thus formally

$$z^{-1}=\frac{1}{z}=\frac{1}{x+\sqrt{-1}y}=\frac{1}{x+\sqrt{-1}y}\cdot\left(\frac{x-\sqrt{-1}y}{x-\sqrt{-1}y}\right)=\left(\frac{x}{x^2+y^2}\right)+\sqrt{-1}\left(\frac{-y}{x^2+y^2}\right)\in\mathbf{C},$$

gives the formula for z^{-1}, namely

$$z^{-1}:=\left(\frac{x}{x^2+y^2}\right)+\sqrt{-1}\left(\frac{-y}{x^2+y^2}\right).$$

For example

$$\frac{1}{2+3\sqrt{-1}}=\frac{2}{13}-\frac{3}{13}\sqrt{-1}.$$

Thus in summary, all 9 axiomatic properties of a field hold for $[\mathbf{C}; +, \bullet]$, and hence we are done, i.e. $[\mathbf{C}; +, \bullet]$ is a field.

Example. The reader can easily verify the following:

$$\mathbf{Q}[\sqrt{-1}] \stackrel{\text{def}}{=} \left\{z = a + \sqrt{-1}b \mid a, b \in \mathbf{Q}\right\}$$

is a subfield of $\mathbf{C}$. Furthermore, $\mathbf{Q}$ is a subfield of $\mathbf{Q}[\sqrt{-1}]$.

Complex Conjugation and the Norm on $\mathbf{C}$.

Conjugation. Let $z = x + \sqrt{-1}y \in \mathbf{C}$ be given. The complex conjugate of z is given by $\overline{z} = x - \sqrt{-1}y$.

Exercise. Show that the operation of complex conjugation is well-defined. [Hint: Use the fact that if $z_1 = x_1 + \sqrt{-1}y_1$ and $z_2 = x_2 + \sqrt{-1}y_2$, then $z_1 = z_2 \Leftrightarrow x_1 = x_2$ & $y_1 = y_2$.]

Exercise: Show that $\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2$, $\overline{z_1 z_2} = \overline{z}_1 \overline{z}_2$, and $\overline{z_1/z_2} = \overline{z}_1/\overline{z}_2$.

Norm. The norm is a map $N : \mathbf{C} \to \mathbf{R}_+ := [0, \infty)$ given by the formula $N(z) = z\overline{z}$. If we write $z = x + \sqrt{-1}y$, then $N(z) = x^2 + y^2$. Note that $N(z) = 0 \Leftrightarrow z = 0$.

Exercise: Show that $N(z_1 z_2) = N(z_2)N(z_2)$. [Hint: Use the results of the previous exercise, namely $\overline{z_1 z_2} = \overline{z}_1 \overline{z}_2$.]

We can easily rewrite the inverse z^{-1} of a given non-zero $z \in \mathbf{C}$ in terms of the norm. Namely, and observing $N(z) > 0$,

$$z^{-1} = \frac{1}{z} \cdot \frac{\overline{z}}{\overline{z}} = \frac{\overline{z}}{N(z)} = \frac{x}{N(z)} + \left(\frac{-y}{N(z)}\right)\sqrt{-1} \in \mathbf{C}.$$

Example: [Gaussian Integers] Define

$$\mathbf{Z}[\sqrt{-1}] = \left\{a + b\sqrt{-1} \;\middle|\; a, b \in \mathbf{Z}\right\}$$

Claim 1) $\mathbf{Z}[\sqrt{-1}]$ is a subring (with unity) of $[\mathbf{C}; +, \bullet]$.

2) $\mathbf{Z}[\sqrt{-1}]$ is not a subfield of $[\mathbf{C}; +, \bullet]$.

Reason for 1): Let $z_1 = a_1 + b_1\sqrt{-1}$, $z_2 = a_2 + b_2\sqrt{-1} \in \mathbf{Z}[\sqrt{-1}]$ be given. Then

$$z_1 + z_2 = (a_1 + a_2) + (b_1 + b_2)\sqrt{-1} \in \mathbf{Z}[\sqrt{-1}],$$

and

$$z_1 z_2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)\sqrt{-1} \in \mathbf{Z}[\sqrt{-1}],$$

since $\mathbf{Z}$ is closed under $+, \bullet$. Therefore $\mathbf{Z}[\sqrt{-1}]$ is closed under $+, \bullet$ from $\mathbf{C}$. Therefore, since $\mathbf{C}$ satisfies the associative, commutative and distributive laws, the same must hold

for $\mathbf{Z}[\sqrt{-1}]$. It is easy to see that $\mathbf{Z}[\sqrt{-1}]$ has additive inverses, and that $\mathbf{Z} \subset \mathbf{Z}[\sqrt{-1}]$. Hence $0,\ 1 \in \mathbf{Z}[\sqrt{-1}]$. Thus $\mathbf{Z}[\sqrt{-1}]$ is a subring of $[\mathbf{C}; +, \bullet]$.

Reason for 2): If $z \in \mathbf{Z}[\sqrt{-1}]$, then $N(z) \in \mathbf{Z}_+ := \{0, 1, 2, 3, \ldots\}$; moreover $z \neq 0 \Leftrightarrow N(z) \in \mathbf{N}$. Now suppose that $z \neq 0$ and that $zw = 1$ for some $w \in \mathbf{Z}[\sqrt{-1}]$. Then

$$N(z)N(w) = N(zw) = N(1) = 1,$$

and therefore $N(z) = N(w) = 1$. If we write $z = a + b\sqrt{-1} \in \mathbf{Z}[\sqrt{-1}]$, then $1 = N(z) = a^2 + b^2$. Thus, since $a, b \in \mathbf{Z}$, it follows that

$$(a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\},$$

i.e.

$$z \in \{1, -1, \sqrt{-1}, -\sqrt{-1}\}.$$

We conclude that $z \in \mathbf{Z}[\sqrt{-1}]$ has a multiplicative inverse $\Leftrightarrow N(z) = 1 \Leftrightarrow z = \pm 1,\ \pm\sqrt{-1}$. So for example $1 + \sqrt{-1} \in \mathbf{Z}[\sqrt{-1}]$, is non-zero, and yet does *not* have a multiplicative inverse in $\mathbf{Z}[\sqrt{-1}]$. Therefore $\mathbf{Z}[\sqrt{-1}]$ is not a subfield of $\mathbf{C}$.

Exercise: Show that $\mathbf{Z}$ is a subring of $\mathbf{Z}[\sqrt{-1}]$.

Definition. Let $\mathbf{A}$ be a ring with unity $1 \neq 0$. An element $a \in \mathbf{A}$ is called a <u>unit</u> if there exists $b \in \mathbf{A}$ such that $ab = 1$, i.e. a has a multiplicative inverse $b = a^{-1} \in \mathbf{A}$. The set of units in $\mathbf{A}$ is denoted by $\mathbf{A}^*$.

Exercise. Show that if $x, y \in \mathbf{A}^*$, then $x^{-1},\ xy \in \mathbf{A}^*$. $\mathbf{A}^*$ is an example of an abelian group. In particular, <u>$\mathbf{A}^*$ is called the group of units in $\mathbf{A}$</u>. [Note that $\pm 1 \in \mathbf{A}^*$.]

Example. $\mathbf{Z}^* = \{1, -1\}$, which is clearly is closed under multiplication and taking multiplicative inverses.

Example. $(\mathbf{Z}[\sqrt{-1}])^* = \{1, -1, \sqrt{-1}, -\sqrt{-1}\}$, which again is closed under multiplication and taking multiplicative inverses.

Example. $\mathbf{R}^* = \{x \in \mathbf{R} \mid x \neq 0\}$. More generally, given any field $\mathbf{F}$, $\mathbf{F}^* = \{x \in \mathbf{F} \mid x \neq 0\}$.

<u>Example</u>: Define

$$\mathbf{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \;\middle|\; a, b \in \mathbf{Q}\right\}$$

Claim. 1) $\mathbf{Q}[\sqrt{2}]$ is a subfield of $[\mathbf{R}; +, \bullet]$.

2) $\mathbf{Q}$ is a subfield of $\mathbf{Q}[\sqrt{2}]$. [This is an exercise for the reader.]

Reason for 1): Let $z_1 = a_1 + b_1\sqrt{2},\ z_2 = a_2 + b_2\sqrt{2} \in \mathbf{Q}[\sqrt{2}]$ be given. Then

$$z_1 + z_2 = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in \mathbf{Q}[\sqrt{2}],$$

and

$$z_1 z_2 = (a_1 a_2 + b_1 b_2) + (a_1 b_2 + 2 b_1 a_2)\sqrt{2} \in \mathbf{Q}[\sqrt{2}],$$

since $\mathbf{Q}$ is closed under $+, \bullet$. Therefore $\mathbf{Q}[\sqrt{2}]$ is closed under $+, \bullet$ from $\mathbf{R}$. Therefore, since $\mathbf{R}$ satisfies the associative, commutative and distributive laws, the same must hold for $\mathbf{Q}[\sqrt{2}]$. It is easy to see that $\mathbf{Q}[\sqrt{2}]$ has additive inverses, and that $\mathbf{Q} \subset \mathbf{Q}[\sqrt{2}]$. Hence $0,\ 1 \in \mathbf{Q}[\sqrt{2}]$ and $1 \neq 0$. Thus $\mathbf{Q}[\sqrt{2}]$ is a subring of $[\mathbf{R}; +, \bullet]$. To show that $\mathbf{Q}[\sqrt{2}]$ is a subfield, we need to verify that there are multiplicative inverses to non-zero elements. For this, we must use the fact that $\sqrt{2} \notin \mathbf{Q}$. We will assume this fact for now. Note that if $z = a + b\sqrt{2} \in \mathbf{Q}[\sqrt{2}]$, then $z = 0 \Leftrightarrow a = b = 0$, for if for example $z = 0$ and say $b \neq 0$, then $\sqrt{2} = -\frac{a}{b} \in \mathbf{Q}$, contrary to the above fact. Thus it follows that $z_1 = z_2 \Leftrightarrow a_1 = a_2$ & $b_1 = b_2$. In particular, the "conjugate" operation given by $\overline{z} := a - b\sqrt{2}$ is <u>well-defined</u>. [Warning: $\overline{z}$ is *not* complex conjugation!] One can show that

$$\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2 \quad ; \quad \overline{z_1 z_2} = \overline{z}_1 \overline{z}_2.$$

We introduce the norm $N : \mathbf{Q}[\sqrt{2}] \to \mathbf{Q}$ by the formula $N(z) = z\overline{z} = a^2 - 2b^2$. Note again, that $N(z) = 0 \Leftrightarrow z = 0$, otherwise one can show that $\sqrt{2} \in \mathbf{Q}$, which violates the fact. Thus if $z \neq 0$, then $N(z) \in \mathbf{Q}$ and $N(z) \neq 0$. So formally, we have:

$$\frac{1}{z} = \frac{1}{z}\frac{\overline{z}}{\overline{z}} = \frac{\overline{z}}{N(z)} = \left(\frac{a}{N(z)}\right) + \left(\frac{-b}{N(z)}\right)\sqrt{2} \in \mathbf{Q}[\sqrt{2}].$$

This gives the formula for $z^{-1} \in \mathbf{Q}[\sqrt{2}]$, namely,

$$z^{-1} = \left(\frac{a}{N(z)}\right) + \left(\frac{-b}{N(z)}\right) = \left(\frac{a}{a^2 - 2b^2}\right) + \left(\frac{-b}{a^2 - 2b^2}\right)\sqrt{2},$$

and we are done.

We now establish the

<u>Fact</u>. $\sqrt{2} \notin \mathbf{Q}$, i.e. $\sqrt{2}$ is irrational.

Reason: Suppose to the contrary that $\sqrt{2} \in \mathbf{Q}$. Then we can write $\sqrt{2} = \frac{p}{q}$, where $p, q \in \mathbf{N}$, and that the fraction $\frac{p}{q}$ is in reduced form, i.e. where p & q have no common integral factors ≥ 2. But

$$\sqrt{2} = \frac{p}{q} \Leftrightarrow \sqrt{2}q = p \Rightarrow 2q^2 = p^2.$$

Since $2q^2$ is even, it follows that p^2 is even, hence $p = 2p_1$ is even (i.e. for some $p_1 \in \mathbf{N}$). Therefore

$$2q^2 = p^2 = (2p_1)^2 = 4p_1^2 \Rightarrow q^2 = 2p_1^2.$$

By the same reasoning, q must also be even, and hence 2 is a common factor of p & q, violating the fact that p & q have no common integral factors ≥ 2. Thus $\sqrt{2} \notin \mathbf{Q}$, and we are done.

Mathematical Induction

Let $P(n)$ be a statement about $n \in \mathbf{N} = \{1, 2, 3, \ldots\}$. The problem is to show that $P(n)$ is true for all $n \in \mathbf{N}$.

$$\underline{\text{Two approaches}}: \begin{cases} \text{(i)} & \text{Indirect approach - argue by contradiction} \\ \text{(ii)} & \text{Direct approach - domino effect} \end{cases}.$$

Induction, Part I: Indirect Approach

Ex. 1. Claim:

$$\text{Statement } P(n): \ 1 + 2 + \ldots + n = \frac{n(n+1)}{2}, \quad \text{for all } n \in \mathbf{N}.$$

Proof. If $n = 1$, then

$$\text{LHS } = 1 = \frac{1(1+1)}{2} = \text{ RHS, therefore } P(1) \text{ is True.}$$

If $n = 2$, then

$$\text{LHS } = 1 + 2 = 3 = \frac{2(2+1)}{2} = \text{ RHS}, \quad \text{therefore } P(2) \text{ is True.}$$

Thus we know that $P(1)$, $P(2)$ are both true. Assume to the contrary that $P(n)$ is in general not true. Thus one can find a smallest positive integer N[†] for which $P(N)$ fails to be true, i.e.:

$$(*) \qquad 1 + 2 + \cdots + N \neq \frac{N(N+1)}{2} \quad [\text{Note } N > 2]$$

Since N is the smallest, clearly $P(N-1)$ is true. Thus,

$$1 + 2 \ldots + (N-1) = \frac{(N-1)\big((N-1)+1\big)}{2}.$$

i.e.

$$1 + \cdots + (N-1) = \frac{(N-1)N}{2}.$$

Adding N to both sides yields:

$$1 + \cdots + (N-1) + N = \frac{(N-1)N}{2} + N$$

[†] This is due to the "well-ordering principle", which says that any non-empty subset of $\mathbf{N}$ has a smallest element.

$$= \frac{(N-1)N}{2} + \frac{2N}{2}$$

$$= \frac{(N+1)N}{2}$$

i.e.

$$1 + \cdots + N = \frac{N(N+1)}{2}, \quad \text{violating } (*).$$

Therefore $P(n)$ must be true for all $n \in \mathbf{N}$.

Ex. 2. Every positive integer is interesting!

Restatement. $P(n)$: "n is interesting", $n \in \mathbf{N}$

Proof. $P(1)$: 1 is interesting, because: 1 is the loneliest number you'll ever be.[†]

$P(2)$: 2 is interesting, because: 2 can be as bad as 1, being the loneliest number to the number 1.

$P(3) : 3 = 1 + 2$, therefore is interesting.

Now lets assume to contrary that $P(n)$ is not in general true. $\Rightarrow P(n)$ fails for some smallest integer N, i.e. "N is boring". But $1, 2, \ldots (N-1)$ are interesting, and N is the $\star$very first$\star$ dull number. Well that's interesting! A contradiction.

Silly Example: Any (finite) collection of billiard balls are RED! Restatement: $P(n)$: Every n billiard balls are red, $n \in \mathbf{N}$.

Proof. Suppose in general not true. Then $P(N)$ fails for some smallest N. Therefore $P(N-1)$ true, i.e. every set of $N-1$ billiard balls are red. Consider N billiard balls: Label them as $\{b_1, b_2, \ldots, b_{N-1}, b_N\}$. Then:

$$\{b_1, \ldots b_N\} = \underbrace{\{b_1, \ldots, b_{N-1}\}}_{N-1 \text{ balls, thus all red}} \bigcup \underbrace{\{b_2, \ldots, b_N\}}_{N-1 \text{ balls, thus all red}} .$$

Hence $\{b_1, \ldots, b_N\}$ are red, being a union of red balls. I.e. $P(N)$ must be true

Question: What is the problem with this proof?

Answer: $P(1)$ is False! $P(1)$: Every billiard ball is red, is clearly false!

Induction, Part II: Direct Approach

[†] Taken from the lyrics of Three Dog Nite.

Given: $P(n)$ is a statement about $n \in \mathbf{N}$. Need to show that $P(n)$ is true for all $n \in \mathbf{N}$. The procedure is this:

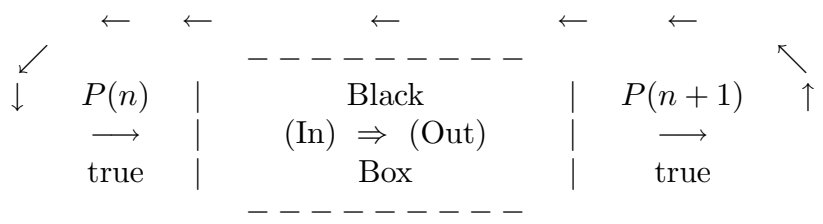
(1) Show that $P(1)$ is true.

(2) Induction step: Show that $P(n)$ true $\Rightarrow P(n+1)$ is true.

(3) Hence $P(n)$ is true for all $n \in \mathbf{N}$.

The procedure works like this:

(1) $\Rightarrow P(1)$ true. But (2) $\Rightarrow P(2) = P(1+1)$ true. Again, by (2): $P(2) \Rightarrow P(3) = P(2+1)$ true. $P(3)$ true $\Rightarrow P(4) = P(3+1)$ true, and so on...



The "Picture" should be seen as a Domino effect:

$$\overset{\text{(Push)}}{\mapsto} /////// |||||||$$

Example. Claim:

$$1 + 3 + 5 + \cdots + (2n-1) = n^2.$$

Restatement: Let $P(n)$: $\quad 1 + 3 + 5 \cdots + (2n-1) = n^2$. Then $P(n)$ true for all $n \in \mathbf{N}$.

Proof. Case $n = 1$: LHS $= 1 =$ RHS $\Rightarrow P(1)$ true.

Induction Step: Assume $P(n)$ is true, for a given $n \geq 1$, i.e.

$$(1) \qquad 1 + 3 + 5 + \ldots + (2n-1) = n^2.$$

Must show that $P(n+1)$ is true, i.e.

$$(2) \qquad 1 + 3 + 5 + \cdots + (2n-1) + \big(2(n+1) - 1\big) = (n+1)^2.$$

Trick: Must make (1) look like (2). To do this, we add $\big(2(n+1)-1\big)$ to both sides of (1). Thus:

$$1 + 3 + 5 + \cdots + (2n-1) + \big(2(n+1) - 1\big) = n^2 + \big(2(n+1) - 1\big).$$

This leads to:

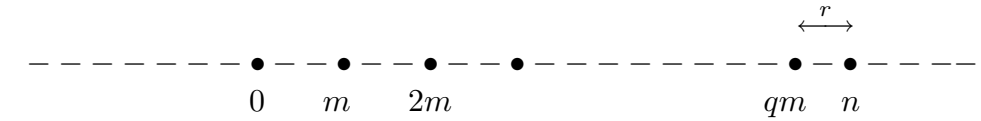
$$1 + 3 + \cdots + \big(2(n+1) - 1\big) = n^2 + 2n + 1 = (n+1)^2, \quad \Rightarrow \ P(n+1) \quad \text{True.}$$

Thus $P(n)$ is true for all $n \in \mathbf{N}$.

Division and Factoring

Euclid Division Algorithm. Let $n, m \in \mathbf{Z}$ be given with $m \geq 1$. Then there exists unique integers $r, q \in \mathbf{Z}$ with $0 \leq r < m$ such that $n = qm + r$.

We give a geometric picture below to "explain" the *existence* of q, r. For simplicity, we assume $n > 0$ and say $n \geq m$; and we leave the geometric picture for the case $n \leq 0$ to the reader.



For the *uniqueness* of q & r, we argue as follows. Suppose

$$(*) \qquad qm + r = n = \tilde{q}m + \tilde{r},$$

where $q, \tilde{q}, r, \tilde{r} \in \mathbf{Z}$ and where $0 \leq r, \tilde{r} < m$. We must show that $q = \tilde{q}$ and $r = \tilde{r}$. But $(*)$ implies that

$$(q - \tilde{q})m = \tilde{r} - r,$$

hence

$$\underbrace{|q - \tilde{q}|m}_{\text{Either } =0 \text{ or } \geq m} \quad = \quad \underbrace{|\tilde{r} - r| < m}_{\text{Follows from } 0 \leq r, \tilde{r} < m} \quad .$$

Thus we must have $q - \tilde{q} = r - \tilde{r} = 0$.

Definition. Given integers n & m with $m \neq 0$, we say that m divides n (in $\mathbf{Z}$), and in this case write $m|n$, if $n = mq$ for some $q \in \mathbf{Z}$ (i.e. zero remainder). Equivalently, m is an integral factor of n.

Example. $2|6$, $3|6$, $7|14$, $2 \not| 5$, where $\not|$ means "does not divide".

Definition. Assume given integers $m, n \in \mathbf{Z}$, not both zero. The Greatest Common Divisor (GCD) of m & n is an integer $d \in \mathbf{N}$ such that:

(1) $d|n$ and $d|m$ (i.e. d is a common divisor, viz., d is a factor).

(2) if $\ell|n$ & $\ell|m$ for some integer $\ell \neq 0$, then $\ell|d$ (i.e. d is the greatest).

Notation: $d = \text{GCD}(m, n) = (m, n)$.

Claim. Let $d = (m, n)$. Then d is unique. Restatement: Suppose d & $d_1 \in \mathbf{N}$ both satisfy (1) and (2) of the above definition. Then $d = d_1$.

Reason: Use d in (1) and set $\ell = d_1$ in (2). Then $d_1|d$. Similarly, d_1 being a GCD implies that $d|d_1$. But

$$d_1|d \Leftrightarrow e_1 d_1 = d \quad \text{for some } e_1 \in \mathbf{N},$$

$$d|d_1 \Leftrightarrow e_2 d = d_1 \quad \text{for some } e_2 \in \mathbf{N}.$$

By substitution, $e_1 e_2 d = d$, hence $e_1 e_2 = 1$. Therefore $e_1 = e_2 = 1$, i.e. $d = d_1$.

Claim. For any pair of integers m & n, not both zero, GCD(m, n) exists, i.e. there exists $d \in \mathbf{N}$ satisfying (1) and (2) above.

Reason: There are essentially three methods of proof. The first is somewhat theoretical, but has the advantage of applying to more generalized situations. The second uses the Euclidean Division Algorithm in an explicit way to compute the GCD. The third approach is a consequence of the Fundamental Theorem of Arithmetic. We discuss the first method (the other methods will be discussed later). We first introduce the concept of an ideal.

Step 1. **Definition.** A subset $\mathcal{U} \subset \mathbf{Z}$ is called an ideal if:

(i) $a, b \in \mathcal{U} \Rightarrow a + b \in \mathcal{U}$, [i.e. $\mathcal{U}$ is closed under $+$ from $\mathbf{Z}$].

(ii) $a \in \mathcal{U},\ b \in \mathbf{Z} \Rightarrow ba \in \mathcal{U}$, [i.e. $\mathcal{U}$ is closed under scalar multiplication from $\mathbf{Z}$].

Picture:

$$\text{(i)} \quad \begin{array}{ccc} \mathcal{U} \times \mathcal{U} & \xrightarrow{+} & \mathcal{U} \\ \cap \quad \cap & & \cap \\ \mathbf{Z} \times \mathbf{Z} & \xrightarrow{+} & \mathbf{Z} \end{array} \qquad \text{(ii)} \quad \begin{array}{ccc} \mathbf{Z} \times \mathcal{U} & \xrightarrow{\bullet} & \mathcal{U} \\ \cap \quad \cap & & \cap \\ \mathbf{Z} \times \mathbf{Z} & \xrightarrow{\bullet} & \mathbf{Z} \end{array}$$

Examples of Ideals.

(1) $\mathcal{U} = (0) := \{0\} \subset \mathbf{Z}$ "zero ideal". [$0 + 0 = 0 \in \mathcal{U}$ and $b \bullet 0 = 0 \in \mathcal{U}$, whenever $b \in \mathbf{Z}$.]

(2) $\mathcal{U} = (1) := \mathbf{Z}$. Clearly an ideal! [Complete ring of integers.]

(3) $\mathcal{U} = (2) := 2\mathbf{Z} \overset{\text{def'n}}{=} \{2q \mid q \in \mathbf{Z}\} = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$ is an ideal. [Details: Suppose $a = 2q_1,\ b = 2q_2$. Then $a + b = 2(q_1 + q_2) \in (2)$. Next, if $a = 2q \in \mathcal{U}$ and $b \in \mathbf{Z}$, then $ba = 2(bq) \in \mathcal{U}$.]

(4) Fix $k \in \mathbf{Z}$, and set $\mathcal{U} = (k) := k\mathbf{Z} = \{kq \mid q \in \mathbf{Z}\} = \{0, \pm k, \pm 2k, \pm 3k, \ldots\}$. Then $\mathcal{U}$ is an ideal (exercise). [This generalizes the previous three examples, where $k = 0, 1, 2$.]

Example:

Definition. An ideal $\mathcal{U} \subset \mathbf{Z}$ is said to be principal, If $\mathcal{U} = (k)$ For some fixed $k \in \mathbf{Z}$.

Step II. **Claim.** Every ideal $\mathcal{U} \subset \mathbf{Z}$ is principal. [In this case we call $\mathbf{Z}$ a PID (= a Principal Ideal Domain).]

Reason: Let $\mathcal{U} \subset \mathbf{Z}$ be any ideal. If $\mathcal{U} = 0 = (0)$, then we are done, by choosing $k = 0$. So assume that $\mathcal{U} \neq (0)$. Note that if $\ell \in \mathcal{U}$ with $\ell \neq 0$, then $\ell,\ -\ell = (-1) \cdot \ell \in \mathcal{U}$.

Thus $\mathcal{U} \cap \mathbf{N} \neq \emptyset$. So choose $k \in \mathcal{U} \cap \mathbf{N}$ to be the *smallest* integer ≥ 1. We want to show that $\mathcal{U} = (k)$. To see this, let $m \in \mathcal{U}$ be given. Then by Euclid's Division Algorithm, $m = qk + r$, for some $q, r, \in \mathbf{Z}$, and where $0 \leq r < k$. Thus $r = m - qk = m + (-q)k \in \mathcal{U}$, i.e. $r \in \mathcal{U}$. But if $r \geq 1$ then $r \in \mathcal{U}$ and $r < k$, which is impossible by definition of the "smallest" k. Therefore $r = 0$, i.e. $m = qk \in (k)$. Since m is any given element of $\mathcal{U}$, it follows that $\mathcal{U} \subset (k)$. However, $(k) \subset \mathcal{U}$, by definition of an ideal. Hence $\mathcal{U} = (k)$, and we're done.

Step III. Conclusion of the proof of the existence of $d = (m, n)$.

First, recall that m & n are not both zero. Let

$$\mathcal{U} = \{xm + yn \mid x, y \in \mathbf{Z}\}.$$

We leave it as an easy exercise for the reader to show that $\mathcal{U} \subset \mathbf{Z}$ is an ideal. Note that $m = 1 \cdot m + 0 \cdot n \in \mathcal{U}$, and $n = 0 \cdot m + 1 \cdot n \in \mathcal{U}$. Thus $\mathcal{U} \neq (0)$, since m & n are not both 0. Since $\mathcal{U}$ is a ideal $\neq (0)$, then by Step II, $\mathcal{U} = (k)$ for some $k \in \mathbf{Z}$ with $k \neq 0$. Note that $\pm k \in (k) = \mathcal{U}$, hence $|k| \in \mathcal{U}$. Put $d = |k|$, and note that $\mathcal{U} = (d)$. We want to show that $d = (m, n)$. But since $m, n \in \mathcal{U} = (d)$, it follows that $m = d\ell_1$ and $n = d\ell_2$ for some $\ell_1, \ell_2 \in \mathbf{Z}$. That is, $d|m$ & $d|n$. Next, since $d \in \mathcal{U} = \{xm + yn \mid x, y \in \mathbf{Z}\}$, it follows that $d = x_0 m + y_0 n$ for some $x_0, y_0 \in \mathbf{Z}$. Now suppose $\ell|m$ & $\ell|n$, $\ell \in \mathbf{Z}$, i.e. $k_1\ell = m$ & $k_2\ell = n$, for some $k_1, k_2 \in \mathbf{Z}$. Then $d = x_0 k_1 \ell + y_0 k_2 \ell = \ell \cdot (x_0 k_1 + y_0 k_2)$. Hence $\ell|d$. Therefore by definition of GCD, $d = (m, n)$, and we're done.

Summary. Given $m, n \in \mathbf{Z}$, not both zero, then the unique $d = (m, n) \in \mathbf{N}$ exists; moreover $d = x_0 m + y_0 n$, for some $x_0, y_0 \in \mathbf{Z}$.

Definition. $m, n \in \mathbf{Z}$, both not zero, are said to be relatively prime if $(m, n) = 1$.

Example. $(2, 3) = 1 \Rightarrow 2, 3$ are relatively prime. $(27, 5) = 1 \Rightarrow 5, 27$ are relatively prime.

Notes:

(1) If $m, n \in \mathbf{Z}$ are not both zero, then:

$$\mathcal{U} \stackrel{\text{def}}{=} \{xm + yn \mid x, y \in \mathbf{Z}\} = (d), \quad \text{where} \quad d = (m, n).$$

(2) Here is an example of (1).

$$\{2x + 3y \mid x, y \in \mathbf{Z}\} = (1), \quad [\text{Use } 1 = (2, 3)].$$

(3) {Odd numbers} $\subset \mathbf{Z}$ is *not* an ideal since (odd) + (odd) = (even).

A method for calculating GCD's. [This also leads to the existence of GCD's.] Assume given $m, n \in \mathbf{Z}$, $m, n \geq 0$, not both zero, say $m > 0$, and let $d = (m, n)$. By Euclid, $n = qm + r, \quad 0 \leq r < m, \quad q \in \mathbf{Z}$

Claim. $(n, m) = (m, r)$.

Reason: Let $d = (n, m)$, and $d_1 = (m, r)$. Then $d|m$ & $d|n \Rightarrow d|(r = n - qm), \quad \Rightarrow d|m$ & $d|r$. Thus $d|d_1$, i.e. $de_1 = d_1$, for some $e_1 \in \mathbf{N}$. Next $d_1|m$ & $d_1|r \Rightarrow d_1|(n = mq + r), \quad \Rightarrow d_1|m$ & $d_1|n$. Thus $d_1|d$, hence $d_1e_2 = d$, for some $e_2 \in \mathbf{N}$. Thus $(e_1e_2)d_1 = d_1$, i.e. $e_1 = e_2 = 1$. Thus $d = d_1$.

Algorithm to compute $d = (n, m)$. Let $n = qm+r, \quad 0 \leq r < m$. If $r = 0$, then $m = d$. So assume $r > 0$. Then $m = q_1r + r_1, \quad 0 \leq r_1 < r$. Then $d = (n, m) = (m, r) = (r, r_1)$. If $r_1 = 0$ then $d = r$ otherwise $r_1 > 0$. Next $r = q_2r_1 + r_2$, $0 \leq r_2 < r_1$. Again, $(r, r_1) = (r_1, r_2)$, and so on. But $r > r_1 > r_2 > \cdots$. Eventually end up with $r_{m+1} = 0$ for some m, hence $d = r_m$.

Ex. Compute $(240, 54)$.

$$240 = 4 \times 54 \ + \ 24 \quad \Rightarrow (240, 54) = (54, 24)$$

$$54 = 2 \times 24 \ + \ 6 \quad \Rightarrow (54, 24) = (24, 6)$$

$$24 = 4 \times 6 \ + \ 0 \quad \Rightarrow (24, 6) = 6$$

Thus $(240, 54) = 6$.

Next: Find integers x & y such that $6 = x240 + y54$.

Solution. Back substitute:

$$6 = 54 - \ 2 \times \left[24 = 240 - 4 \times 54\right]$$

$$6 = (-2) \times 240 \ + \ 9 \times 54$$

Thus $x = -2$ and $y = 9$ will do. Note that

$$6 = (-2) \times 240 \ + \ 9 \times 54 = (-2 + 54) \times 240 \ + \ (9 - 240) \times 54$$

hence $x = 52$ and $y = -231$ will also do. In other words, there are many such choices of x & y.

Claim-Definition. Let $p \in \mathbf{N}$, with $p \geq 2$. Then p is said to be a prime if either of the following two equivalent conditions hold for p.

(1) Whenever $p|(ab)$, for some $a, b, \in \mathbf{Z}$, then either $p|a$ or $p|b$. [This is the "true" definition of a prime.]

(2) Whenever $p = uv$, for some $u, v \in \mathbf{Z}$, then either $u = \pm 1$ (hence $p = \pm v$) or $v = \pm 1$ (hence $p = \pm u$). [This is the "true" definition of an irreducible.]

Claim. (1) $\Leftrightarrow$ (2), i.e. (1) & (2) are the same statements.

Reason: (1) $\Rightarrow$ (2), i.e. assume p satisfies (1) and suppose $p = uv$. Must show that $u = \pm 1$ or $v = \pm 1$. But $p = uv \overset{(1)}{\Rightarrow} p|u$ or $p|v$. Case 1: $p|u$, thus $pe = u$ for some $e \in \mathbf{Z}$. Thus $p = uv = p(ev)$. Thus $ev = 1$, hence $e = \pm 1$, $v = \pm 1$. Case 2: Similarly $p|v \Rightarrow u = \pm 1$. Conversely, we must show that (2) $\Rightarrow$ (1), i.e. suppose p satisfies (2), and that $p|(ab)$. We must show that either $p|a$ or $p|b$. If $p|a$ then we're done. So lets assume $p \not| a$. Therefore we must show that $p|b$. Let $d = (p, a)$. Then $d|a$ & $d|p$; in particular $de = p$ for some $e \in \mathbf{N}$. Since (2) holds, it follows that either $d = \pm 1$ (hence $d = 1$) or $e = \pm 1$ (hence $e = 1$). If, for example, $e = 1$, then $d = p$, and so $d|a \Rightarrow p|a$, which is not the case. Therefore $d = 1$, and hence there are integers $x, y \in \mathbf{Z}$ such that $xp + ya = (p, a) = d = 1$. Therefore multiplying this equation by b gives $xpb + yab = b$. Since $p|(ab)$ we have $p\ell = ab$ for some $\ell \in \mathbf{Z}$. Substituting this in the above equation gives $xpb + yp\ell = b$, i.e. $p(xb + y\ell) = b$. Since $xb + y\ell \in \mathbf{Z}$, it follows that $p|b$, and we're done.

We are now able to establish the

Fundamental Theorem of Arithmetic. Let n be an integer ≥ 2. Then n can be written as a product of primes in a unique way.

Restatement. The Theorem has two parts to it, namely the *existence* of a prime decomposition, and the *uniqueness* of that prime decomposition.

Existence: We can write $n = p_1^{\ell_1} \cdots p_N^{\ell_N}$, where $\{p_1, \ldots, p_N\}$ are distinct primes, and $\ell_1, \ldots, \ell_N \in \mathbf{N}$.

Uniqueness: Suppose we have

$$p_1^{\ell_1} \cdots p_N^{\ell_N} = n = q_1^{k_1} \cdots q_r^{k_r},$$

where

$$\{p_1, \ldots, p_N\} \quad \text{are distinct primes,}$$

and

$$\{q_1, \ldots, q_r\} \quad \text{are distinct primes,}$$

and where

$$\ell_1, \ldots, \ell_N, k_1, \ldots, k_r \in \mathbf{N}.$$

Then $N = r$, and up to relabelling, $p_1 = q_1, \ldots, p_N = q_N$ and $\ell_1 = k_1, \ldots, \ell_N = k_N$.

Reason: First we show the existence of a prime decomposition by mathematical induction on $n \in \mathbf{N}$, $n \geq 2$, by proving this statement:

$$P(n): \quad m \text{ is a product of primes for } 2 \leq m \leq n.$$

Case $n = 2$: $P(2)$ is obviously true since 2 is prime.

Induction step: We show that $P(n)$ true $\Rightarrow P(n+1)$ true. But if $n + 1 = p$ is prime, then $n+1$ is equal to its own prime decomposition, and hence since $P(n)$ is true, it follows

that m has a prime decomposition for $m \leq n+1$. Thus $P(n+1)$ is true in the case $n+1$ is prime. On the other hand, if $n+1$ is not prime, then we can write $n+1 = ab$, where $1 < a, b \leq n$. Since $P(n)$ is assumed true, it follows that $a = \underline{p}_1 \cdots \underline{p}_{N_1}$ and $b = \underline{\underline{p}}_1 \cdots \underline{\underline{p}}_{N_2}$ are products of primes. Therefore

$$n+1 = \big(\underline{p}_1 \cdots \underline{p}_{N_1}\big) \cdot \big(\underline{\underline{p}}_1 \cdots \underline{\underline{p}}_{N_2}\big)$$

is a product of primes.

We now establish uniqueness. It basically follows from the equivalence of the two definitions of prime ((1) & (2) above). Recall the setting above, namely

$$\underbrace{p_1^{\ell_1} \cdots p_N^{\ell_N}}_{\text{LHS}} = n = \underbrace{q_1^{k_1} \cdots q_r^{k_r}}_{\text{RHS}}.$$

Since $p_1|$LHS, it follows that $p_1|$RHS. Hence $p_1|q_1(q_1^{k_1-1}q_2^{k_2}\cdots q_r^{k_r})$, so either $p_1|q_1$ or $p_1|(q_1^{k_1-1}q_2^{k_2}\cdots q_r^{k_r})$ by (1). If $p_1|q_1$, then $p_1 = q_1$ by (2). Otherwise, continue bleeding off a q-factor of $(q_1^{k_1-1}q_2^{k_2}\cdots q_r^{k_r})$ until we get $p|q_i$ for some i. Up to relabelling, we might as well assume $i = 1$. We continue this procedure for the remaining p factors of the LHS. It follows then that $r \geq N$ and that $p_1 = q_1, \ldots, p_N = q_N$; moreover $k_1 \geq \ell_1, \ldots, k_N \geq \ell_N$. We now redo the above argument, but interchange the role of p's and q's. Thus by symmetry reasoning, we also have $r \leq N$, $q_1 = p_1, \ldots, q_r = p_r$; moreover $\ell_1 \geq k_1, \ldots, \ell_r \geq k_r$. Therefore, $r = N$ and $p_1 = q_1, \ldots, p_N = q_N$ and $\ell_1 = k_1, \ldots, \ell_N = k_N$, and we're done.

Consequence 1: There are infinitely many prime numbers.

Reason: Suppose to the contrary that there are only finitely many primes, say the $\{p_1 \ldots p_m\}$ = all the prime numbers. Let $N = 1 + (p_1 \cdots p_m) \in \mathbf{N}$. Then $N \geq 2$. By the Fundamental Theorem of Arithmetic, we can write

$$N = p_1^{\ell_1} \cdots p_m^{\ell_m}, \quad \text{where } \ell_1, \ldots, \ell_m \geq 0, \text{ and } \ell_{j_0} \geq 1 \text{ for some } j_0 \in \{1, \ldots, m\}.$$

Thus $p_{j_0}|N$ and further, $p_{j_0}|(p_1 \cdots p_m)$. Hence $p_{j_0}|\big(N - (p_1 \cdots p_n)\big)$, i.e. $p_{j_0}|1$, which is impossible. Thus there can only be finitely many primes.

Consequence 2: Let $p \in \mathbf{N}$ be a prime number. Then $\sqrt{p} \notin \mathbf{Q}$.

Reason: Lets assume to the contrary that $\sqrt{p} = a/b \in \mathbf{Q}$, where $a, b \in \mathbf{N}$. If we set $d = (a, b)$ and write $a = da_1,\ b = db_1$, then

$$\frac{a}{b} = \frac{da_1}{db_1} = \frac{a_1}{b_1}, \quad \text{where} \quad (a_1, b_1) = 1.$$

Hence we may assume that $(a, b) = 1$, i.e. a/b is a fraction in reduced form. Thus:

$$\sqrt{p} = \frac{a}{b} \Rightarrow b\sqrt{p} = a \Rightarrow b^2 p = a^2.$$

Therefore

$$p|(b^2p) \Rightarrow p|a^2 \quad \overset{p \text{ prime}}{\Rightarrow} \quad p|a \Rightarrow pe = a, \text{ for some } e \in \mathbf{N}.$$

This implies that

$$b^2p = a^2 = p^2e^2, \quad \text{hence} \quad b^2 = pe^2 \Rightarrow p|b^2 \quad \overset{p \text{ prime}}{\Rightarrow} \quad p|b.$$

We deduce that $p|a$ & $p|b$, hence $(a,b) \geq p > 1$, a contradiction to our assumption that $(a,b) = 1$. Therefore $\sqrt{p} \notin \mathbf{Q}$.

Computing GCD's via Prime Decomposition

Observation. Assume given $d, n \in \mathbf{N}$ such that $d|n$. Then the prime decomposition of d forms part of the prime decomposition of n. This is because $de = n$ for some $e \in \mathbf{N}$, and that:

$$\big[\text{Prime Decomposition of } d\big] \cdot \big[\text{Prime Decomposition of } e\big] \;=\; \big[\text{Prime Decomposition of } n\big];$$

using the uniquess part of the Fundamental Theorem of Arithmetic.

Now let $n, m \in \mathbf{N}$, and $d = (m,n)$. Write:

$$n = p_1^{\ell_1} \cdots p_N^{\ell_N},$$

$$m = p_1^{k_1} \cdots p_N^{k_N},$$

where $\ell_1, \ldots, \ell_N, k_1, \ldots, k_N \geq 0$, and $\{p_1, \ldots, p_N\}$ are distinct primes.

Example. $\begin{array}{rcl} 6 & = & 2^1 \times 3^1 \times 5^0 \\ 30 & = & 2^1 \times 3^1 \times 5^1 \end{array}$

Choose $r_i = \min\{\ell_i, k_i\}$, $i = 1, \ldots, N$. Then clearly

$$d = p_1^{r_1} \cdots p_N^{r_N}.$$

Example. GCD$(27, 33) =$? Solution: $\begin{array}{rcl} 33 & = & 3^1 \times 11^1 \\ 27 & = & 3^3 \times 11^0 \end{array}$. Thus $d = 3^1 \times 11^0 = 3$.

Least Common Multiples

Definition. Let $m, n \in \mathbf{Z}$, $m, n \neq 0$, be given. The Least Common Multiple of m & n, denoted by LCM(m,n) or $[m,n]$, is an integer $\ell \in \mathbf{N}$ satisfying:

1) $n|\ell$ and $m|\ell$.

2) If, for $k \in \mathbf{Z}$, $n|k$ and $m|k$, then $\ell|k$.

Remarks. (1) As in the case of GCD's, the LCM is unique, i.e. there is only 1 LCM(m, n).

(2) The existence of LCM(m, n) is as follows:

$$n = p_1^{\ell_1} \cdots p_N^{\ell_N},$$

$$m = p_1^{k_1} \cdots p_N^{k_N},$$

then if we set $t_i = \max\{\ell_i, k_i\}$, $i = 1, \ldots, N$, we have:

$$\ell := [m, n] = p_1^{t_1} \cdots p_N^{t_N}.$$

Claim.

$$[m, n] = \frac{m \cdot n}{(m, n)}.$$

Reason: It is obvious that

$$m \cdot n = p_1^{\ell_1 + k_1} \cdots p_N^{\ell_N + k_N},$$

and that:

$$\ell_i + k_i = \min\{\ell_i, k_i\} + \max\{\ell_i, k_i\} = r_i + t_i.$$

Therefore:

$$m \cdot n = \left(p_1^{r_1} \cdots p_N^{r_N}\right)\left(p_1^{t_1} \cdots p_N^{t_N}\right) = (m, n)[m, n].$$

Example. $(27, 33) = 3$, hence

$$[27, 33] = \frac{27 \times 33}{3} = 9 \times 33 = 297.$$

Equivalence relations

As for motivation, we mention three essential properties of equality "=" on a given set X.

1) [Reflexivity] $x = x$, for any $x \in X$.

2) [Symmetry] $x = y \Rightarrow y = x$, for $x, y, \in X$.

3) [Transitivity] $x = y \ \& \ y = z \Rightarrow x = z$, for $x, y, z \in X$.

Notation: For a given set X, set $X \times X = \{(x, y) \mid x, y \in X\}$.

Definition. A relation $\mathcal{R}$ on a set X is given by a subset $S_{\mathcal{R}} \subset X \times X$. We say that x is related to y via $\mathcal{R}$, and write $x\mathcal{R}y$, if $(x, y) \in S_{\mathcal{R}}$.

Example. If $\mathcal{R}$ is equality"=", then

$$S_{\mathcal{R}} = \{(x, y) \in X \times X \mid x = y\} = \{(x, x) \in X \times X \mid x \in X\}.$$

Note that $x\mathcal{R}y$ means $(x, y) \in S_{\mathcal{R}}$, i.e. means that $x = y$. Thus equality "=" is an example of a relation.

Definition. Let X be a set, and $\mathcal{R}$ a relation on X, defined by a subset $S_{\mathcal{R}} \subset X \times X$. Then $\mathcal{R}$ is called an <u>equivalence relation</u> on X if the following three properties hold:

1) [Reflexivity] $x\mathcal{R}x$. [Equivalently, $\{(x, x) \mid x \in X\} \subset S_{\mathcal{R}}$.]

2) [Symmetry] $x\mathcal{R}y \Rightarrow y\mathcal{R}x$. [Equivalently, $(x, y) \in S_{\mathcal{R}} \Rightarrow (y, x) \in S_{\mathcal{R}}$.]

3) [Transitivity] $x\mathcal{R}y \ \& \ y\mathcal{R}z \ \Rightarrow \ x\mathcal{R}z$. [Equivalently, $(x, y) \in S_{\mathcal{R}} \ \& \ (y, z) \in S_{\mathcal{R}} \ \Rightarrow (x, z) \in S_{\mathcal{R}}$.]

Notation: If $\mathcal{R}$ is an equivalence relation on a set X, we usually write "$\sim$", instead of $\mathcal{R}$. Thus, for $x, y, z \in X$:

1) [Reflexivity] $x \sim x$.

2) [Symmetry] $x \sim y \Rightarrow y \sim x$.

3) [Transitivity] $x \sim y \ \& \ y \sim z \ \Rightarrow \ x \sim z$.

Ex. The relation $\mathcal{R}$ given by equality "=", is an equivalence relation.

Ex. Let $X =$ class of Math 228 students. We write, for students $x, y \in X$, $x \sim y$ if x and y have the same sex. It is reasonably clear that $\sim$ is an equivalence relation.

Ex. Let $X = \mathbf{R}$, and consider the relation $\mathcal{R}$ on $\mathbf{R}$ given by: $x\mathcal{R}y \Leftrightarrow x \leq y$. Then $x \leq x$, hence reflexivity holds. Also $x \leq y \ \& \ y \leq z \ \Rightarrow \ x \leq z$, hence transitivity holds.

But $x \leq y \not\Rightarrow y \leq x$. Thus symmetry *fails.* Therefore $\mathcal{R}$ is not an equivalence relation on $\mathbf{R}$.

Further Notation: Let A and B be subsets of some bigger set. If $A \cap B = \emptyset$, we write $A \cup B = A \coprod B$ (i.e. disjoint union).

Key Example. Let X be a set. A partitioning of X is by definition a given disjoint union.

$$X = \coprod_{\underbrace{\alpha \in I}_{I=\text{some index set}}} X_\alpha \quad \leftarrow \quad \begin{array}{c}\text{also called a coset} \\ \text{decomposition; } X_\alpha = \text{ a coset}\end{array}$$

We define an equivalence relation $\mathcal{R} =$ "$\sim$" on X as follows: $x \sim y \Leftrightarrow x, y \in X_\alpha$, i.e. x and y belong to the same X_α. [Details: $x, x \in X_\alpha \Rightarrow x \sim x$; $x \sim y \Leftrightarrow x, y \in X_\alpha \Leftrightarrow y, x \in X_\alpha \Leftrightarrow y \sim x$; $x \sim y$ & $y \sim z$ means that $x, y, z \in X_\alpha \Rightarrow x \sim z$. Also, it is easy to see that the subset defining the relation $\mathcal{R}$ is given $S_\mathcal{R} = \coprod_{\alpha \in I} X_\alpha \times X_\alpha$.]

Ex. A

$$\underbrace{\{1,2,3,4\}}_{X} = \underbrace{\{1,2\}}_{X_{\alpha_1}} \coprod \underbrace{\{3\}}_{X_{\alpha_2}} \coprod \underbrace{\{4\}}_{X_{\alpha_3}}$$

So for example, if we write $\sim$ to mean "equivalent to", and $\not\sim$ to mean "not equivalent to", then:

$$\begin{array}{llll} 1 \sim 1 & 2 \sim 2 & 3 \sim 3 & 4 \sim 4 \\ 1 \sim 2 & 1 \not\sim 3 & 1 \not\sim 4 & 2 \not\sim 3 \\ 2 \not\sim 4 & 3 \not\sim 4 & & \end{array}$$

Ex. B Let $\mathcal{H}$ be the human race. Thus $x \in \mathcal{H}$ means that x is a human being. For $x, y \in \mathcal{H}$, we define a relation on $\mathcal{H}$ as follows: We write $x\mathcal{R}y$ if x and y are friends. It is reasonably clear that $x\mathcal{R}x$, i.e. evey human being is a friend of his(her)self, and that $x\mathcal{R}y \Rightarrow y\mathcal{R}x$. However it is not the case that if $x\mathcal{R}y$ and $y\mathcal{R}z$, then $x\mathcal{R}z$, i.e. just because x and y are friends, and y and z are friends, does not mean that x and z are friends. Thus even though $\mathcal{R}$ is reflexive and symmetric, the transitivity property fails, and hence $\mathcal{R}$ is not an equivalence relation on $\mathcal{H}$.

Claim. All equivalence relations are given by the Key Example.

Reason: Let X be a set with a given equivalence relation $\sim$. We want to show that $\sim$ comes from a given partition of X. We begin with the following notation. For $x \in X$, we put

$$X_x = \{y \in X \mid y \sim x\}.$$

Since $x \sim x$ it follows that $x \in X_x$, hence

$$X = \bigcup_{x \in X} X_x.$$

To arrive at a partition, viz. disjoint union ($\coprod$), we need the following Observation, for any given $x_1, x_2 \in X$, namely:

$$\textit{Either: } X_{x_1} = X_{x_2}, \text{ (in which case } x_1 \sim x_2),$$
$$\textit{or: } X_{x_1} \cap X_{x_2} = \emptyset, \text{ (in which case } x_1 \not\sim x_2).$$

If we assume the observation for now, then by "throwing away repeats", we arrive at a partition:

$$X = \coprod_{\underbrace{x_\alpha \in I}_{(I = \text{ some subset} \subset X)}} X_{x_\alpha};$$

moreover it is easy to see that $\sim$ comes from this partition. Next, we explain why the Observation above holds: If $X_{x_1} \cap X_{x_2} \neq \emptyset$, then choose $y \in X_{x_1} \cap X_{x_2}$. Then $x_1 \sim y$ and $y \sim x_2$, hence $x_1 \sim x_2$. Further, if $z \in X_{x_1}$, then $z \sim x_1$ and $x_1 \sim x_2 \Rightarrow z \sim x_2$, i.e. $z \in X_{x_2}$. Thus $X_{x_1} \subset X_{x_2}$, and by similar reasoning (symmetry), it follows that $X_{x_2} \subset X_{x_1}$. Thus $X_{x_1} = X_{x_2}$. It is now easy to deduce the observation from this.

Ex. C Let $X = \mathbf{Z}$, and for $n, m \in \mathbf{Z}$, we write $n \sim m$ to mean that $2|(n-m)$, i.e. $n - m$ is even. Note that there is a natural partition of $\mathbf{Z}$, namely:

$$\mathbf{Z} = \{\text{Even Integers}\} \quad \coprod \quad \{\text{Odd Integers}\};$$

moreover $n \sim m$ is equivalent to saying that n and m are either *both even* or *both odd.* Thus $\sim$ is the equivalence relation defined by this partition of $\mathbf{Z}$.

$\star\star\star$ Main Example $\star\star\star$

Fix $n \in \mathbf{N}$, $n \geq 2$. Define a relation $\sim$ on $\mathbf{Z}$ as follows: For $x, y \in \mathbf{Z}$, we write $x \sim y$ to mean $n|(x-y)$.

Claim. $\sim$ is an equivalence relation on $\mathbf{Z}$.

Reason:

1) [Reflexivity] $x - x = 0 = 0 \cdot n$. Thus $n|(x-x)$, hence $x \sim x$.

2) [Symmetry] $x \sim y \Rightarrow n|(x-y)$ hence $qn = x-y$, for some $q \in \mathbf{Z}$. Thus $(-q)n = y-x$, i.e. $n|(y-x)$. Hence $y \sim x$.

3) [Transitivity] $x \sim y$ & $y \sim z$. Therefore $n|(x-y)$ & $n|(y-z)$, i.e. $qn = x-y$ & $kn = y-z$ for some $q, k \in \mathbf{Z}$. Thus $x - z = (x-y) + (y-z) = qn + kn = (q+k)n$. Thus $n|(x-z)$, and hence $x \sim z$.

Continuing with this main example, we introduce "the integers modulo n", denote by:

$$\mathbf{Z}_n \stackrel{\text{def}}{=} \{\text{equivalence classes } \overline{x} \mid x \in \mathbf{Z}\},$$

i.e. where we write $\overline{x} = \overline{y}$ to mean $x \sim y$, i.e. $n|(x-y)$.

Question. What does $\mathbf{Z}_n$ look like?

Answer. For every $x \in \mathbf{Z}$, and by Euclid's Division Algorithm, we have $x = qn + r$ where $0 \leq r < n$, and $q \in \mathbf{Z}$. Thus

$$x - r = qn \Rightarrow n|(x-r).$$

i.e. $x \sim r$, i.e. $\overline{x} = \overline{r}$. Thus

$$\mathbf{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

For example $n|n \Rightarrow \overline{n} = \overline{0}$, and $n|\big((n+1)-1\big) \Rightarrow \overline{n+1} = \overline{1}$.

In terms of coset decomposition

$$\mathbf{Z} \quad = \quad \underbrace{\{n\mathbf{Z}+0\}}_{\overline{0}} \coprod \underbrace{\{n\mathbf{Z}+1\}}_{\overline{1}} \coprod \cdots \coprod \underbrace{\{n\mathbf{Z}+(n-1)\}}_{\overline{n-1}},$$

where $n\mathbf{Z} + r := \{qn + r \mid q \in \mathbf{Z}\}$. Note that there is a natural map:

$$\begin{array}{ccc} \mathbf{Z} & \to & \mathbf{Z}_n \\ x & \mapsto & \overline{x} \end{array}$$

and diagram

$$\begin{array}{ccc} \mathbf{Z} \times \mathbf{Z} & \stackrel{+,\bullet}{\longrightarrow} & \mathbf{Z} \\ \downarrow & & \downarrow \\ \mathbf{Z}_n \times \mathbf{Z}_n & \stackrel{+,\bullet}{\longrightarrow} & \mathbf{Z}_n \end{array}$$

In other words, we claim that there is induced $+, \bullet$ on $\mathbf{Z}_n$.

Preliminary Definition.

1) $\overline{x} + \overline{y} \stackrel{\text{def}}{=} \overline{x+y}$.

2) $\overline{x} \overline{y} \stackrel{\text{def}}{=} \overline{xy}$.

Claim. $+, \bullet$ on $\mathbf{Z}_n$ are well-defined operations.

Restatement: If $x \sim x_1$ & $y \sim y_1$, then $x + y \sim x_1 + y_1$, and $xy \sim x_1 y_1$. Equivalently, if $\overline{x} = \overline{x}_1$ and $\overline{y} = \overline{y}_1$, then $\overline{x+y} = \overline{x_1 + y_1}$, and $\overline{xy} = \overline{x_1 y_1}$.

Details: $\overline{x} = \overline{x}_1 \Leftrightarrow x = x_1 + qn$, and $\overline{y} = \overline{y}_1 \Leftrightarrow y = y_1 + kn$, for some $q, k \in \mathbf{Z}$. Thus $x + y = x_1 + y_1 + (q+k)n$, and $xy = x_1 y_1 + x_1 kn + y_1 qn + qkn^2$, i.e. $xy = x_1 y_1 + (x_1 k + y_1 q + qkn)n$. Thus $\overline{x+y} = \overline{x_1 + y_1}$, and $\overline{xy} = \overline{x_1 y_1}$.

Claim. $[\mathbf{Z}_n; +, \bullet]$ is a ring with unity.

Reason:

$$\overline{0}+\overline{x}=\overline{0+x}=\overline{x} \quad ; \quad \overline{1}\cdot\overline{x}=\overline{1\cdot x}=\overline{x}.$$

Thus $\overline{0}$ is the zero element and $\overline{1}$ is the unity. Next, the commutative, distributive, and associative laws on $\mathbf{Z}$ descend to the same laws on $\mathbf{Z}_n$. This follows from the fact that $+, \bullet$ on $\mathbf{Z}_n$ are induced from $+, \bullet$ on $\mathbf{Z}$. Finally, $\overline{x}+\overline{(-x)}=\overline{0} \Rightarrow$ we have additive inverses. Thus $[\mathbf{Z}_n; +, \bullet]$ satisfies the properties that define a ring with unity.

Examples of $\mathbf{Z}_n$

Ex. $\mathbf{Z}_2=\{\overline{0},\overline{1}\}$.

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\bullet$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

For example, $-\overline{1}=\overline{1}$. Since $\overline{1}$ is the only non-zero element, and $\overline{1}\neq\overline{0}$, it is clear that $\mathbf{Z}_2$ is a field. This example was studied earlier.

Ex. $\mathbf{Z}_3=\{\overline{0},\overline{1},\overline{2}\}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

For example, $-\overline{1}=\overline{2}$, $-\overline{2}=\overline{1}$. Now since $\overline{2}^{-1}=\overline{2}$, hence all non-zero elements have multiplicative inverses, it follows that $\mathbf{Z}_3$ is a field. This example was studied earlier as well.

Ex. $\mathbf{Z}_4=\{\overline{0},\overline{1},\overline{2},\overline{3}\}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Note that the group of units is given by $\mathbf{Z}_4^* = \{\overline{1}, \overline{3}\}$. For example $\overline{3}^{-1} = \overline{3}$. However $\overline{2}$ is not a unit, by the multiplication table. In fact $\overline{2} \cdot \overline{2} = \overline{0}$. The element $\overline{2}$ is an example of a zero divisor (or "divisor of zero"). Clearly $\mathbf{Z}_4$ is *not* a field.

Ex. $\mathbf{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

For example $-\overline{1} = \overline{4},\ -\overline{2} = \overline{3},\ -\overline{3} = \overline{2},\ -\overline{4} = \overline{1}$. Also $\overline{2}^{-1} = \overline{3},\ \overline{3}^{-1} = \overline{2},\ \overline{4}^{-1} = \overline{4}$. Thus it is easy to see that $\mathbf{Z}_5$ is a field.

Ex. $\mathbf{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Note that from the $\bullet$ table, that we have $\mathbf{Z}_6^* = \{\overline{1}, \overline{5}\}$, (here $\overline{5}^{-1} = \overline{5}$). Also, $\overline{3}\cdot\overline{4} = \overline{0}$, $\overline{3}\cdot\overline{2} = \overline{0}$. Thus $\{\overline{2}, \overline{3}, \overline{4}\}$ are examples of zero divisors. It is obvious that $\mathbf{Z}_6$ is *not* a field.

Examples $\mathbf{Z}_4$ and $\mathbf{Z}_6$ provide motivation for the following definition,

Definition. Let $\mathbf{A}$ be a ring with unity $1 \neq 0$. A zero divisor is an element $x \in \mathbf{A}$ with the property that $xy = 0$ for some $y \in \mathbf{A}$, $y \neq 0$. [Note: $0 \in \mathbf{A}$ is a zero divisor since $1 \cdot 0 = 0$.]

Ex. The zero divisors in $\mathbf{Z}_4$ are $\{\overline{0}, \overline{2}\}$. [Furthermore, the units are $\{\overline{1}, \overline{3}\}$, hence $\mathbf{Z}_4 =$ {Units} $\coprod$ {Zero Divisors}.]

Ex. The zero divisors in $\mathbf{Z}_6$ are $\{\overline{0}, \overline{2}, \overline{3}, \overline{4}\}$. [Furthermore, the units are $\{\overline{1}, \overline{5}\}$, hence $\mathbf{Z}_6 =$ {Units} $\coprod$ {Zero Divisors}.]

Important Remark. Let $\mathbf{A}$ be a ring with unity $1 \neq 0$. Then a unit can *never* be a zero divisor. For if $x \in \mathbf{A}^*$ is a unit, and if $y \in \mathbf{A}$ is given such that $xy = 0$, then $0 = x^{-1}0 = x^{-1}xy = y$. Thus $xy \neq 0$ for any $y \in \mathbf{A}$ with $y \neq 0$.

Definition. Let $\mathbf{A}$ be a ring with unity $1 \neq 0$. Then $\mathbf{A}$ is called an integral domain if $\mathbf{A}$ has no non-zero zero divisors. [Restatement: If $\mathbf{A}$ is a ring with unity $1 \neq 0$, then $\mathbf{A}$ is an integral domain $\Leftrightarrow \big[\{xy = 0\} \Rightarrow \{x = 0 \text{ or } y = 0, \text{ for any } x, y \in \mathbf{A}\}\big]$.]

Remarks and Examples. (i) $\mathbf{Z}$ is an integral domain.

(ii) Any field $\mathbf{F}$ is an integral domain. For if $x \in \mathbf{F}$ is non-zero, then x is a unit, hence not a zero divisor. [Hence $\mathbf{Z}_2$, $\mathbf{Z}_3$, $\mathbf{Z}_5$, being fields, are integral domains.]

(iii) We will eventually show that $\mathbf{Z}_n =$ {Zero Divisors} $\coprod$ {Units}, as can be easily verified in the cases $n = 2, 3, 4, 5, 6$. This is not the case for general rings, such as the integers $\mathbf{Z}$!

Now recall that the group of units in $\mathbf{Z}_n$ is denoted by $\mathbf{Z}_n^*$. Also recall that for $n, m \in \mathbf{N}$, n, m are relatively prime if $(n, m) := \text{GCD}(n, m) = 1$.

Claim. $\mathbf{Z}_n^* = \{\overline{x} \mid (x, n) = 1\}$.

Ex. Suppose $n = p$ is prime. Then $\mathbf{Z}_p^* = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$ = the non-zero elements of $\mathbf{Z}_p$. Thus $\mathbf{Z}_p$ is a field.

Ex. $\mathbf{Z}_4^* = \{\overline{1}, \overline{3}\}$. [Using $(1, 4) = (3, 4) = 1$, $(2, 4) = 2$.]

Ex. $\mathbf{Z}_6^* = \{\overline{1}, \overline{5}\}$. [Using $(1, 6) = (5, 6) = 1$, $(2, 6) = 2$, $(3, 6) = 3$, $(4, 6) = 2$.]

Reason for the Claim: Suppose that $(x, n) = 1$. Then $1 = ax + bn$ for some $a, b \in \mathbf{Z}$. Thus:

$$\overline{1} = \overline{ax + bn} = \overline{ax} + \underbrace{\overline{b}\overline{n}}_{=\overline{0}} = \overline{a} \cdot \overline{x}, \quad \text{i.e. } \overline{1} = \overline{a} \cdot \overline{x},$$

hence $\overline{x}$ is a unit, i.e. $\overline{x} \in \mathbf{Z}_n^*$. [In this case $\overline{a} = \overline{x}^{-1}$.] Conversely, suppose that $\overline{x} \in \mathbf{Z}_n^*$, i.e. $\overline{x} \cdot \overline{y} = \overline{1}$, for some $\overline{y} \in \mathbf{Z}_n$. Thus

$$\overline{xy - 1} = \overline{x} \cdot \overline{y} - \overline{1} = \overline{0}, \quad \text{i.e. } n|(xy - 1).$$

Hence $xy - 1 = qn$ for some $q \in \mathbf{Z}$, or equivalently, $xy + (-q)n = 1$. Now let $d = (x, n)$. then $d|x$ and $d|n$. Therefore $d|\big(xy + (-q)n\big)$, i.e. $d|1$. Thus since $d \in \mathbf{N}$, it follows that $d = 1$. In other words, $(x, n) = 1$, and the claim is proven.

Claim.

$$\mathbf{Z}_n = \mathbf{Z}_n^* \coprod \{\text{Zero Divisors}\}.$$

Reason: Let $\overline{x} \in \mathbf{Z}_n$ be given, with $\overline{x} \notin \mathbf{Z}_n^*$, and further let $d = (x, n)$. Then we know by the above claim that $d \geq 2$. So write $x = ud$ and $n = vd$, and note that $1 \leq v < n$, since $d \geq 2$. Therefore $\overline{v} \neq \overline{0}$, and yet

$$\overline{v} \cdot \overline{x} = \overline{vx} = \overline{uvd} = \overline{u} \cdot \overline{n} = \overline{0}.$$

Hence $\overline{x}$ is a zero divisor.

Ex. $\overline{4} \in \mathbf{Z}_6$ is a zero divisor, since $(4, 6) = 2 > 1$. Note that $6 = v \cdot d$, where $v = 3$ and $d = 2$ as in the above discussion (and where $\overline{x} = \overline{4}$, $n = 6$). According to the above discussion $\overline{v} \cdot \overline{x} = \overline{0}$. This is the same as $\overline{3} \cdot \overline{4} = \overline{12} = \overline{2} \cdot \overline{6} = \overline{0}$, which is obvious!

Claim. The following statements are equivalent, for $n \in \mathbf{N}$, $n \geq 2$:

1) $\mathbf{Z}_n$ is a field.

2) $\mathbf{Z}_n$ is an integral domain.

3) $n = p$ is prime.

Reason: The basic idea is this. If $n = p$ is prime, then we learned that $\mathbf{Z}_p$ is a field, hence an integral domain. However, if n is not prime, then $n = a \cdot b$, where $1 < a < n$, $1 < b < n$. Thus $\overline{a}\overline{b} = \overline{n} = \overline{0}$ and yet $\overline{a}, \overline{b} \neq \overline{0}$. Thus $\mathbf{Z}_n$ has non-zero zero divisors (which cannot be units), hence is neither a field, nor an integral domain.

Ex. Find the units and zero divisors of $\mathbf{Z}_{12}$. Solution: $\mathbf{Z}_{12}^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$. The zero divisors are the remaining elements in $\mathbf{Z}_{12}$, namely $\{\overline{0}, \overline{2}, \overline{3}, \overline{4}, \overline{6}, \overline{8}, \overline{9}, \overline{10}\}$.

Ex. Find the multiplicatve inverse of $\overline{3}$ in $\mathbf{Z}_{17}$. [Note: Observe that $\mathbf{Z}_{17}$ is a field, since 17 is prime. Thus $\overline{3}^{-1}$ can be found in $\mathbf{Z}_{17}$.] Solution: Since $(3, 17) = 1$, it follows that $1 = 3x + 17y$ for some $x, y \in \mathbf{Z}$. Therefore modulo 17, we have $\overline{1} = \overline{3}\overline{x} + \overline{17}\overline{y} = \overline{3}\overline{x}$. Hence $\overline{x} = \overline{3}^{-1}$. Therefore we are done if we know x. But we learned how to solve for x and y earlier, by back substitution. First of all, by Euclid's Division:

$$17 = 5 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

Thus by back substitution we have:

$$1 = 3 - 1 \times \big[2 = 17 - 5 \times 3\big] = 6 \cdot 3 - 17, \quad x = 6,\ y = -1.$$

In particular, $\overline{3}^{-1} = \overline{6}$.

Examples of Subrings of $\mathbf{Z}_n$

Ex. $2\mathbf{Z}_6 \stackrel{\text{def}}{=} \{\overline{2} \cdot \overline{0}, \overline{2} \cdot \overline{1}, \overline{2} \cdot \overline{2}, \overline{2} \cdot \overline{3}, \overline{2} \cdot \overline{4}, \overline{2} \cdot \overline{5}\} = \{\overline{0}, \overline{2}, \overline{4}\}$. The corrsponding $+, \bullet$ tables are:

$+$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{0}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{2}$

$\bullet$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$

The tables imply that $2\mathbf{Z}_6$ is closed under $+, \bullet$ from $\mathbf{Z}_6$, and that there is a zero element and additive inverses. Further $\overline{4}$ is the unity $\neq \overline{0}$, and $\overline{2}^{-1} = \overline{2}$. It follows that $2\mathbf{Z}_6$ is a subring of $\mathbf{Z}_6$; moreover $2\mathbf{Z}_6$ is a field, even though $\mathbf{Z}_6$ isn't!

Ex. $4\mathbf{Z}_8 = \{\overline{0}, \overline{4}\}$ is a subring of $\mathbf{Z}_8$, as one can deduce from the $+, \bullet$ tables below:

$+$	$\overline{0}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{4}$
$\overline{4}$	$\overline{4}$	$\overline{0}$

$\bullet$	$\overline{0}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{4}$	$\overline{0}$	$\overline{0}$

Note that there is no unity, hence $4\mathbf{Z}_8$ is not a field. In fact, all the elements $\{\overline{0}, \overline{4}\}$ of $4\mathbf{Z}_8$ are zero divisors!

Ex. $5\mathbf{Z}_{10} = \{\overline{0}, \overline{5}\}$, with corresponding tables below, is a subring of $\mathbf{Z}_{10}$.

$+$	$\overline{0}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{0}$

$\bullet$	$\overline{0}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{5}$	$\overline{0}$	$\overline{5}$

It is easy to see that $\overline{5}$ is the unity, and that $5\mathbf{Z}_{10}$ is a field, even though $\mathbf{Z}_{10}$ is not a field. Note that one can form a dictionary between the two fields:

$$5\mathbf{Z}_{10} = \{\overline{0}, \overline{5}\} \quad \leftrightarrow \quad \{\overline{0}, \overline{1}\} = \mathbf{Z}_2.$$

Such dictionaries will be explored in more detail later.

We recall that any field is an integral domain; however the converse statement is *false.* There are examples of integral domains that are not fields. [Take the ring of integers $\mathbf{Z}$, for example.] However, for $\mathbf{Z}_n$, we recall that $\mathbf{Z}_n$ is a field $\Leftrightarrow$ $\mathbf{Z}_n$ is an integral domain. Furthermore, as a set, $\mathbf{Z}_n$ is finite. This leads us to the following partial converse result:

Claim. Any *finite* integral domain is a field. [Restatement: Let $\mathbf{A}$ be an integral domain, and assume that $\mathbf{A}$ is finite. Let $x \in \mathbf{A}$, $x \neq 0$ be given. Then there is an element $y \in \mathbf{A}$ such that $xy = 1 \in \mathbf{A}$.]

Reason: Let $x \in \mathbf{A}$, $x \neq 0$ be given, and consider the subset $\Sigma \subset \mathbf{A}$ given by

$$\Sigma := \{x^n \mid n \in \mathbf{N}\} = \{x = x^1, x^2, x^3, \ldots\}.$$

Since $\mathbf{A}$, and hence also Σ, is finite, we must have repeats in the powers $\{x^n\}_{n\in\mathbf{N}}$. In other words, for some $k, m \in \mathbf{N}$ with $k > m$, $x^m = x^k$. Therefore $x^m(x^{k-m} - 1) = x^k - x^m = 0$. Since $x \neq 0$ and $\mathbf{A}$ is an integral domain, $x^m \neq 0$ and therefore $x^{k-m} - 1 = 0$, or $x^{k-m} = 1$. Note that $k - m \in \mathbf{N}$. If $k - m = 1$, then $x = 1$, and hence $y := x^{-1} = 1 \in \mathbf{A}$. If $k - m \geq 2$, then $k - m - 1 \in \mathbf{N}$ and $x \cdot x^{k-m-1} = x^{k-m} = 1$. Thus $y := x^{-1} = x^{k-m-1} \in \mathbf{A}$, and we are done.

We want to impress upon the reader the relationship between the three fundamental areas below.

We will study the relationship of Algebra to Geometry later on. For the time being, we will consider an application of Algebra to Number Theory.

The Euler Phi Function

Definition. The Euler Phi function is a map $\varphi : \mathbf{N} \to \mathbf{N}$ given by the prescription:

$$\varphi(n) = {}^{\#}\big\{m \in \mathbf{N} \;\big|\; 1 \leq m \leq n \;\&\; (m,n) = 1\big\}.$$

Note that $\varphi(1) = 1$. The connection between this map and ring theory is given by the following observation:

Observation: For $n \in \mathbf{N}$, $n \geq 2$, we have $\varphi(n) = {}^{\#}\mathbf{Z}_n^*$.

Ex. If $p \in \mathbf{N}$ is prime, then $\varphi(p) = {}^{\#}\mathbf{Z}_p^* = {}^{\#}\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\} = p - 1$.

Ex. $\varphi(4) = \varphi(2^2) = {}^{\#}\mathbf{Z}_4^* = {}^{\#}\{\overline{1}, \overline{3}\} = 2 = 2^2 - 2^1$.

Ex. $\varphi(6) = \varphi(2 \cdot 3) = {}^{\#}\mathbf{Z}_6^* = {}^{\#}\{\overline{1}, \overline{5}\} = 2 = \varphi(2) \cdot \varphi(3)$.

Ex. $\varphi(8) = \varphi(2^3) = {}^{\#}\mathbf{Z}_8^* = {}^{\#}\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\} = 4 = 2^3 - 2^2$.

The essential properties of this map φ follow from the two claims below.

Claim 1. Let $m, n \in \mathbf{N}$. If $(m,n) = 1$, then $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Claim 2. If $p \in \mathbf{N}$ is prime, and if $m \in \mathbf{N}$ is given, then $\varphi(p^m) = p^m - p^{m-1}$. [For example, if $m = 1$, then $\varphi(p) = \varphi(p^1) = p^1 - p^0 = p - 1$.]

We will postpone the reason for the claims for now, by first showing how these two claims allow us to "compute" $\varphi(n)$ for any $n \in \mathbf{N}$. To do this, for $n \geq 2$, write $n = p_1^{\ell_1} \cdots p_N^{\ell_N}$, where $\{p_1, \ldots, p_N\}$ are distinct primes and $\ell_1, \ldots, \ell_N \in \mathbf{N}$. Then by applying the two claims repeatedly, we arrive at:

$$\varphi(n) = \varphi(p_1^{\ell_1}) \cdots \varphi(p_N^{\ell_N}) = \big(p_1^{\ell_1} - p_1^{\ell_1 - 1}\big) \cdots \big(p_N^{\ell_N} - p_N^{\ell_N - 1}\big).$$

Ex. $\varphi(28) = \varphi(2^2 \cdot 7) = \varphi(2^2) \cdot \varphi(7) = \big(2^2 - 2^1\big) \cdot (7 - 1) = 12$.

Proof of Claim 1 (Outline only)

Let $m, n \in \mathbf{N}$ be integers ≥ 2, and consider

$$\mathbf{Z}_m \times \mathbf{Z}_n := \{(\overline{x}, \overline{y}) \mid \overline{x} \in \mathbf{Z}_m,\ \overline{y} \in \mathbf{Z}_n\}.$$

We want to compare the product ring $\mathbf{Z}_m \times \mathbf{Z}_n$, (where $\mathbf{Z}_m \times \mathbf{Z}_n$ has componentwise $+$ and $\bullet$[†]), to $\mathbf{Z}_{mn}$. The following notation seems useful. Let $z \in \mathbf{Z}$ be given. We write $\overline{z}_n$ to mean z modulo n, i.e. $\overline{z}_n = \overline{z} \in \mathbf{Z}_n$, i.e. as an element of the ring $\mathbf{Z}_n$. We construct a map $\Phi : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by the formula $\Phi(\overline{z}_{mn}) = (\overline{z}_m, \overline{z}_n)$. Note that Φ is well-defined, for if $\overline{w}_{mn} = \overline{z}_{mn}$, then $(mn)|(w-z)$, hence $m|(w-z)$ and $n|(w-z)$. Thus $\Phi(\overline{w}_{mn}) = (\overline{w}_m, \overline{w}_n) = (\overline{z}_m, \overline{z}_n) = \Phi(\overline{z}_{mn})$. As an example calculation, if e.g. $m = 3$ and $n = 2$, then $\Phi(\overline{5}_6) = (\overline{5}_3, \overline{5}_2) = (\overline{2}_3, \overline{1}_2)$. Note that $\mathbf{Z}_{mn}$ and $\mathbf{Z}_m \times \mathbf{Z}_n$ contain the same number of elements, namely mn. The map Φ has the nice property that it preserves ring structures and unity, namely Φ takes $(+, \bullet)$ to $(+, \bullet)$ and $\Phi(\overline{1}_{mn}) = (\overline{1}_m, \overline{1}_n)$. Φ is an example of a ring homomorphism, that which will be discussed later on. Next, if $\Phi(\overline{z}_{mn}) = (\overline{0}_m, \overline{0}_n)$, then $m|z$ and $n|z$; moreover, by the Fundamental Theorem of Arithmetic, if $(m, n) = 1$, then $(mn)|z$, hence $\overline{z}_{mn} = \overline{0}_{mn}$. From here, it is easy to deduce that Φ is one-to-one, in the case $(m, n) = 1$. Since $\mathbf{Z}_{mn}$ and $\mathbf{Z}_m \times \mathbf{Z}_n$ have the same number of elements, this translates to saying that in the case where $(m, n) = 1$, $\Phi : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ is a bijective homomorphism, called an isomorphism. We record this result:

Chinese Remainder Theorem. If m, n are relatively prime integers ≥ 2, then

$$\Phi : \mathbf{Z}_{mn} \xrightarrow{\sim} \mathbf{Z}_m \times \mathbf{Z}_n,$$

is an isomorphism.

Now let us assume $(m, n) = 1$. Then the fact that Φ preserves ring structures and unity implies that Φ preserves units, in particular

$$\Phi : \mathbf{Z}_{mn}^* \xrightarrow{\sim} \left(\mathbf{Z}_m \times \mathbf{Z}_n\right)^*,$$

is an isomorphism (of groups). Finally, it is reasonably obvious that $\left(\mathbf{Z}_m \times \mathbf{Z}_n\right)^* = \mathbf{Z}_m^* \times \mathbf{Z}_n^*$. Therefore, since $(m, n) = 1$,

$$\varphi(m \cdot n) = {}^{\#}\mathbf{Z}_{mn}^* = {}^{\#}\left(\mathbf{Z}_m \times \mathbf{Z}_n\right)^* = {}^{\#}\mathbf{Z}_m^* \cdot {}^{\#}\mathbf{Z}_n^* = \varphi(m) \cdot \varphi(n).$$

This proves claim 1.

Proof of Claim 2

First of all, for $1 \leq N \leq p^m$, we can write $N = q \cdot p + r$, where $0 \leq r \leq p-1$. Note that q is in the range $q = 0, \ldots, p^{m-1}$. Furthermore, it is easy to see that

$$(N, p^m) = 1 \Leftrightarrow (N, p) = 1 \Leftrightarrow N = qp + r, \text{ where } 1 \leq r \leq p-1,\ 0 \leq q \leq p^{m-1} - 1.$$

Thus

$${}^{\#}\{N \mid 1 \leq N \leq p^m,\ \&\ (N, p^m) = 1\} = (p-1)p^{m-1} = p^m - p^{m-1}.$$

This establishes claim 2.

[†] Where $(\overline{x}_m, \overline{y}_n) + (\overline{u}_m, \overline{v}_n) = (\overline{x}_m + \overline{u}_m, \overline{y}_n + \overline{v}_n)$, $(\overline{x}_m, \overline{y}_n) \bullet (\overline{u}_m, \overline{v}_n) = (\overline{x}_m \cdot \overline{u}_m, \overline{y}_n \cdot \overline{v}_n)$, with unity $(\overline{1}_m, \overline{1}_n)$ and zero element $(\overline{0}_m, \overline{0}_n)$.

Solutions of Equations in Rings

Let $\mathbf{A}$ be an integral domain. Fix $a, b \in \mathbf{A}$, with $a \neq 0$. Let x be an indeterminate (i.e. a variable).

Claim. The equation $ax + b = 0$ has at most one solution in $\mathbf{A}$.

Reason: Suppose that $u, v \in \mathbf{A}$ both satisfy this equation, i.e.

$$\begin{aligned} au + b &= 0 \\ av + b &= 0 \end{aligned}$$

Then subtracting gives $a(u - v) = 0$. But $a \neq 0$ and $\mathbf{A}$ is an integral domain. Therefore $u - v = 0$, i.e. $u = v$.

Remark. If $\mathbf{A} = \mathbf{F}$ is a field, then $ax + b = 0$, with $a \neq 0$, has a unique solution in $\mathbf{F}$. Namely, $x = a^{-1}(-b) \in \mathbf{F}$.

Ex. Let $\mathbf{A} = \mathbf{Z}$. Then for example, $2x + 1 = 0$ has no solution in $\mathbf{Z}$. However, this equation has a solution in $\mathbf{Q}$, namely $x = -\frac{1}{2}$.

This leads us to the concept of a quotient field. Assume given an integral domain $\mathbf{A}$ with unity $1 \in \mathbf{A}$. The quotient field of $\mathbf{A}$, denoted by $\mathbf{K} := \mathrm{Quot}(\mathbf{A})$, is given by the following prescription[†]:

$$\mathbf{K} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbf{A}, b \neq 0, \ \& \ \frac{a_1}{b_1} = \frac{a_2}{b_2} \Leftrightarrow a_1 b_2 = b_1 a_2 \text{ in } \mathbf{A} \right\}.$$

Note that we can view $\mathbf{A} \subset \mathbf{K}$ as a subring, by the identification $a \in \mathbf{A} \mapsto \frac{a}{1} \in \mathbf{K}$. It is obvious by this construction that $\mathbf{K}$ is a field. Thus for an integral domain $\mathbf{A}$, with $a, b \in \mathbf{A}$ and $a \neq 0$, the equation $ax + b = 0$ always has a (unique) solution in $\mathbf{K}$, namely $x = -\frac{b}{a} \in \mathbf{K}$.

Ex. $\mathrm{Quot}(\mathbf{Z}) = \mathbf{Q}$.

Ex. Let $\mathbf{F}$ be a field. Then $\mathrm{Quot}(\mathbf{F}) = \mathbf{F}$.

Quadratic Equations over a Field $\mathbf{F}$

For motivation, suppose we consider the quadratic equation

$$ax^2 + bx + c = 0, \quad (a \neq 0),$$

[†] In some texts, the construction of quotient fields begins with pairs $(a, b) \in \mathbf{A}^2$, with $b \neq 0$, for which $(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1 b_2 = b_1 a_2$ in $\mathbf{A}$, and eventually identify $\frac{a}{b} \leftrightarrow (a, b)$. We could do it this way, but lets not.

with $a, b, c \in \mathbf{R}$ (or in $\mathbf{C}$). Then the quadratic formula gives

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \in \mathbf{C}.$$

If we try to solve the same equation over a given field $\mathbf{F}$, i.e., where $a, b, c \in \mathbf{F}$, then we may run into the problem where $2 = 0 \in \mathbf{F}$, and so the above quadratic formula would not work. [For example $\overline{2} = \overline{0} \in \mathbf{Z}_2$.] It seems natural to detemine those fields where such a formula would still work. This leads us to the following:

Assume given a $\mathbf{F}$ with unity $1_{\mathrm{F}} \in \mathbf{F}$, we consider the map

$$\Phi : \mathbf{Z} \to \mathbf{F}, \quad \Phi(m) = m \cdot 1_{\mathrm{F}} := \begin{cases} \underbrace{1_{\mathrm{F}} + \cdots + 1_{\mathrm{F}}}_{m \text{ times}} & \text{if } m > 0 \\ 0 & \text{if } m = 0 \\ \underbrace{(-1_{\mathrm{F}}) + \cdots + (-1_{\mathrm{F}})}_{|m| \text{ times}} & \text{if } m < 0 \end{cases}$$

Φ has the following "nice" properties:

1) $\Phi(n + m) = \Phi(n) + \Phi(m)$, i.e. Φ preserves addition $(+)$. [Reason: $\Phi(n + m) = (n + m) \cdot 1_{\mathrm{F}} = n \cdot 1_{\mathrm{F}} + m \cdot 1_{\mathrm{F}} = \Phi(n) + \Phi(m)$.]

2) $\Phi(n \cdot m) = \Phi(n) \cdot \Phi(m)$, i.e. Φ preserves multiplication $(\bullet)$. [Reason: $\Phi(n \cdot m) = (n \cdot m) \cdot 1_{\mathrm{F}} = (n \cdot 1_{\mathrm{F}}) \cdot (m \cdot 1_{\mathrm{F}}) = \Phi(n) \cdot \Phi(m)$.]

3) $\Phi(1) = 1_{\mathrm{F}}$, i.e. Φ preserves unity.

Properties 1), 2) and 3) are the conditions that define Φ as a ring homomorphism. A natural question is whether one can "count" in $\mathbf{F}$, or put differently, whether Φ is one-to-one. As we will see below, a way of measuring this is by introducing the kernel of the homomorphism Φ:

$$\ker \Phi := \{n \in \mathbf{Z} \mid \Phi(n) = 0\}.$$

Note that $\Phi(0) = 0$, hence $0 \in \ker \Phi$. However, $\Phi(1) = 1_{\mathrm{F}} \neq 0$, hence $1 \notin \ker \Phi$. Therefore $\ker \Phi \neq \mathbf{Z}$.

Claim. $\ker \Phi$ is an ideal in $\mathbf{Z}$.

Reason: We must show the following:

(A) $m, n \in \ker \Phi \Rightarrow m+n \in \ker \Phi$. [Restatement: $\Phi(m) = \Phi(n) = 0 \Rightarrow \Phi(m+n) = 0$.]

(B) $m \in \ker \Phi$ and $n \in \mathbf{Z} \Rightarrow \Phi(n \cdot m) = 0$. [Restatement: $\Phi(m) = 0$ & $n \in \mathbf{Z} \Rightarrow \Phi(n \cdot m) = 0$.]

Details:

(A) Given $\Phi(m) = \Phi(n) = 0$, then $\Phi(m+n) = \underbrace{\Phi(m)}_{=0} + \underbrace{\Phi(n)}_{=0} = 0$.

(B) Given $\Phi(m) = 0$ and $n \in \mathbf{Z}$, then $\Phi(n \cdot m) = \Phi(n) \cdot \underbrace{\Phi(m)}_{=0} = 0$.

This proves the claim.

Since $\ker \Phi \subset \mathbf{Z}$ is an ideal, it must be of the form $\ker \Phi = (k) := \{q \cdot k \mid q \in \mathbf{Z}\}$ for some integer $k \geq 0$. Furthermore $k \neq 1$ since $\ker \Phi \neq (1) = \mathbf{Z}$.

Ex. $\mathbf{F} = \mathbf{Z}_5$,

$$\Phi : \mathbf{Z} \to \mathbf{Z}_5, \quad \Phi(m) = \overline{m}.$$

Note that $\Phi(m) = 0 \Leftrightarrow \overline{m} = \overline{0} \Leftrightarrow 5|m$. Thus $\ker \Phi = \{q \cdot 5 \mid q \in \mathbf{Z}\} = (5)$.

Ex. $\mathbf{F} = \mathbf{R}$. Then $\Phi : \mathbf{Z} \hookrightarrow \mathbf{R}$ is the inclusion. Therefore $\ker \Phi = 0 = (0)$.

Claim. Consider the map $\Phi : \mathbf{Z} \to \mathbf{F}$, where $\mathbf{F}$ is a field. Then:

(i) If $\ker \Phi = 0$, then Φ is one-to-one.

(ii) If $\ker \Phi \neq 0$, then $\ker \Phi = (p)$ for some prime $p \in \mathbf{N}$.

Reason: (i) We first observe that $\Phi(0) = 0$. Next $0 = \Phi(x + (-x)) = \Phi(x) + \Phi(-x)$, hence $\Phi(-x) = -\Phi(x)$. Now suppose $\ker \Phi = 0$, and that $\Phi(x) = \Phi(y)$ for some $x, y \in \mathbf{Z}$. Then $\Phi(x-y) = \Phi(x+(-y)) = \Phi(x) + \Phi(-y) = \Phi(x) - \Phi(y) = 0$, hence $x - y \in \ker \Phi = 0$, i.e. $x - y = 0$, or $x = y$. Thus Φ is one-to-one.

(ii) We recall that $\ker \Phi \neq (1)$, hence $\ker \Phi = (n)$ for some integer $n \geq 2$. There is an induced map $\overline{\Phi} : \mathbf{Z}_n \to \mathbf{F}$ completing the diagram below:

$$\begin{array}{ccc} \mathbf{Z} & \xrightarrow{\Phi} & \mathbf{F} \\ \downarrow & \overline{\Phi} \nearrow & \\ \mathbf{Z}_n & & \end{array}$$

Namely, $\overline{\Phi}$ is defined by the formula $\overline{\Phi}(\overline{m}) = \Phi(m)$. We must first check that $\overline{\Phi}$ is well-defined. Suppose that $\overline{m}_1 = \overline{m}_2$. We must show that $\Phi(m_1) = \Phi(m_2)$. But $\overline{m}_1 = \overline{m}_2 \Leftrightarrow n|(m_1 - m_2) \Leftrightarrow m_1 - m_2 \in \ker \Phi \Leftrightarrow \Phi(m_1 - m_2) = 0 \Leftrightarrow \Phi(m_1) = \Phi(m_2)$. Thus $\overline{\Phi}$ is well-defined. Next, one can show that $\ker \overline{\Phi} = \overline{0} \in \mathbf{Z}_n$, and in particular this implies that $\overline{\Phi} : \mathbf{Z}_n \hookrightarrow \mathbf{F}$ is a one-to-one homomorphism of rings (where in particular, addition and multiplication of rings is preserved). Since $\mathbf{F}$ is a field, hence an integral domain, it follows that $\mathbf{Z}_n$ is an integral domain (hence a field). Therefore $n = p$ is prime. This leads us to the following way of characterizing fields:

Definition. Assume given a field $\mathbf{F}$ and corresponding homomorphism $\Phi : \mathbf{Z} \to \mathbf{F}$. We define the characteristic of $\mathbf{F}$ by the formula:

$$\mathrm{Char}(\mathbf{F}) = \begin{cases} 0 & \text{if } \ker \Phi = (0) \\ p > 0 & \text{if } \ker \Phi = (p),\ p \text{ a prime} \end{cases}.$$

Ex. $\mathrm{Char}(\mathbf{R}) = \mathrm{Char}(\mathbf{C}) = \mathrm{Char}(\mathbf{Q}) = 0$. $\mathrm{Char}(\mathbf{Z}_2) = 2$, $\mathrm{Char}(\mathbf{Z}_3) = 3$, $\mathrm{Char}(\mathbf{Z}_5) = 5$, and more generally, $\mathrm{Char}(\mathbf{Z}_p) = p$ for a prime $p \in \mathbf{N}$.

Remark. If $\mathrm{Char}(\mathbf{F}) = 0$, then one can think of Φ as identifying $\mathbf{N} \subset \mathbf{F}$, and hence one can "count" in the field $\mathbf{F}$. On the contrary, if $\mathrm{Char}(\mathbf{F}) = p > 0$, then one can think of Φ as identifying $\mathbf{Z}_p \subset \mathbf{F}$, in which case one cannot "count" in $\mathbf{F}$ (i.e. this: $\overline{1}, \overline{1}+\overline{1} = \overline{2}, \ldots, \overline{p} = \overline{0}$, is cyclic).

Back to Quadratic Equations

We want to solve the equation

$$ax^2 + bx + c = 0,$$

where x is a variable, and $a, b, c \in \mathbf{F}$, $a \neq 0$. We first observe that $\mathrm{Char}(\mathbf{F}) \neq 2 \Leftrightarrow 2 \neq 0 \in \mathbf{F} \Leftrightarrow 2^{-1} \in \mathbf{F}$. We will restrict ourselves to the case where $\mathrm{Char}(\mathbf{F}) \neq 2$. Also, we will write, for $\lambda \in \mathbf{F}$, $\lambda \neq 0$, $\frac{1}{\lambda}$ instead of λ^{-1}. Thus formally we can solve for x:

$$ax^2 + bx + c = 0 \Leftrightarrow \frac{1}{a}\Big(ax^2 + bx + c = 0\Big) = 0 \Leftrightarrow \left(x + \frac{b}{2a}\right)^2 + \frac{c}{a} - \frac{b^2}{4a^2} = 0$$

$$\Leftrightarrow \left(x + \frac{b}{2a}\right)^2 + \frac{4ac - b^2}{4a^2} = 0 \Leftrightarrow x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \Leftrightarrow x = \frac{-b \pm \sqrt{\Delta}}{2a},$$

where $\Delta = b^2 - 4ac \in \mathbf{F}$. The essential problem here is that $\sqrt{\Delta}$ may not belong to $\mathbf{F}$.

Ex. $\mathbf{F} = \mathbf{R}$, $x^2 + 1 = 0$, (here $a = c = 1,\ b = 0$). Then $\Delta = -4$, hence $\sqrt{\Delta} = \sqrt{-4} \notin \mathbf{R}$; moreover there is no solution of this equation in $\mathbf{R}$. [Note that the solution lies in $\mathbf{C}$, which is a quadratic field extension of $\mathbf{R}$. We will revisit this idea later.]

Now suppose for example, that $\sqrt{\Delta} \in \mathbf{F}$, i.e. there exists $\delta \in \mathbf{F}$ such that $\delta^2 = \Delta$. Then we can solve for $x \in \mathbf{F}$, namely:

$$x = \frac{-b \pm \sqrt{\Delta}}{2a} = \frac{-b \pm \delta}{2a}; \quad \text{(or we can write } x = 2^{-1}a^{-1}\big(-b \pm \sqrt{b^2 - 4ac}\big)\text{)}.$$

Ex. $\mathbf{F} = \mathbf{Z}_5$, and the equation:

$$x^2 + \overline{2}x + \overline{2} = \overline{0}.$$

[Here we interpret $a = \overline{1},\ b = \overline{2},\ c = \overline{2}$.] Then $\Delta = \overline{4} - \overline{8} = \overline{4} - \overline{3} = \overline{1}$. Thus $\sqrt{\Delta} = \pm\overline{1} = \{\overline{1}, -\overline{1} = \overline{4}\} \subset \mathbf{Z}_5$. Thus by the quadratic formula,

$$x = \overline{2}^{-1}(-\overline{2} \pm \overline{1}) \overset{-\overline{3}=\overline{2}}{=} \overline{2}^{-1}\{\overline{2}, \overline{2}^2 = \overline{4}) = \{\overline{1}, \overline{2}\}.$$

Ex. $\mathbf{F} = \mathbf{Z}_5$, and the equation:

$$x^2 - \overline{2} = \overline{0}.$$

[Here we interpret $a = \overline{1},\ b = \overline{0},\ c = -\overline{2}$.] Then $\Delta = \overline{8} = \overline{3}$. Consider the table of values:

$$\begin{array}{rcl} \overline{0}^2 & = & \overline{0} \\ \overline{1}^2 & = & \overline{1} \\ \overline{2}^2 & = & \overline{4} \\ \overline{3}^2 & = & \overline{4} \\ \overline{4}^2 & = & \overline{1} \end{array}$$

It is clear that neither $\overline{2}$ nor $\overline{3}$ appear in the righthand column of this table. Thus $x^2 - \overline{2} = \overline{0}$ has no solution in $\mathbf{Z}_5$, and $\sqrt{\Delta} \notin \mathbf{Z}_5$.

This leads us to:

Main Theorem. For any given quadratic equation over a given field $\mathbf{F}$, namely:

$$ax^2 + bx + c = 0, \quad (a, b, c \in \mathbf{F},\ a \neq 0),$$

there is a field extension $\tilde{\mathbf{F}}$ of $\mathbf{F}$, i.e. a field $\tilde{\mathbf{F}}$ for which $\mathbf{F} \subset \tilde{\mathbf{F}}$ is a subfield, such that the quadratic equation has a solution in $\tilde{\mathbf{F}}$.

Ex. $x^2 + 1 = 0$, $\mathbf{F} = \mathbf{R}$. The solutions x are $\pm\sqrt{-1} \in \mathbf{C}$. In this case $\mathbf{C} = \tilde{\mathbf{F}} = \tilde{\mathbf{R}}$.

It is worthwhile mentioning the:

Fundamental Theorem of Algebra. Any polynomial equation of the form:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

[where $a_0, \ldots, a_n \in \mathbf{C}$, $n \in \mathbf{N}$, $a_n \neq 0$, and x is an indeterminate], has a solution in $\mathbf{C}$.

Rather than prove the main theorem above, we will illustrate it by an example.

Example. Consider the equation

$$x^2 + x + \overline{1} = \overline{0},$$

with coefficients in $\mathbf{Z}_2$, i.e. $a = \overline{1},\ b = \overline{1},\ c = \overline{1}$. Set $p(x) = x^2 + x + \overline{1}$, and note that $p(\overline{0}) = \overline{1} \neq \overline{0}$, $p(\overline{1}) = \overline{3} = \overline{1} \neq \overline{0}$. Thus the quadratic equation $p(x) = \overline{0}$ has no solution in $\mathbf{F} = \mathbf{Z}_2$. As in the case of inventing a solution $\pm\sqrt{-1}$ to $x^2+1 = 0$ in the previous example, we "invent" a solution to $p(x) = \overline{0}$, and call it α. Note that $\alpha \notin \mathbf{Z}_2$ since $p(\alpha) = \overline{0}$, i.e.

$$\alpha^2 + \alpha + \overline{1} = \overline{0}.$$

Note that $\pm\overline{1} = \overline{1}$ in $\mathbf{Z}_2$. Thus $\alpha^2 = -\alpha - \overline{1} = \alpha + \overline{1}$. For $\mathbf{F} = \mathbf{Z}_2$, set $\tilde{\mathbf{F}} = \mathbf{Z}_2[\alpha] := \{\overline{a} + \overline{b}\alpha \mid \overline{a}, \overline{b} \in \mathbf{Z}_2\}$. Note that $\tilde{\mathbf{F}} = \{\overline{0}, \overline{1}, \alpha, \overline{1} + \alpha\}$ has 4 elements. Addition and multiplication are defined in the obvious way:

$$(\overline{a} + \overline{b}\alpha) + (\overline{c} + \overline{d}\alpha) = (\overline{a} + \overline{c}) + (\overline{b} + \overline{d})\alpha \in \tilde{\mathbf{F}},$$

$$(\overline{a} + \overline{b}\alpha) \cdot (\overline{c} + \overline{d}\alpha) = \big(\overline{ac} + \overline{bd}[\alpha^2 = \alpha + \overline{1}]\big) + (\overline{a}\overline{d} + \overline{b}\overline{c})\alpha = (\overline{ac} + \overline{bd}) + (\overline{a}\overline{d} + \overline{b}\overline{c} + \overline{bd})\alpha \in \tilde{\mathbf{F}}.$$

Since $\tilde{\mathbf{F}}$ has only 4 elements, we can easily give the $+, \bullet$ tables below.

$+$	$\overline{0}$	$\overline{1}$	α	$\overline{1}+\alpha$
$\overline{0}$	$\overline{0}$	$\overline{1}$	α	$\overline{1}+\alpha$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{1}+\alpha$	α
α	α	$\overline{1}+\alpha$	$\overline{0}$	$\overline{1}$
$\overline{1}+\alpha$	$\overline{1}+\alpha$	α	$\overline{1}$	$\overline{0}$

$\bullet$	$\overline{0}$	$\overline{1}$	α	$\overline{1}+\alpha$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	α	$\overline{1}+\alpha$
α	$\overline{0}$	α	$\overline{1}+\alpha$	$\overline{1}$
$\overline{1}+\alpha$	$\overline{0}$	$\overline{1}+\alpha$	$\overline{1}$	α

Note that $\alpha^{-1} = \alpha+\overline{1}$ and that $(\overline{1}+\alpha)^{-1} = \alpha$. For example $\alpha(\overline{1}+\alpha) = \alpha^2+\alpha = (\alpha+\alpha)+\overline{1} = \overline{2}\alpha + \overline{1} = \overline{0}\cdot\alpha + \overline{1} = \overline{1}$. It is obvious that $\tilde{F}$ is a field and that $\mathbf{Z}_2 = \mathbf{F} \subset \mathbf{Z}_2[\alpha] = \tilde{\mathbf{F}}$ is a subfield. Finally, by construction, $x^2 + x + \overline{1} = \overline{0}$ has a solution in $\tilde{\mathbf{F}}$. Note: Consider the diagram:

$$\begin{array}{ccc} \mathbf{Z} & \xrightarrow{\Phi} & \mathbf{Z}_2[\alpha] \\ \downarrow & \overline{\Phi}\ \nearrow & \\ \mathbf{Z}_2 & & \end{array}$$

It is easy to see that $\overline{\Phi}$ gives the inclusion of $\mathbf{Z}_2$ in $\mathbf{Z}_2[\alpha]$, hence $\overline{\Phi}$ is one-to-one, and that $\mathrm{char}(\mathbf{Z}_2[\alpha]) = 2$.

Polynomial Rings

Let $\mathbf{A}$ be a ring, and x an indeterminate. A polynomial with coefficients in $\mathbf{A}$ is given by a formal sum:

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_0, \ldots, a_n \in \mathbf{A},$$

where n is an integer ≥ 0. It is convenient to rewrite $p(x)$ in the form:

$$p(x) = \sum_{i=0}^{n} a_i x^i; \quad \text{where } a_0 x^0 := a_0.$$

The zero polynomial is the polynomial where all the coefficients a_i's are zero. If $a_n \neq 0$, we define $\deg p(x) = n$. The degree of the zero polynomial is taken to be $-\infty$.

Ex. $p(x) = a_0 \neq 0 \Rightarrow \deg p(x) = 0$. $p(x) = a_1 x + a_0,\ a_1 \neq 0, \Rightarrow \deg p(x) = 1$. $p(x) = a_2 x^2 + a_1 x + a_0,\ a_2 \neq 0, \Rightarrow \deg p(x) = 2$. We now put:

$$\mathbf{A}[x] = \big\{\text{Polynomials with coefficients in } \mathbf{A}\big\}.$$

[Note: If $\mathbf{A}$ has unity $1 \in \mathbf{A}$, then we write x^d for $1 \cdot x^d$.]

Addition and Multiplication of Polynomials:

+: Let $\left.\begin{array}{l} p(x) = a_n x^n + \cdots + a_1 x + a_0 \\ q(x) = b_m x^m + \cdots + b_1 x + b_0 \end{array}\right\} \in \mathbf{A}[x]$ be given. We can always arrange for $m = n$, for if say $m < n$, then we can declare $b_{m+1} = \cdots b_n = 0$ and write $q(x) = b_n x^n + \cdots b_1 x + b_0$. Thus we can write:

$$\left.\begin{array}{rcl} p(x) & = & \sum_{i=0}^{n} a_i x^i \\ q(x) & = & \sum_{i=0}^{n} b_i x^i \end{array}\right\} \quad \Rightarrow p(x) + q(x) \stackrel{\text{def}}{=} \sum_{i=0}^{n} (a_i + b_i) x^i = (a_n + b_n)x^n + \cdots + (a_0 + b_0).$$

•: Again, let $\left.\begin{array}{l} p(x) = a_n x^n + \cdots + a_1 x + a_0 \\ q(x) = b_m x^m + \cdots + b_1 x + b_0 \end{array}\right\} \in \mathbf{A}[x]$ be given. Then we define:

$$p(x) \cdot q(x) = a_n b_m x^{n+m} + (a_n b_{m-1} + b_m a_{n-1}) x^{n+m-1} + \cdots$$

$$+\Big(\sum_{i+j=k} a_i b_j\Big) x^k + \cdots + (a_1 b_0 + b_1 a_0) x + a_0 b_0.$$

Using summation notation, this becomes:

$$p(x) \cdot q(x) = \sum_{k=0}^{n+m} \Big(\sum_{i+j=k} a_i b_j\Big) x^k \in \mathbf{A}[x].$$

Claim. $\mathbf{A}[x]$ is a ring under $+, \bullet$ defined above; moreover $\mathbf{A} \subset \mathbf{A}[x]$ is a subring. Furthermore, $\mathbf{A}$ has a unity $\Leftrightarrow$ $\mathbf{A}[x]$ has a unity. *[We leave this claim as an exercise for the reader.]*

Remarks. (i) It is obvious that $\deg\big(p(x)+q(x)\big) \leq \max\big\{\deg p(x), \deg q(x)\big\}$. For example in $\mathbf{Z}[x]$:

$$\deg\begin{bmatrix} x^3+x+1 \\ + \\ 2x^2+6 \end{bmatrix} = \deg(x^3+2x^2+x+7) = 3 = \max\big\{\underbrace{\deg(x^3+x+1)}_{3}, \underbrace{\deg(2x^2+6)}_{2}\big\}.$$

$$\deg\begin{bmatrix} x^2+x+1 \\ + \\ -x^2+2x+4 \end{bmatrix} = \deg(3x+5) = 1 < 2 = \max\{\underbrace{\deg(x^2+x+1)}_{2}, \underbrace{\deg(-x^2+2x+4)}_{2}\}.$$

$$\deg\big((x^3+x+1)+(x^3+6)\big) = \deg(2x^3+x+7) = 3 = \max\big\{\underbrace{\deg(x^3+x+1)}_{3}, \underbrace{\deg(x^3+6)}_{3}\big\}.$$

(ii) Write $p(x) = a_n x^n + \cdots + a_0,\ q(x) = b_m x^m + \cdots + b_0 \in \mathbf{A}[x]$, where $a_n,\ b_m \neq 0$. Thus $\deg p(x) = n$, and $\deg q(x) = m$. Recall the product $p(x)\cdot q(x)$ looks like:

$$p(x)\cdot q(x) = a_n b_m x^{n+m} + \text{ lower degree terms}\ldots.$$

then it is easy to see that

$$\deg\big(p(x)\cdot q(x)\big) \leq \deg p(x) \ + \ \deg q(x).$$

To see how we can get a strict inequality ($<$), observe that it could happen that $a_n b_m = 0$, even though $a_n, b_n \neq 0$ [i.e. $\mathbf{A}$ need not be an integral domain!]

Ex. Let $p(x) = \overline{2}x^2,\ q(x) = \overline{2}x^2 + \overline{1} \in \mathbf{Z}_4[x]$. Then $\overline{2} \neq \overline{0} \in \mathbf{Z}_4$ and hence $\deg p(x) = \deg q(x) = 2$. But

$$p(x)\cdot q(x) = \overline{4}x^4 + \overline{2}x^2 = \overline{2}x^2,$$

since $\overline{4} = \overline{0}$ in $\mathbf{Z}_4$. Thus $\deg\big(p(x)\cdot q(x)\big) = 2 < 4 = \deg p(x) + \deg q(x)$. Note that $\mathbf{Z}_4$ is not an integral domain.

(iii) *It is obvious that if* $\mathbf{A}$ *is an integral domain, then:*

$$\deg\big(p(x)\cdot q(x)\big) = \deg p(x) + \deg q(x).$$

As an application of (iii) above, we arrive at:

Claim. (1) $\mathbf{A}$ is an integral domain $\Leftrightarrow$ $\mathbf{A}[x]$ is an integral domain.

(2) If $\mathbf{A}$ is an integral domain, then $\big(\mathbf{A}[x]\big)^* = \mathbf{A}^*$.

Reason: (1) Since $\mathbf{A} \subset \mathbf{A}[x]$ is a subring, it follows that $\mathbf{A}[x]$ an integral domain $\Rightarrow \mathbf{A}$ an integral domain; moreover if $\mathbf{A}$ has unity $1 \neq 0$, then this same unity $1 \neq 0$ is a unity for $\mathbf{A}[x]$. Now lets suppose that $\mathbf{A}$ is an integral domain, and assume given $p(x), q(x) \in \mathbf{A}[x]$ such that $p(x) \cdot q(x) = 0$. We must show that $p(x) = 0$ or $q(x) = 0$. But

$$-\infty \stackrel{\text{def}}{=} \deg 0 = \deg\big(p(x) \cdot q(x)\big) \underset{\text{Integral Domain}}{\overset{\mathbf{A} \text{ an}}{=}} \deg p(x) + \deg q(x).$$

Therefore either $\deg p(x) = -\infty$ (hence $p(x) = 0$), or $\deg q(x) = -\infty$ (hence $q(x) = 0$). This proves part (1).

(2) Assume that $\mathbf{A}$ is an integral domain, and that $p(x), q(x) \in \mathbf{A}[x]$ are given such that $p(x) \cdot q(x) = 1$ ($\Rightarrow p(x), q(x) \in \big(\mathbf{A}[x]\big)^*$). Then:

$$0 = \deg 1 = \deg\big(p(x) \cdot q(x)\big) \underset{\text{Integral Domain}}{\overset{\mathbf{A} \text{ an}}{=}} \underbrace{\deg p(x)}_{\geq 0} + \underbrace{\deg q(x)}_{\geq 0}.$$

Therefore $\deg p(x) = \deg q(x) = 0$, i.e. $0 \neq p(x) = p \in \mathbf{A},\ 0 \neq q(x) = q \in \mathbf{A}$, and that $p \cdot q = 1 \in \mathbf{A}$. Therefore $p(x) = p \in \mathbf{A}^*$ and $q(x) = q \in \mathbf{A}^*$. Thus $\big(\mathbf{A}[x]\big)^* \subset \mathbf{A}^*$ and clearly $\mathbf{A}^* \subset \big(\mathbf{A}[x]\big)^*$. Hence $\big(\mathbf{A}[x]\big)^* = \mathbf{A}^*$, and we're done.

Ex. $\big(\mathbf{Z}[x]\big)^* = \mathbf{Z}^* = \{1, -1\}$. This is because $\mathbf{Z}$ is an integral domain.

Ex. Let $\mathbf{F}$ be a field (hence an integral domain). Then $\big(\mathbf{F}[x]\big)^* = \mathbf{F}^* = \{x \in \mathbf{F} \mid x \neq 0\}$. Note that since $\big(\mathbf{F}[x]\big)^* \neq \{p(x) \in \mathbf{F}[x] \mid p(x) \neq 0\}$, it follows that $\mathbf{F}[x]$ is not a field. [E.g. $\big(\mathbf{Z}_2[x]\big)^* = \mathbf{Z}_2^* = \{\overline{1}\}$. Thus for example $x,\ x + \overline{1}$ have no multiplicative inverses in $\mathbf{Z}_2[x]$.]

The assumption that $\mathbf{A}$ is an integral domain in the above claim is essential:

Ex. $\big(\mathbf{Z}_4[x]\big)^* \neq \mathbf{Z}_4^*$. For example $(\overline{2}x + \overline{1})^2 = \overline{1}$, hence $(\overline{2}x + \overline{1}) \in \big(\mathbf{Z}_4[x]\big)^*$. Note that $\mathbf{Z}_4$ is not an integral domain.

Summary

Let $\mathbf{A}$ be a ring. Then:

1) $\mathbf{A}[x]$ is a ring and $\mathbf{A} \subset \mathbf{A}[x]$ is a subring.

2) If $\mathbf{A}$ has unity $1 \in \mathbf{A}$, then $\mathbf{A}[x]$ has the same unity $1 \in \mathbf{A}[x]$.

3) $\mathbf{A}$ is an integral domain $\Leftrightarrow \mathbf{A}[x]$ is an integral domain.

4) If $\mathbf{A}$ is an integral domain, then $\big(\mathbf{A}[x]\big)^* = \mathbf{A}^*$.

Evaluation of Polynomials

Let $\mathbf{A}$ be a ring, and $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{A}[x]$. Fix $\xi \in \mathbf{A}$. We set $p(\xi) = a_n \xi^n + \cdots + a_1 \xi + a_0 \in \mathbf{A}$.

Definition. $\xi \in \mathbf{A}$ is said to be a root of $p(x)$ if $p(\xi) = 0$.

Ex. $p(x) = x^2 - 1 \in \mathbf{Z}[x]$. Then $p(\pm 1) = 0$, hence $\{1, -1\}$ are roots of $p(x)$.

Ex. $p(x) = x^2 + \overline{1} \in \mathbf{Z}_2[x]$. (Note: $x^2 = \overline{1} \cdot x^2$.) Then $p(\overline{1}) = \overline{1}^2 + \overline{1} = \overline{0}$, $p(\overline{0}) = \overline{1} \neq \overline{0}$. $\overline{1}$ is a root of $p(x)$. [Note that $x^2 + \overline{1} = x^2 + \underbrace{\overline{2}x}_{=\overline{0}} + \overline{1} = (x + \overline{1})^2$.]

Ex. **Warning.** In general, i.e. over general fields $\mathbf{F}$, polynomials (in $\mathbf{F}[x]$) are not functions. For instance $p(x) = x^2 + x \in \mathbf{Z}_2[x]$ is not the zero polynomial, and yet $p(x)$ takes the value $\overline{0}$ on $\mathbf{Z}_2$, i.e. $p(\overline{0}) = \overline{0},\ p(\overline{1}) = \overline{0}$.

Definition. Let $\mathbf{F}$ be a field, and $\mathbf{F}[x]$ the corresponding polynomial ring. A non-constant polynomial $p(x) \in \mathbf{F}[x]$ is said to be irreducible, if $p(x)$ cannot be factored as a product $p(x) = f(x) \cdot g(x)$, where $f(x), g(x) \in \mathbf{F}[x]$ and where $\deg f(x) < \deg p(x)$ and $\deg g(x) < \deg f(x)$.

Remark. If $p(x) \in \mathbf{F}[x]$ is non-constant, and not irreducible, then $p(x)$ is said to be reducible.

Ex. Any polynomial of degree 1 in $\mathbf{F}[x]$ is irreducible. (Why?)

Ex. In $\mathbf{Q}[x]$, $x^2 + 1 = \frac{1}{2}(2x^2 + 2)$ is not a "proper" factorization. In fact, $x^2 + 1$ is irreducible in $\mathbf{Q}[x]$. [Reason below.]

Ex. $x^2 + \overline{1}$ is reducible in $\mathbf{Z}_2[x]$. Recall earlier that we noted: $x^2 + \overline{1} = (x + \overline{1})^2$. In this case, if we write $p(x) = x^2 + \overline{1}$, then $p(x) = f(x) \cdot g(x)$ where $f(x) = g(x) = x + \overline{1}$. Also $\deg p(x) = 2$, whereas $\deg f(x) = \deg g(x) = 1$.

Ex. $x^2 + 1$ is irreducible in $\mathbf{R}[x]$ (hence it is likewise irreducible in $\mathbf{Q}[x]$). Reason: Suppose to the contrary that $x^2 + 1 = f(x) \cdot g(x)$ is reducible, i.e. where $\deg f(x) = \deg g(x) = 1$. Then we can write $f(x) = a_1 x + a_0$ and $g(x) = b_1 x + b_0$, where $a_0, a_1, b_0, b_1 \in \mathbf{R}$; moreover from the equation $x^2 + 1 = f(x) \cdot g(x)$, it is easy to see that $a_0, a_1, b_0, b_1 \neq 0$. Hence $x = -\frac{a_0}{a_1}$ is a real root of $f(x)$, and therefore $\big(-\frac{a_0}{a_1}\big)^2 + 1 = f\big(-\frac{a_0}{a_1}\big) \cdot g\big(-\frac{a_0}{a_1}\big) = 0$. But $-\frac{a_0}{a_1} \in \mathbf{R} \Rightarrow \big(-\frac{a_0}{a_1}\big)^2 + 1 \geq 1$. Therefore $x^2 + 1$ must be irreducible.

Ex. $x^2 + 1$ is reducible in $\mathbf{C}[x]$. In this case $x^2 + 1 = (x + \sqrt{-1})(x - \sqrt{-1})$, $\sqrt{-1} \in \mathbf{C}$.

Finding $\mathbf{Q}$*-roots of Polynomials in* $\mathbf{Z}[x]$

Assume given $p(x) \in \mathbf{Z}[x]$, where we can assume is in the form:

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,\ a_0, \ldots, a_n \in \mathbf{Z},\ a_0 \neq 0,\ a_n \neq 0.$$

Suppose that $p(r) = 0$ for some $r \in \mathbf{Q}$. As before, we can assume that $r = \frac{k}{m}$, where $k, m \in \mathbf{Z}$ and that $\mathrm{GCD}(k, m) = 1$. [Note that $a_0 \neq 0 \Rightarrow r \neq 0$; in particular $k, m \neq 0$.] Thus:

$$0 = p\left(\frac{k}{m}\right) = a_n\left(\frac{k}{m}\right)^n + a_{n-1}\left(\frac{k}{m}\right)^{n-1} + \cdots + a_1\left(\frac{k}{m}\right) + a_0.$$

Multiplying both sides by m^n yields:

$$0 = m^n \cdot 0 = m^n p\left(\frac{k}{m}\right) = a_n k^n + a_{n-1}k^{n-1}m + \cdots + a_1 k m^{n-1} + a_0 m^n.$$

Therefore:

$$\text{(I)} \qquad a_0 m^n \;=\; k\big(-a_n k^{n-1} - a_{n-1}k^{n-2}m - \cdots - a_1 m^{n-1}\big).$$

$$\text{(II)} \qquad a_n k^n \;=\; m\big(-a_{n-1}k^{n-1} - \cdots - a_1 k m^{n-2} - a_0 m^{n-1}\big).$$

Note that by using $(k, m) = 1$ and the Fundamental Theorem of Arithmetic:

$$k|\text{RHS of (I)} \quad \Rightarrow k|(a_0 m^n) \quad \overset{(k,m)=1}{\Rightarrow} \quad k|a_0.$$

$$m|\text{RHS of (II)} \quad \Rightarrow m|(a_n k^n) \quad \overset{(k,m)=1}{\Rightarrow} \quad m|a_n.$$

Upshot: *The only candidates for $\mathbf{Q}$-roots of $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{Z}[x]$, (where $a_0, a_n \neq 0$), are rational numbers $r \in \mathbf{Q}$ of the form:*

$$r \in \left\{ \frac{k}{m} \;\middle|\; k, m \in \mathbf{Z},\ (k, m) = 1,\ \text{and where } k|a_0 \ \&\ m|a_n \right\}.$$

[Remark. The assumption that the constant term $a_0 \neq 0$ is very mild. If for example $a_0 = 0$ but say $a_1 \neq 0$, then we can write $p(x) = a_n x^n + \cdots + a_1 x = x \cdot \underbrace{(a_n x^{n-1} + \cdots + a_1)}_{\text{constant term } a_1 \neq 0}$.]

Observation: $p(x)$ is said to be a monic polynomial if $a_1 = 1$, i.e. $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. In this case, the only $\mathbf{Q}$-roots of a monic polynomial $p(x) \in \mathbf{Z}[x]$ are $\mathbf{Z}$-roots. This is because in the Upshot above, r is of the form $r = \frac{k}{m}$ where $m|(a_n = 1)$, hence $m = \pm 1$, i.e. $r = \pm k \in \mathbf{Z}$.

Ex. Let $p(x) = x^2 - 2 \in \mathbf{Z}[x]$. Then the only candidates for $\mathbf{Q}$-roots of $p(x)$ are of the form $r = k/m$ where $k|2$ and $m|1$, i.e. of the form $\{\pm 1, \pm 2\}$. Clearly none of these are roots of $p(x)$. Note that $p(x)$ has real roots, namely $\pm\sqrt{2}$. Thus we have given another reason why $\sqrt{2} \notin \mathbf{Q}$.

Ex: Show that the real number $\sqrt[3]{3} \notin \mathbf{Q}$. Solution: Notice that $\sqrt[3]{3}$ is a root of the equation $x^3 - 3 = 0$. Thus $\sqrt[3]{3} \notin \mathbf{Q} \Leftrightarrow p(x)$ has no $\mathbf{Q}$-roots, where $p(x) = x^3 - 3$. But the only candidates for $\mathbf{Q}$-roots of $p(x)$ are where $r = k/m$, $k|3$, $m|1$, i.e. of the form $\{\pm 1, \pm 3\}$, and clearly none of these are roots of $p(x)$. [Note: $p(x)$ also has two $\mathbf{C}$-roots, which are complex conjugates of each other.]

Example. Let $p(x) = x^4 + 2x^3 - 2x^2 - 2x + 4 \in \mathbf{Z}[x]$. The candidates for $\mathbf{Q}$-roots are $r = k/m$, where $k|4$ and $m|1$, i.e. of the form $\{\pm 1, \pm 2, \pm 4\}$. One checks that $p(\pm 1)$, $p(\pm 4)$ and $p(2)$ are all non-zero, and that $p(-2) = 0$. Thus $r = -2$ is the only $\mathbf{Q}$-root. An elementary fact that we will show later [Euclid] is that $p(r) = 0 \Leftrightarrow (x - r)$ is a factor of $p(x)$ (in $\mathbf{Q}[x]$). In our case, $(x + 2) = (x - (-2))$ is a factor of $p(x)$. We now do long division:

$$
\begin{array}{rcccccccccc}
 & x^3 & - & 2x & + & 2 & & & & \\
 & -- & - & -- & - & -- & - & -- & - & -- \\
x+2 \;\big)\; & x^4 & + & 2x^3 & - & 2x^2 & - & 2x & + & 4 \\
 & x^4 & + & 2x^3 & & & & & & \\
 & -- & - & -- & - & -- & - & -- & - & -- \\
 & & & & & -2x^2 & - & 2x & + & 4 \\
 & & & & & -2x^2 & - & 4x & & \\
 & & & & & -- & - & -- & - & -- \\
 & & & & & & & 2x & + & 4 \\
 & & & & & & & 2x & + & 4 \\
 & & & & & & & -- & - & -- \\
 & & & & & & & & & 0
\end{array}
$$

Thus we have

$$p(x) = (x + 2)(x^3 - 2x + 2).$$

If we view $p(x) \in \mathbf{Q}[x]$ via the subring inclusion $\mathbf{Z}[x] \subset \mathbf{Q}[x]$, then it is easy to see that $x + 2$ is irreducible in $\mathbf{Q}[x]$ (In fact, even in $\mathbf{Z}[x]$, but we will not pursue this line of enquiry here). It is easy to see that likewise $x^3 - 2x + 2$ is irreducible in $\mathbf{Q}[x]$. We use the fact that $x^3 - 2x + 2$ has no $\mathbf{Q}$-roots (Why? Hint: the only candidates for $\mathbf{Q}$-roots of $x^3 - 2x + 2 \in \mathbf{Z}[x]$ are $\{\pm 1, \pm 2\}$), together with:

Claim. Let $\mathbf{F}$ be a field. Then any polynomial $p(x) \in \mathbf{F}[x]$ of degree 2 or 3, is irreducible in $\mathbf{F}[x] \Leftrightarrow p(x)$ has no root in $\mathbf{F}$.

Reason: Suppose $p(x) = f(x) \cdot g(x)$ is reducible, i.e. where $\deg f(x) < \deg p(x)$, $\deg g(x) < \deg p(x)$. Then since $\deg p(x) = 2$ or 3, it follows that either $\deg f(x) = 1$ or $\deg g(x) = 1$. Suppose that e.g. $\deg f(x) = 1$. Then $f(x) = ax + b$ where $a, b \in \mathbf{F}$ and $a \neq 0$. Thus $f(-\frac{b}{a}) = 0$, hence $p(-\frac{a}{b}) = 0$ as well. Thus $p(x)$ has a root in $\mathbf{F}$, namely $-\frac{a}{b} \in \mathbf{F}$. Therefore, if $p(x)$ has no root in $\mathbf{F}$, it must be irreducible.

Remark. The above claim relies on the assumption that $\deg p(x) \leq 3$. For example, the degree 4 polynomial $(x^2 + 1)^2 \in \mathbf{R}[x]$ is clearly reducible in $\mathbf{R}[x]$, and yet has no root in $\mathbf{R}$.

Ex. Factor $p(x) = x^3 + x^2 + \overline{3} \in \mathbf{Z}_5[x]$ as far as possible (i.e. into a product of irreducibles). Solution: We look for roots of $p(x)$, where we recall that $p(x)$, being of degree 3, is reducible $\Leftrightarrow$ $p(x)$ has a root in $\mathbf{F} := \mathbf{Z}_5$. We need only check among the five values in $\mathbf{Z}_5$ for a root of $p(x)$ in $\mathbf{Z}_5$. Note that $p(\overline{1}) = \overline{0}$, hence $(x + \overline{4}) = (x - \overline{1})$ is a factor of $p(x)$ (by Euclid). We find the quotient factor $q(x)$ by long division:

$$
\begin{array}{rcccccccl}
 & x^2 & + & \overline{2}x & + & \overline{2} & & & \\
 & -- & - & -- & - & -- & - & -- & \\
x+\overline{4} \;\big)\; & x^3 & + & x^2 & + & \overline{3} & & & \\
 & x^3 & + & \overline{4}x^2 & & & & & \\
 & -- & - & -- & - & -- & - & -- & \\
 & & & \overline{2}x^2 & + & \overline{3} & & & [\text{Use } -\overline{3} = \overline{2}] \\
 & & & \overline{2}x^2 & + & \overline{3}x & & & [\text{Use } \overline{8} = \overline{3}] \\
 & & & -- & - & -- & - & -- & \\
 & & & & & -\overline{3}x & + & \overline{3} & \\
 & & & & & -\overline{3}x & + & \overline{3} & [\text{Use } \overline{2} = -\overline{3}] \\
 & & & & & -- & - & -- & \\
 & & & & & & & \overline{0} &
\end{array}
$$

Thus

$$p(x) = x^3 + x^2 + \overline{3} = \underbrace{(x + \overline{4})}_{(x-\overline{1})}\underbrace{(x^2 + \overline{2}x + \overline{2})}_{q(x)}$$

Again, we recall that $q(x)$, being of degree 2, is reducible $\Leftrightarrow$ $q(x)$ has a root in $\mathbf{F} := \mathbf{Z}_5$. We observe that $q(\overline{1}) = \overline{5} = \overline{0}$. Hence again, $x - \overline{1} = x + \overline{4}$ is a factor of $q(x)$. Again, by long division:

$$
\begin{array}{rcccccl}
 & x & + & \overline{3} & & & \\
 & -- & - & -- & - & -- & \\
x+\overline{4} \;\big)\; & x^2 & + & \overline{2}x & + & \overline{2} & \\
 & x^2 & + & \overline{4}x & & & \\
 & -- & - & -- & - & -- & \\
 & & & \overline{3}x & + & \overline{2} & [\text{Use } -\overline{2} = \overline{3}] \\
 & & & \overline{3}x & + & \overline{2} & \\
 & & & -- & - & -- & \\
 & & & & & \overline{0} &
\end{array}
$$

Thus

$$(x^3 + x^2 + \overline{3}) = (x + \overline{4})^2(x + \overline{3}) = (x - \overline{1})^2(x - \overline{2}),$$

gives the decomposition of $p(x)$ into irreducibles[†].

[†] Alternatively, since $p(\overline{1}) = p(\overline{2}) = \overline{0}$, it follows that both $(x - \overline{1})$ and $(x - \overline{2})$ are factors of $p(x)$. Since $p(\overline{3})$ and $p(\overline{4})$ are both non-zero, it follows that $p(x)$ has either $(x - \overline{1})$ or $(x - \overline{2})$ as a double factor. But this can be detected by the formal derivative $p'(x) = \overline{3}x^2 + \overline{2}x$. In this case $p'(\overline{1}) = \overline{0}$ and $p'(\overline{2}) \neq \overline{0}$. Thus $x = \overline{1}$ is a double root. Hence $p(x) = (x - \overline{1})^2(x - \overline{2})$.

Euclid's Division Algorithm for Polynomials over Fields

Euclid's Algorithm. Let $\mathbf{F}$ be a field, with corresponding polynomial ring $\mathbf{F}[x]$. Assume given $f(x),\ g(x) \in \mathbf{F}[x]$, with $g(x) \neq 0$. Then there exists unique polynomials $q(x),\ r(x) \in \mathbf{F}[x]$, such that $f(x) = q(x) \cdot g(x) + r(x)$, where $\deg r(x) < \deg g(x)$.

Reason: There are two parts to the reasoning, namely the existence part, and the uniqueness part.

Existence. Let $d = \deg f,\ m = \deg g \geq 0$. If $m > d$, then we can write $f(x) = 0 \cdot g(x) + f(x)$, i.e. $q(x) = 0$ and $r(x) = f(x)$, with $\deg r(x) = d < m = \deg g(x)$. Thus we may assume that $d \geq m$. We can write

$$f(x) = a_d x^d + \cdots + a_0, \quad g(x) = b_m x^m + \cdots + b_0, \quad a_d, b_m \neq 0.$$

We are going to argue by induction on the degree of f, the initial cases of $\deg f \leq 1$ being 'obvious'. Set

$$h(x) = f(x) - \frac{a_d}{b_m} x^{d-m} g(x).$$

Then it is obvious that $\deg h < \deg f$. Hence by induction on degree,

$$f(x) - \frac{a_d}{b_m} x^{d-m} g(x) = h(x) = q_1(x) \cdot g(x) + r(x),$$

where $\deg r(x) < \deg g(x)$. Thus

$$f(x) = \underbrace{\left(\frac{a_d}{b_m} x^{d-m} + q_1(x) \right)}_{\text{Call this } q(x)} \cdot g(x) + r(x),$$

and we have now established the existence part.

Uniqueness. Suppose that

$$f(x) = q(x) \cdot g(x) + r(x) = \tilde{q}(x) \cdot g(x) + \tilde{r}(x),$$

where $\deg r(x),\ \deg \tilde{r}(x) < \deg g(x)$. Then:

$$\big(q(x) - \tilde{q}(x)\big) \cdot g(x) = \tilde{r}(x) - r(x),$$

and hence

$$\underbrace{\deg \big(q(x) - \tilde{q}(x)\big) + \deg g(x)}_{\deg \geq \deg g(x),\ or\ \ \deg = -\infty} = \underbrace{\deg \big(\tilde{r}(x) - r(x)\big)}_{\deg < \deg g(x)}$$

By comparison of degrees on both sides, and with the assumption that $\deg g(x) \geq 0$, it is clear that $\deg \big(q(x) - \tilde{q}(x)\big) = -\infty$, hence $q(x) - \tilde{q}(x) = 0,\ \Rightarrow \tilde{r}(x) - r(x) = 0$, i.e. $q(x) = \tilde{q}(x)$ and $r(x) = \tilde{r}(x)$. This establishes uniqueness.

Ex. $f(x) = x^3 + x + 1,\ g(x) = x + 1 \in \mathbf{Q}[x]$. We long divide:

$$
\begin{array}{rcccccccccc}
 & x^2 & - & x & + & 2 & = & q(x) & & \\
 & -- & - & -- & - & -- & - & -- & - & -- \\
x+1 \ \big) & x^3 & + & x & + & 1 & & & & \\
 & x^3 & + & x^2 & & & & & & \\
 & -- & - & -- & - & -- & - & -- & - & -- \\
 & & & -x^2 & + & x & + & 1 & & \\
 & & & -x^2 & - & x & & & & \\
 & & & & & -- & - & -- & - & -- \\
 & & & & & 2x & + & 1 & & \\
 & & & & & 2x & + & 2 & & \\
 & & & & & & & -- & - & -- \\
 & & & & & & & -1 & = & r(x)
\end{array}
$$

Thus

$$f(x) = \underbrace{(x^2 - x + 2)}_{q(x)} \cdot \underbrace{(x+1)}_{g(x)} + \underbrace{(-1)}_{r(x)}.$$

A Consequence of Euclid's Algorithm: Let $p(x) \in \mathbf{F}[x]$, $r_0 \in \mathbf{F}$ be given. Then r_0 is a root of $p(x) \Leftrightarrow (x - r_0)$ is a factor of $p(x)$ [i.e. $p(x) = q(x) \cdot (x - r_0)$ for some $q(x) \in \mathbf{F}[x]$].

Reason: By applying Euclid's algorithm to $p(x) \leftrightarrow f(x), \quad (x - r_0) \leftrightarrow g(x)$, we have

$$p(x) = q(x) \cdot (x - r_0) + r, \quad \deg r < \deg(x - r_0) = 1.$$

Thus $r \in \mathbf{F}$. If r_0 is a root, then:

$$0 = p(r_0) = q(r_0)(r_0 - r_0) \ + \ r = r, \quad \Rightarrow r = 0.$$

Thus r_0 a root $\Rightarrow (x - r_0)$ is a factor of $p(x)$. Conversely, if $(x - r_0)$ is a factor of $p(x)$, then $p(x) = q(x) \cdot (x - r_0)$ for some $q(x) \in \mathbf{F}[x]$, and hence $p(r_0) = q(r_0)(r_0 - r_0) = 0$. Thus r_0 is a root $\Leftrightarrow (x - r_0)$ is a factor of $p(x)$.

Ex. Let $p(x) = x^5 + x^2 + x + \overline{1} \in \mathbf{Z}_2[x]$. Factor $p(x)$ as far as possible in $\mathbf{Z}_2[x]$. Solution: We do this by trial and error. If we can find a root of $p(x)$ in $\mathbf{Z}_2$, then by the above consequence, we will have found a factor of $p(x)$. Note that $p(\overline{1}) = \overline{0}$, hence

$(x-\overline{1}) = (x+\overline{1})$ is a factor of $p(x)$. We long divide:

$$
\begin{array}{rcccccccccccc}
 & x^4 & + & x^3 & + & x^2 & + & \overline{1} & & & & & \\
 & -- & - & -- & - & -- & - & -- & - & -- & & & \\
x+\overline{1} \;\big)\; & x^5 & + & x^2 & + & x & + & \overline{1} & & & & & \\
 & x^5 & + & x^4 & & & & & & & & & \\
 & -- & - & -- & - & -- & - & -- & - & -- & & & \\
 & & & x^4 & + & x^2 & + & x & + & \overline{1} & & & \\
 & & & x^4 & + & x^3 & & & & & & & \\
 & & & & & -- & - & -- & - & -- & & & \\
 & & & & & x^3 & + & x^2 & + & x & + & \overline{1} & \\
 & & & & & x^3 & + & x^2 & & & & & \\
 & & & & & -- & - & -- & - & -- & - & -- & \\
 & & & & & & & & & x & + & \overline{1} & \\
 & & & & & & & & & x & + & \overline{1} & \\
 & & & & & & & & & -- & - & -- & \\
 & & & & & & & & & & & \overline{0} &
\end{array}
$$

Thus

$$p(x) = (x+\overline{1})\underbrace{(x^4+x^3+x^2+\overline{1})}_{\text{Call this } q(x)}.$$

Again, we have $q(\overline{1}) = \overline{0}$, thus $(x+\overline{1})$ is a factor of $q(x)$. We again long divide:

$$
\begin{array}{rcccccccccc}
 & x^3 & + & x & + & \overline{1} & & & & & \\
 & -- & - & -- & - & -- & - & -- & - & -- & \\
x+\overline{1} \;\big)\; & x^4 & + & x^3 & + & x^2 & + & \overline{1} & & & \\
 & x^4 & + & x^3 & & & & & & & \\
 & -- & - & -- & - & -- & - & -- & - & -- & \\
 & & & & & x^2 & + & \overline{1} & & & \\
 & & & & & x^2 & + & x & & & \\
 & & & & & -- & - & -- & - & -- & \\
 & & & & & & & x & + & \overline{1} & \\
 & & & & & & & x & + & \overline{1} & \\
 & & & & & -- & - & -- & - & -- & \\
 & & & & & & & & & \overline{0} &
\end{array}
$$

Thus

$$p(x) = (x+\overline{1})\cdot q(x) = (x+\overline{1})^2\underbrace{(x^3+x+\overline{1})}_{\text{Call this } h(x)}.$$

Note that since $\deg h(x) = 3$, it follows from an earlier result that $h(x)$ is irreducible in $\mathbf{Z}_2[x] \Leftrightarrow h(x)$ has no root in $\mathbf{Z}_2$. But $h(\overline{0}) = h(\overline{1}) = \overline{1} \neq \overline{0}$, hence $p(x) = (x+\overline{1})^2(x^3+x+\overline{1})$

is a factorization into irreducibles in $\mathbf{Z}_2[x]$. Thus this is as far as we can factor $p(x)$ in $\mathbf{Z}_2[x]$.

Definition. Let $p(x) \in \mathbf{F}[x]$ be a non-zero polynomial, and suppose $p(r) = 0$ for some $r \in \mathbf{F}$ [$\Rightarrow (x - r)$ is a factor of $p(x)$]. Let $\ell \in \mathbf{N}$ be the largest integer for which $p(x) = (x - r)^\ell q(x)$, where $q(x) \in \mathbf{F}[x]$ satisfies $q(r) \neq 0$. Then ℓ is called the multiplicity of the root r.

Exercise. Notation as in the above definition. Show that $r \in \mathbf{F}$ is a root of $p(x)$ of multiplicitity $\ell \Leftrightarrow$

$$p^{(m)}(r) = \begin{cases} 0 & \text{if } 0 \leq m \leq \ell - 1 \\ \neq 0 & \text{if } m = \ell \end{cases},$$

where $p^{(0)}(r) = p(r)$ and for $m \in \mathbf{N}$,

$$p^{(m)}(r) = \frac{d^m}{dx^m} p(x)\big|_{x=r}.$$

[If $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbf{F}[x]$, then

$$\frac{dp(x)}{dx} = n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 \in \mathbf{F}[x]$$

is the formal derivative.]

Ex. Recall the previous example, where

$$p(x) = (x - \overline{1})^2 \underbrace{(x^3 + x + \overline{1})}_{\text{Call this } q(x)} \in \mathbf{Z}_2[x].$$

Then the multiplicity of of the root $\overline{1}$ is 2, since $q(\overline{1}) \neq \overline{0}$.

Claim. Let $\mathbf{A}$ be an integral domain, and $p(x) \in \mathbf{A}[x]$ a polynomial of degree $d \geq 0$. Then $p(x)$ has at most d roots in $\mathbf{A}$ (including multiplicity as a polynomial in $\mathbf{K}[x]$, where $\mathbf{K} = \text{Quot}(\mathbf{A})$).

Ex. $p(x) = (x-1)(x^2-1) = (x-1)(x-1)(x+1) = (x-1)^2(x+1) \in \mathbf{Z}[x]$. $\deg p(x) = 3$, with roots 1 (multiplicity 2) and -1 (multiplicity 1). Thus 3 roots in $\mathbf{Z}$, including multiplicity.

Ex. $p(x) = 2x - 1 \in \mathbf{Z}[x]$. Then $\deg p(x) = 1$, and yet $p(x)$ has no root in $\mathbf{Z}$. [Note however that $p(x)$ has a root in $\mathbf{Q}$.]

Ex. $p(x) = (x-1)(x^2+1) \in \mathbf{R}[x]$. $\deg p(x) = 3$, and yet $p(x)$ has only 1 root in $\mathbf{R}$. Note that as a polynomial over $\mathbf{C}$, $p(x) = (x-1)(x-\sqrt{-1})(x+\sqrt{-1}) \in \mathbf{C}[x]$ has 3 roots in $\mathbf{C}$.

Reason for the claim: We will argue by induction on $\deg p(x) \geq 0$. Observe that $\deg p(x) = 0 \Rightarrow 0 \neq p(x) \in \mathbf{A}$, hence 0 roots. Also recall that if $\deg p(x) = 1$, then $p(x)$ has at most 1 root in $\mathbf{A}$. [Recall that in this case, $\deg p(x) = 1 \Rightarrow p(x)$ has exactly 1 root in $\mathbf{K} := \text{Quot}(\mathbf{A})$.] We now assume that $\deg p(x) = d \geq 2$ and that the claim holds for all polynomials of degree $< d$. Note that $\mathbf{A}[x] \subset \mathbf{K}[x]$, so that if we show that $p(x)$ has at most d roots in $\mathbf{K}$, then clearly it has at most d roots in $\mathbf{A}$. Thus we may assume that $\mathbf{A} = \mathbf{K}$ is a field, with $p(x) \in \mathbf{K}[x]$ of degree $d \geq 2$. If $p(x)$ has no roots in $\mathbf{K}$, then we're done. So assume $p(r_1) = 0$ for some $r_1 \in \mathbf{K}$. Therefore $(x - r_1)$ is a factor of $p(x)$ in $\mathbf{K}[x]$, i.e. $p(x) = (x - r_1) \cdot q(x)$, where $q(x) \in \mathbf{K}[x]$ has degree $= d - 1$. By induction on d, $q(x)$ has at most $d - 1$ roots in $\mathbf{K}$, say $\{r_2, \ldots, r_k\}$ (including multiplicity), where $k \leq d$. Therefore $q(x) = (x - r_2) \cdots (x - r_k) \cdot h(x)$ for some $h(x) \in \mathbf{K}[x]$, where $h(x)$ has no roots in $\mathbf{K}$. Therefore $p(x) = (x - r_1)(x - r_2) \cdots (x - r_k) \cdot h(x)$; moreover, for $r \in \mathbf{K}$,

$$p(r) = 0 \Leftrightarrow (r - r_1) \cdots (r - r_k) \cdot \underbrace{h(r)}_{h(r) \neq 0} = 0 \Leftrightarrow (r - r_j) = 0 \text{ for some } 1 \leq j \leq k.$$

Thus $\{r_1, \ldots, r_k\}$ are precisely the roots of $p(x)$ in $\mathbf{K}$, and hence $p(x)$ has $k \leq d$ roots in $\mathbf{K}$ (including multiplicity).

Ex. The above claim requires $\mathbf{A}$ to be an integral domain. For example, consider $p(x) = x^3 - x \in \mathbf{Z}_8[x]$. Then $p(x)$ has 5 roots in $\mathbf{Z}_8$, namely $\{\overline{0}, \overline{1}, \overline{3}, \overline{5}, \overline{7}\}$, and yet $\deg p(x) = 3$. Note that $\mathbf{Z}_8$ is not an integral domain.

We now reformulate the earlier statement of the Fundamental Theorem of Algebra, which says that $\mathbf{C}$ is algebraically closed, namely:

Theorem. Let $p(x) \in \mathbf{C}[x]$ be a polynomial of degree $d \geq 1$. Then $p(x)$ can be factored in a unique way:

$$p(x) = c(x - r_1) \cdots (x - r_d),$$

where $c, r_1, \ldots, r_d \in \mathbf{C}$, and $c \neq 0$.

The following picture is what we have in mind to work out for $\mathbf{F}[x]$, where $\mathbf{F}$ is a field,

and to illustrate the analogy betwen $\mathbf{Z}$ and $\mathbf{F}[x]$.

$\mathbf{Z}$	$\mathbf{F}[x]$
$\mathrm{Quot}(\mathbf{Z}) = \mathbf{Q}$, $\begin{bmatrix}\text{Rational}\\ \text{Numbers}\end{bmatrix}$	$\mathrm{Quot}(\mathbf{F}[x]) = \mathbf{F}(x) = \frac{\text{Polynomial}}{\text{Polynomial} \neq 0}$, $\begin{bmatrix}\text{Rational}\\ \text{Functions}\end{bmatrix}$
Integral Domain	Integral Domain
Euclidean Division	Euclidean Division
Primes = Irreducibles	Primes = Irreducibles $(\star)$
PID = Principal Ideal Domain	Principal Ideal Domain $(\star)$
Existence of GCD's	Existence of GCD's $(\star)$
Fundamental Theorem of Arithmetic	Fundamental Theorem of Arithmetic $(\star)$

[The items marked with a $(\star)$ is what we have yet to work out.]

Definition. (i) Let $f(x),\ g(x) \in \mathbf{F}[x]$ be given. We say that f divides g (or f is a factor of g), and write it as $f|g$, if $g(x) = q(x) \cdot f(x)$ for some $q(x) \in \mathbf{F}[x]$.

(ii) Assume given $f(x),\ g(x) \in \mathbf{F}[x]$, not both zero. $d(x) \in \mathbf{F}[x]$ is said to be a <u>common divisor</u> of f and g, if $d|f$ and $d|g$.

(iii) A common divisor $d(x)$ of f and g is said to be the Greatest Common Divisor (GCD) of f & g if whenever d_1 is a common divisor of f and g, then $d_1|d$. [Notation $d = \mathrm{GCD}(f, g) = (f, g)$.]

Claim. Let $d = (f, g)$. Then d is unique up to mutiplication by a unit in $\mathbf{F}[x]$. <u>Restatement</u>: Suppose that d_1 is also a GCD of f and g. Then $d = cd_1$ for some non-zero $c \in \mathbf{F}$.

<u>Reason</u>: By definition of GCD's, we have that $d|d_1$ and $d_1|d$. That is, $u_1 \cdot d = d_1$ and $u_2 \cdot d_1 = d$, for some $u_1, u_2 \in \mathbf{F}[x]$. Therefore $(u_1u_2) \cdot d = d$, i.e. $u_1 \cdot u_2 = 1$. This implies that $u_1, u_2 \in \mathbf{F}[x]^* = \mathbf{F}^*$, and we're done.

Claim. For any pair f & $g \in \mathbf{F}[x]$, not both zero, $d = \mathrm{GCD}(f, g)$ exists.

<u>Reason</u>: This will be established in three steps, paralleling the situation for the integers. As before, we first introduce the concept of an ideal.

<u>Step I</u>. **Definition.** A subset $\mathcal{U} \subset \mathbf{F}[x]$ is called an <u>ideal</u> if:

(i) $a, b \in \mathcal{U} \Rightarrow a + b \in \mathcal{U}$, [i.e. $\mathcal{U}$ is closed under $+$ from $\mathbf{F}[x]$].

(ii) $a \in \mathcal{U},\ b \in \mathbf{F}[x] \Rightarrow ba \in \mathcal{U}$, [i.e. $\mathcal{U}$ is closed under scalar multiplication from $\mathbf{F}[x]$].

Picture:

$$\text{(i)}\quad \begin{array}{ccc} \mathcal{U}\times\mathcal{U} & \stackrel{+}{\to} & \mathcal{U} \\ \cap\ \ \cap & & \cap \\ \mathbf{F}[x]\times\mathbf{F}[x] & \stackrel{+}{\to} & \mathbf{F}[x] \end{array} \qquad \text{(ii)}\quad \begin{array}{ccc} \mathbf{F}[x]\times\mathcal{U} & \stackrel{\bullet}{\to} & \mathcal{U} \\ \cap\ \ \cap & & \cap \\ \mathbf{F}[x]\times\mathbf{F}[x] & \stackrel{\bullet}{\to} & \mathbf{F}[x] \end{array}$$

Examples of Ideals.

(1) Fix an $h(x) \in \mathbf{F}[x]$, and set $\mathcal{U} = (h) := h\mathbf{F}[x] = \{h \cdot q \mid q \in \mathbf{F}[x]\}$. For example, $(1) = \mathbf{F}[x]$, $(0) = 0$. Also, if $c \in (\mathbf{F}[x])^* = \mathbf{F}^*$, then $(c) = \mathbf{F}[x]$. It is easy to see that $\mathcal{U}$ is an ideal. [Details: Let $f_1 = q_1 \cdot h,\ f_2 = q_2 \cdot h \in \mathcal{U},\ g \in \mathbf{F}[x]$ be given. Then $f_1 + f_2 = (q_1 + q_2) \cdot h \in \mathcal{U}$, and $g \cdot f_1 = (g \cdot q_1) \cdot h \in \mathcal{U}$.]

(2) Let $f,\ g \in \mathbf{F}[x]$ be given as in the claim. Then $\mathcal{U}_0 := \{q \cdot f + k \cdot g \mid q, k \in \mathbf{F}[x]\}$ is an ideal. [Details: Let $f_1 = q_1 \cdot f + k_1 \cdot g,\ f_2 = q_2 \cdot f + k_2 \cdot g \in \mathcal{U}_0,\ h \in \mathbf{F}[x]$ be given. Then $f_1 + f_2 = (q_1 + q_2) \cdot f + (k_1 + k_2) \cdot g \in \mathcal{U}_0$, and $h \cdot f_1 = (h \cdot q_1) \cdot f + (h \cdot k_1) \cdot g \in \mathcal{U}_0$.] Note that $f = 1 \cdot f + 0 \cdot g \in \mathcal{U}_0$, and likewise $g = 0 \cdot f + 1 \cdot g \in \mathcal{U}_0$.

Definition. An ideal $\mathcal{U} \subset \mathbf{F}[x]$ is said to be principal, if $\mathcal{U} = (h)$ for some fixed $h \in \mathbf{F}[x]$.

Step II. **Claim.** Every ideal $\mathcal{U} \subset \mathbf{F}[x]$ is principal. [In this case we call $\mathbf{F}[x]$ a PID (= a Principal Ideal Domain).]

Reason: Let $\mathcal{U} \subset \mathbf{F}[x]$ be any ideal. We might as well assume that $\mathcal{U} \neq (0)$ and $\mathcal{U} \neq (1)$, since $(0),\ (1)$ are principal. Since $\mathcal{U} \neq (0)$, it follows that there exists a non-zero $h \in \mathcal{U}$ of smallest degree. Thus $\deg h \geq 0$; moreover $\deg h = 0 \Leftrightarrow h \in \mathbf{F}^* \Leftrightarrow (h) = (1)$. Thus it is clear that $\deg h \geq 1$. We want to show that $\mathcal{U} = (h)$. To see this, let $f \in \mathcal{U}$ be given. Then by Euclid's Division Algorithm, $f = qh + r$, for some $q, r, \in \mathbf{F}[x]$, and where $\deg r < \deg h$. Thus $r = f - q \cdot h = f + (-q) \cdot h \in \mathcal{U}$, i.e. $r \in \mathcal{U}$. But if $\deg r \geq 0$ then $r \in \mathcal{U}$ and $\deg r < \deg h$, which is impossible by definition of the "smallest degree" h. Therefore $r = 0$, i.e. $f = q \cdot h \in (h)$. Since f is any given element of $\mathcal{U}$, it follows that $\mathcal{U} \subset (h)$. However, $(h) \subset \mathcal{U}$, by definition of an ideal. Hence $\mathcal{U} = (h)$, and we're done.

Step III. Conclusion of the proof of the existence of $d = (f, g)$.

First, recall that f & g are not both zero. Recall the ideal

$$\mathcal{U}_0 = \{q \cdot f + k \cdot g \mid q, k \in \mathbf{F}[x]\},$$

and further recall that $f, g \in \mathcal{U}_0$. Thus $\mathcal{U}_0 \neq (0)$, and hence by Step II, $\mathcal{U}_0 = (d)$ for some $d \in \mathbf{F}[x]$ with $d \neq 0$. We want to show that $d = (f, g)$. But since $f, g \in \mathcal{U}_0 = (d)$, it follows that $f = d \cdot \ell_1$ and $g = d \cdot \ell_2$ for some $\ell_1, \ell_2 \in \mathbf{F}[x]$. That is, $d|f$ & $d|g$. Next, since $d = d \cdot 1 \in \mathcal{U}_0 = \{q \cdot f + k \cdot g \mid q, k \in \mathbf{F}[x]\}$, it follows that $d = q_0 \cdot f + k_0 \cdot g$ for some

$q_0, k_0 \in \mathbf{F}[x]$. Now suppose $d_1|f$ & $d_1|g$, for some $d_1 \in \mathbf{F}[x]$, i.e. $k_1 \cdot d_1 = f$ & $k_2 \cdot d_1 = g$, for some $k_1, k_2 \in \mathbf{F}[x]$. Then $d = q_0 \cdot f + k_0 \cdot g = (k_1 q_0 + k_2 k_0) \cdot d_1$. Hence $d_1|d$. Therefore by definition of GCD, $d = (f, g)$, and we're done.

Summary. Given $f, g \in \mathbf{F}[x]$, not both zero, then $d = (f, g) \in \mathbf{F}[x]$ exists and is unique up to multiplication by a unit; moreover $d = q_0 \cdot f + k_0 \cdot g$, for some $q_0, k_0 \in \mathbf{F}[x]$.

Definition. $f,\ g \in \mathbf{F}[x]$, both not zero, are said to be relatively prime if $(f, g) = 1$.

Ex. In $\mathbf{Q}[x]$, or $\mathbf{R}[x]$ or $\mathbf{C}[x]$, $f := x + 1,\ g := x^2 + 1$ are relatively prime. This can easily be deduced from the fact that

$$1 = \frac{1}{2}(x^2 + 1) \ - \ \frac{(x-1)}{2} \cdot (x + 1).$$

[Another approach to this is to use an analogue of the Fundamental Theorem of Arithmetic for $\mathbf{F}[x]$, to be discussed shortly. Note that in $\mathbf{C}[x]$, $x^2 + 1 = (x + \sqrt{-1})(x - \sqrt{-1})$, and that $x + 1$, $x + \sqrt{-1}$ and $x - \sqrt{-1}$ are distinct primes (irreducibles).]

We defined the concept of an ideal in the special cases where the rings in question were $\mathbf{Z}$ and $\mathbf{F}[x]$. The definition of an ideal for a general ring $\mathbf{A}$ requires a little more care:

Definition. Let $\mathbf{A}$ be a ring. A *subring* $\mathcal{U} \subset \mathbf{A}$ is called an ideal if $\mathbf{A} \bullet \mathcal{U} \subset \mathcal{U}$, i.e. for any $a \in \mathbf{A}$, and $b \in \mathcal{U}$, the product $a \cdot b \in \mathcal{U}$.

Exercise. Let $\mathbf{A}$ be a ring, and fix $a \in \mathbf{A}$. Show that $(a) := \{b \cdot a \mid b \in \mathbf{A}\}$ is an ideal in $\mathbf{A}$.

How does this definition compare with the earlier definitions of an ideal in the case where $\mathbf{A} = \mathbf{Z}$ or $\mathbf{F}[x]$? The answer is given by:

Claim. Suppose that the ring $\mathbf{A}$ has unity $1 \in \mathbf{A}$. Then a subset $\mathcal{U} \subset \mathbf{A}$ is an ideal if either of the two equivalent statements hold:

1) $\mathcal{U} \subset \mathbf{A}$ is a subring and $\mathbf{A} \bullet \mathcal{U} \subset \mathcal{U}$.

2) $x,\ y \in \mathcal{U}$ and $z \in \mathbf{A} \Rightarrow x + y,\ z \cdot x \in \mathcal{U}$.

Reason: It is clear that 1) $\Rightarrow$ 2). Conversely, if $\mathcal{U}$ satisfies 2), then we must show that $\mathcal{U} \subset \mathbf{A}$ is a subring. Going through the properties required of a subring, the bottom line is to show the existence of additive inverses. This is easy, since $\pm 1 \in \mathbf{A}$, hence for any $x \in \mathcal{U}$, $-x = (-1) \cdot x \in \mathcal{U}$. This establishes the claim.

Now based on our understanding of ideals in the integral domains $\mathbf{Z}$ and $\mathbf{F}[x]$, we now introduce:

Definition. Let $\mathbf{A}$ be an integral domain. Then $\mathbf{A}$ is called a Principal Ideal Domain, or PID for short, if every ideal $\mathcal{U} \subset \mathbf{A}$ is principal, i.e. $\mathcal{U} = (a)$ for some $a \in \mathbf{A}$.

Ex. $\mathbf{Z}$ and $\mathbf{F}[x]$ are PID's.

For the next definition, we need the following notation. Let $\mathbf{A}$ be a ring, and assume given $a, b \in \mathbf{A}$. We say that a divides b, denoted by $a|b$, if $a \cdot c = b$ for some $c \in \mathbf{A}$.

Definition. Let $\mathbf{A}$ be an integral domain.

1) An element $a \in \mathbf{A}$, $a \notin \mathbf{A}^*$, $a \neq 0$ is said to be <u>irreducible</u>, if whenever $a = uv$ for some $u, v \in \mathbf{A}$, then either $u \subset \mathbf{A}^*$ or $v \in \mathbf{A}^*$.

2) An element $p \in \mathbf{A}$, $p \notin \mathbf{A}^*$, $p \neq 0$, is said to be <u>prime</u> if whenever $p|(ab)$, then either $p|a$ or $p|b$.

The following definition is a generalization of the statement of the Fundamental Theorem of Arithmetic for integral domains.

Definition. Let $\mathbf{A}$ be an integral domain. Then $\mathbf{A}$ is called a Unique Factorization Domain (UFD) if, for any given non-zero $a \in \mathbf{A}$ with $a \notin \mathbf{A}^*$, a can be factored in the form:

$$a = b_1^{\ell_1} \cdots b_N^{\ell_N},$$

where $\{b_1, \ldots, b_N\}$ are distinct[†] irreducible elements of $\mathbf{A}$ and $\ell_1, \ldots, \ell_N \in \mathbf{N}$. Moreover, this decomposition is required to be unique, in the sense that if we also have $a = q_1^{k_1} \cdots q_r^{k_r}$, where $\{q_1, \ldots, q_r\}$ are distinct irreducibles and $k_1, \ldots, k_r \in \mathbf{N}$, then $r = N$, and up to relabelling, $q_1 = (\text{unit}) \cdot b_1, \ldots, q_N = (\text{unit}) \cdot b_N$, and $k_1 = \ell_1, \ldots, k_N = \ell_N$.

Ex. $\mathbf{Z}$ is a UFD.

Theorem. Any PID is a UFD. (Proof Later.) Thus for example, $\mathbf{F}[x]$ is a UFD.

We will first give a direct argument as to why $\mathbf{F}[x]$ is a UFD, based on a similar argument for $\mathbf{Z}$. We first observe the following:

Claim. An element $h \in \mathbf{F}[x]$ is prime $\Leftrightarrow$ it is irreducible.

<u>Reason</u>: Let us first assume that h is prime, and that $h = u \cdot v$, $u, v \in \mathbf{F}[x]$. Then $h|(u \cdot v) \Rightarrow h|u$ or $h|v$. If for example, $h|u$, then $h \cdot k = u$ for some $k \in \mathbf{F}[x]$. Therefore $h = u \cdot v = h \cdot k \cdot v$. Hence $k \cdot v = 1$, hence $v \in (\mathbf{F}[x])^*$. Therefore h prime $\Rightarrow h$ is irreducible. Conversely, suppose that h is irreducible, and that $h|(a \cdot b)$, $a, b \in \mathbf{F}[x]$. If $h|a$ then we're done. So we may assume that $h \not| a$. Let $d = (h, a)$. Then $d|h$ and h irreducible $\Rightarrow$ (up to $\times$ (unit), either $d = h$ or $d = 1$. But $d = h \Rightarrow h|a$, which is not the case. Therefore

[†] I.e. $b_i \neq (\text{unit}) \cdot b_j$ for $i \neq j$.

$d = 1$, hence $1 = k_1 \cdot h + k_2 \cdot a$, for some $k_1, k_2 \in \mathbf{F}[x]$. Thus multiplication by b gives $b = b \cdot k_1 \cdot h + k_2 \cdot a \cdot b$. But $h | \big(b \cdot k_1 \cdot h + k_2 \cdot a \cdot b\big)$, hence $h|b$, and we're done.

Theorem. $\mathbf{F}[x]$ is a UFD.

Reason: If we go back to the proof of the similar statement for $\mathbf{Z}$ (Fundamental Theorem of Arithmetic), one can see that the uniqueness statement hinges on showing that prime is the same as irreducible, and that the proof of uniqueness for an irreducible decomposition in $\mathbf{F}[x]$ is essentually the same for the uniquess of a prime decomposition in $\mathbf{Z}$. Since we have verified that this is the case for $\mathbf{F}[x]$, viz. prime = irreducible, we need only verify the existence of an irreducible decomposition. Let $f \in \mathbf{F}[x]$ be nonconstant (i.e. $f \notin \mathbf{F}$; equivalently, $f \neq 0$, and is not a unit; or equivalently, $\deg f \geq 1$). If $\deg f = 1$, then f is irreducible, hence equal to its own irreducible decomposition. Therefore we may assume $d = \deg f \geq 2$, and proceed by induction by assuming the existence of an irreducible decomposition for polynomials of degree $\leq d - 1$. So given f of degree $d \geq 2$, either f is irreducible (hence it is equal to its own irreducible decomposition), or $f = g \cdot h$, where $\deg g,\ \deg h \leq d - 1$. But by induction, g and h have irreducible decompositions, hence so does f. Thus $\mathbf{F}[x]$ is a UFD.

Another reason why $\mathbf{Z}$ and $\mathbf{F}[x]$ are UFD's, is from the following:

Theorem. PID $\Rightarrow$ UFD.

Warning. There are examples of UFD's that are not PID's. [For example, the polynomial ring in two variables: $\mathbf{F}[x, y]$. More on this later.]

Reason for the Theorem: This will involve four steps.

Step I. Let $\mathbf{A}$ be an integral domain. Then $(a) = (b) \Leftrightarrow a = u \cdot b$, where $u \in \mathbf{A}^*$. [Reason: If $(a) = (b)$, then $a = a \cdot 1 \in (a) = (b)$ and $b = b \cdot 1 \in (b) = (a)$. Thus $a = u \cdot b$ and $b = v \cdot a$ for some $u, v \in \mathbf{A}$. Thus $a = (u \cdot v) \cdot a$. Note that either a, b are both zero, or both non-zero. If $a = b = 0$ then $a = (\text{unit}) \cdot b$. So assume $a, b \neq 0$. Then $u \cdot v = 1$, hence $u, v \in \mathbf{A}^*$, and hence $a = (\text{unit}) \cdot b$. Conversely, if $a = (\text{unit}) \cdot b$, then it is an easy exercise to show that $(a) = (b)$.]

Step II. Now assume that $\mathbf{A}$ is a PID, and suppose that we are given an ascending "chain" of ideals in $\mathbf{A}$ of the form:

$$\mathcal{U}_1 \subset \mathcal{U}_2 \subset \mathcal{U}_3 \subset \cdots \subset \mathcal{U}_n \subset \mathcal{U}_{n+1} \subset \cdots \subset \mathbf{A}.$$

Then for some $N \in \mathbf{N}$, we have $\mathcal{U}_N = \mathcal{U}_{N+1} = \mathcal{U}_{N+2} = \cdots$, i.e. the chain stabilizes. [$\mathbf{A}$ is an example of a Noetherian ring.] [Reason: Put $\mathcal{U} = \bigcup_{n \in \mathbf{N}} \mathcal{U}_n \subset \mathbf{A}$. Then it is an easy exercise to verify that $\mathcal{U}$ is an ideal in $\mathbf{A}$. But since $\mathbf{A}$ is a PID, we must have that $\mathcal{U} = (b)$ for some $b \in \mathbf{A}$. Thus $b = b \cdot 1 \in (b) = \mathcal{U} = \bigcup_{n \in \mathbf{N}} \mathcal{U}_n$, and hence $b \in \mathcal{U}_N$ for some $N \in \mathbf{N}$.

Thus $\mathcal{U} = (b) \subset \mathcal{U}_N \subset \mathcal{U}$, hence $\mathcal{U}_N = \mathcal{U}$. Hence $\mathcal{U}_N \subset \mathcal{U}_{N+1} \subset \mathcal{U}_{N+2} \subset \cdots \subset \mathcal{U} \Rightarrow \mathcal{U}_N = \mathcal{U}_{N+1} = \mathcal{U}_{N+2} = \cdots$.]

Ex. In $\mathbf{Z}$, $(0) \subset (p) \subset (1) = \mathbf{Z}$ is a chain of ideals.

Step III. *Existence of an Irreducible Decomposition.*

Now assume that $\mathbf{A}$ is a PID, and let $a \in \mathbf{A}$ be given with $a \neq 0$ and $a \notin \mathbf{A}^*$.

Claim. Can write $a = b_1 \cdots b_m$, where $b_1, \ldots, b_m$ are irreducible, (but not necessarily distinct).

Reason: Let us assume to the contrary that such a decomposition doesn't exist. Then we can assume this situation:

$$\begin{array}{cccc} a & = & a_1 \cdot b_1 & a_1, b_1 \notin \mathbf{A}^* \\ b_1 & = & a_2 \cdot b_2 & a_2, b_2 \notin \mathbf{A}^* \\ b_2 & = & a_3 \cdot b_3 & a_3, b_3 \notin \mathbf{A}^* \\ b_3 & = & a_4 \cdot b_4 & a_4, b_4 \notin \mathbf{A}^* \\ \& & \text{so} & \text{on} \ldots \end{array}$$

Then we arrive at a chain of ideals that never stabilizes, viz.:

$$(a) \underset{\neq}{\subset} (b_1) \underset{\neq}{\subset} (b_2) \underset{\neq}{\subset} (b_3) \underset{\neq}{\subset} \cdots$$

This obviously violates the result in Step II. Hence we arrive at an irreducible decomposition $a = b_1 \cdots b_m$ as claimed.

Step IV. *Uniqueness of the Irreducible Decomposition*

Everything hinges on showing that prime = irreducible for a PID $\mathbf{A}$. It is an easy exercise to show that prime $\Rightarrow$ irreducible[†]. We will show that irreducible $\Rightarrow$ prime. Let $p \in \mathbf{A}$ be irreducible, and assume that $p|(a \cdot b)$ for some $a, b \in \mathbf{A}$. We can assume that $p \not| a$, otherwise we're done. Consider the ideal $\mathcal{U} := \{x \cdot p + y \cdot a \mid x, y \in \mathbf{A}\}$. Since $\mathbf{A}$ is a PID, it follows that $\mathcal{U} = (d) := \{k \cdot d \mid k \in \mathbf{A}\}$, for some $d \in \mathbf{A}$. Note that $p = 1 \cdot p + 0 \cdot a \in \mathcal{U}$, and $a = 0 \cdot p + 1 \cdot a \in \mathcal{U}$. Further, since $\mathcal{U} = (d)$, it follows that $d|p$ and $d|a$. Thus $d \cdot e = p$ for some $e \in \mathbf{A}$; moreover p irreducible $\Rightarrow$ either $d \in \mathbf{A}^*$ or $e \in \mathbf{A}^*$. If $e \in \mathbf{A}^*$, then $d = e^{-1} \cdot p$. Hence $d|a \Rightarrow (e^{-1} \cdot p)|a \Rightarrow p|a$, which is not the case. Therefore $d \in \mathbf{A}^*$. Note that $d = x_0 \cdot p + y_0 \cdot a$ for some $x_0, y_0 \in \mathbf{A}$. Hence

$$1 = \big(\underbrace{d^{-1} \cdot x_0}_{x_1}\big) \cdot p + \big(\underbrace{d^{-1} \cdot y_0}_{y_1}\big) \cdot a \quad = \quad x_1 \cdot p + y_1 \cdot a, \quad x_1, y_1 \in \mathbf{A}.$$

[†] Let $p \in \mathbf{A}$ be prime, and suppose $p = u \cdot v$, for some $u, v \in \mathbf{A}$. Then $p = u \cdot v \Rightarrow p|(u \cdot v) \Rightarrow p|u$ or $p|v$. If $p|u$ say, then $p \cdot e = u$, thus $p = u \cdot v = p \cdot e \cdot v$. Thus $e \cdot v = 1, \Rightarrow e, v \in \mathbf{A}^*$. In particular $p = u \cdot v$ where $v \in \mathbf{A}^*$. Thus p is irreducible.

Now multiply both sides by b, viz.:

$$b = x_1 \cdot p \cdot b + y_1 \cdot (a \cdot b).$$

But $p|(a \cdot b)$ and $p|(x_1 \cdot p \cdot b) \Rightarrow p|\big(x_1 \cdot p \cdot b + y_1 \cdot (a \cdot b)\big)$, i.e. $p|b$, and we're done.

Ex. We give an example of an integral domain that is not a UFD (hence not a PID). Let $\mathbf{A} = \{a + b\sqrt{-5} \mid a, b \in \mathbf{Z}\}$. One can easily verify that $\mathbf{A}$ is a subring of $\mathbf{C}$, hence $\mathbf{A}$ must be an integral domain. However, it is easy to show that $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are irreducible elements[†] in $\mathbf{A}$, and that:

$$2 \cdot 3 = 6 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$$

gives two different irreducible decompositions of 6. Hence $\mathbf{A}$ is not a UFD.

Exercise. Let $\mathbf{A}$ be a UFD, $K = \mathrm{Quot}(\mathbf{A})$ and $p(x) \in \mathbf{A}[x]$ a monic polynomial. Show that any $\mathbf{K}$-root of $p(x)$ must be an $\mathbf{A}$-root.

[†] For $z \in \mathbf{A}$, consider the norm $N(z) = z\overline{z}$. Then $N(z) \geq 0$ is an integer; moreover $N(z) = 1 \Leftrightarrow z \in \mathbf{A}^* \Leftrightarrow z = \pm 1$. Further, $N(z) < 5 \Rightarrow z \in \mathbf{Z}$. So for example, $z \cdot w = 2 \Rightarrow N(z)N(w) = N(z \cdot w) = N(2) = 4$, hence $z, w \in \mathbf{Z}$, and therefore either $z = \pm 1$ or $w = \pm 1$. Thus $2 \in \mathbf{A}$ is irreducible. A similar story holds for $3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$.

Appendix: Gauss's Lemma

We prove in this section that $\mathbf{Z}[x]$ is a UFD, and more generally, if $\mathbf{A}$ is a UFD then $\mathbf{A}[x]$ is a UFD. This is a consequence of Gauss's Lemma. For example, as a consequence, we know that $\mathbf{F}[x]$ being a UFD $\Rightarrow \mathbf{F}[x,y] := \big(\mathbf{F}[x]\big)[y]$ is a UFD, where $\mathbf{F}[x,y]$ is the ring of polynomials in the variables x and y. Thus by induction the polymonial ring in n variables $\mathbf{F}[x_1,\ldots,x_n]$, is a UFD. For $n \geq 2$, one can argue that $\mathbf{F}[x_1,\ldots,x_n]$ is not a PID. For example the ideal $(x,y) := \{x\cdot f(x,y)+y\cdot g(x,y) \mid f,g \in \mathbf{F}[x,y]\}$ is not principal. Thus Gauss's Lemma also provides examples of UFD's that are not PID's.

Formulation of the Lemma

Let $\mathbf{A}$ be a UFD, and $\mathbf{K} = \mathrm{Quot}(\mathbf{A})$ be its quotient field. Fix an irreducible $p \in \mathbf{A}$. For any given non-zero $a \in \mathbf{A}$, we can write $a = p^\nu q$, where $q \in \mathbf{A}$, $\nu \geq 0$ is an integer, and where $(p,q) = 1$. Now let $b \in \mathbf{A}$ be also non-zero, and write $b = p^\mu k$, $(p,k) = 1$, μ an integer ≥ 0. Then $\frac{a}{b} = p^{\nu-\mu}\frac{q}{k}$, where p is relatively prime to both numerator q and denominator k, and where $\nu - \mu \in \mathbf{Z}$. Thus for any non-zero element $\xi \in \mathbf{K}$, we can write $\xi = p^\ell h$, where $\ell \in \mathbf{Z}$, $h \in \mathbf{K}$ and where p is relatively prime to both the numerator and denominator of h. Let $f(x) = a_n x^n + \cdots + a_0 \in \mathbf{K}[x]$ be a non-zero polynomial. We define the p-content of $f(x)$ by the prescription $c_p(f) = p^\nu$, where $\nu \in \mathbf{Z}$ is the *minimum* integer among the list $\{\nu_i \mid a_i \neq 0,\ a_i = p^{\nu_i}k_i$, where p is relatively prime to both numerator and denominator of $k_i \in \mathbf{K}\}$. We define the content of f to be

$$c(f) = \prod_{p \text{ irreducible}} c_p(f).$$

[Note that $c_p(f)$ and hence $c(f)$ are defined only up to multiplication by units in $\mathbf{A}$.]

Ex. Let $f(x) = \frac{1}{4}x^3 + 3x^2 + \frac{1}{6}x + 7 \in \mathbf{Q}[x]$. Then for any prime $p \in \mathbf{Z}$:

$$c_p(f) = \begin{cases} 1 & \text{if } p \neq 2,3 \\ \frac{1}{2^2} = \frac{1}{4} & \text{if } p = 2 \\ \frac{1}{3} & \text{if } p = 3 \end{cases}$$

Thus $c_p(f) = \frac{1}{4}\cdot\frac{1}{3} = \frac{1}{12}$. Note that $f = c_p(f)\cdot f_1$, where $f_1 = 12\cdot f = 3x^3+36x^2+2x+84 \in \mathbf{Z}[x]$, and where $c(f_1) = 1$.

It is reasonably obvious that for any non-zero $f \in \mathbf{K}[x]$, $f = c(f)\cdot f_1$, where $f_1 \in \mathbf{A}[x]$, and $c(f_1) = 1$. In fact, for any non-zero $h \in \mathbf{K}[x]$, $c(h) = 1 \Rightarrow h \in \mathbf{A}[x]$.

Gauss's Lemma. Let $f,g \in \mathbf{K}[x]$ be non-zero polynomials. Then $c(f\cdot g) = c(f)\cdot c(g)$.

Proof: Note that for any non-zero $a \in \mathbf{K}$ and non-zero $h \in \mathbf{K}[x]$, $c(a\cdot h) = a\cdot c(h)$. In particular, if we write $f = c(f)\cdot f_1$ and $g = c(g)\cdot g_1$, then $c(f\cdot g) = c(f)\cdot c(g) \Leftrightarrow c(f_1\cdot g_1) = 1$.

Thus we may assume that $c(f) = c(g) = 1$ (hence $f, g \in \mathbf{A}[x]$) and show that $c(f \cdot g) = 1$. Now write

$$f = a_n x^n + \cdots + a_0, \quad a_n \neq 0,\ a_0, \ldots, a_n \in \mathbf{A},$$

$$g = b_m x^m + \cdots + b_0, \quad b_m \neq 0, \quad b_0, \ldots, b_m \in \mathbf{A}.$$

It suffices to show that $c_p(f \cdot g) = 1$ for all irreducible $p \in \mathbf{A}$. Fix an irreducible $p \in \mathbf{A}$. Since $c_p(f) = c_p(g) = 1$, it follows that there is a smallest $0 \leq r \leq n$, $0 \leq s \leq m$ for which p is relatively prime to both a_r and b_s, i.e. $(p, a_r) = 1$ and $(p, b_s) = 1$, and yet $p | a_i$ for $i < r$ and $p | b_j$ for $j < s$. But in the product $f \cdot g$, the constant term in front of x^{r+s} is

$$\sum_{i+j=r+s} a_i b_j = \big(a_r b_s + [\sum_{i+j=r+s, i<r} a_i b_j \ + \sum_{i+j=r+s, j<s} a_i b_j]\big).$$

Note that $p \big| [\sum_{i+j=r+s, i<r} a_i b_j \ + \ \sum_{i+j=r+s, j<s} a_i b_j]$, hence $p \not\big| \big(\sum_{i+j=r+s} a_i b_j\big)$, otherwise $p | (a_r b_s)$, which implies that either $p | a_r$ or $p | b_s$. Thus $c(f \cdot g) = 1$.

Now let $f \in \mathbf{A}[x]$ be a non-constant polynomial. Then it is easy to see that $c(f) \in \mathbf{A}$, and that we can write

$$f = c(f) \cdot f_1 = p_1^{\ell_1} \cdots p_N^{\ell_N} h_1^{k_1} \cdots h_M^{k_M},$$

where $c(f) = p_1^{\ell_1} \cdots p_N^{\ell_N}$ is the irreducible decomposition in $\mathbf{A}$ of $c(f)$, $\{p_1, \ldots, p_N\}$ being distinct irreducibles (up to times a unit) in $\mathbf{A}$, $\ell_1, \ldots, \ell_n, k_1, \ldots, k_M \in \mathbf{N}$, $h_1, \ldots, h_M \in \mathbf{A}[x]$, $c(h_1) = \cdots = c(h_M) = 1$, $\{h_1, \ldots, h_M\}$ distinct irreducibles (up to times a unit) as elements in $\mathbf{K}[x]$. One can argue that this decomposition is unique, and hence $\mathbf{A}[x]$ is a UFD.

Ex. Recall, as a consequence, $\mathbf{Z}[x]$ is a UFD. We can factor for example $f = 12x^3 - 48x^2 + 6x + 36 \in \mathbf{Z}[x]$ into irreducibles as follows:

$$c_p(f) = \begin{cases} 1 & \text{if } p \neq 2, 3 \\ 2 & \text{if } p = 2 \\ 3 & \text{if } p = 3 \end{cases}$$

Thus $c(f) = 6$, and $f = 6 \cdot (2x^3 - 8x^2 + x + 6)$, where $c(2x^3 - 8x^2 + x + 6) = 1$. We wish to show that $2x^3 - 8x^2 + x + 6$ is irreducible in $\mathbf{Q}[x]$, and this amounts to showing that $2x^3 - 8x^2 + x + 6$ has no $\mathbf{Q}$-roots (being of degree 3). But the only candidates for $\mathbf{Q}$-roots are $\{\pm 1, \pm 2, \pm 3, \pm 6, \pm \frac{1}{2}, \pm \frac{3}{2}\}$, and none of these turn out to be roots of $2x^3 - 8x^2 + x + 6$. Thus

$$f = 2 \cdot 3 \cdot (2x^3 - 8x^2 + x + 6)$$

gives the irreducible decomposition of f in $\mathbf{Z}[x]$.

Ring Homomorphisms

Assume given rings $\mathbf{A}$, $\mathbf{B}$ with respective unities 1_A, 1_B. A ring homomorphism is a map $T : \mathbf{A} \to \mathbf{B}$ which satisfies the following: (Assume given any $a_1, a_2 \in \mathbf{A}$)

1) $T(a_1 + a_2) = T(a_1) + T(a_2)$,

2) $T(a_1 \cdot a_2) = T(a_1) \cdot T(a_2)$,

3) $T(1_A) = 1_B$.

Remarks. Let $T : \mathbf{A} \to \mathbf{B}$ be a ring homomorphism. Then:

(i) $T(0) = 0$. [Reason: $T(0) = T(0 + 0) = T(0) + T(0) \Rightarrow T(0) = 0$.]

(ii) For any $a, b \in \mathbf{A}$, $T(a-b) = T(a)-T(b)$. [Reason: First $0 = T(0) = T(b+(-b)) = T(b) + T(-b)$, hence $T(-b) = -T(b)$. Thus $T(a - b) = T(a + (-b)) = T(a) + T(-b) = T(a) - T(b)$.] Exercise: Show that $a \in \mathbf{A}^* \Rightarrow T(a) \in \mathbf{B}^*$.

(iii) The image of T, namely $\mathrm{Im}(T) = T(\mathbf{A}) := \{T(a) \mid a \in \mathbf{A}\}$, is a subring of $\mathbf{B}$. [This is an exercise for the reader.]

(iv) The kernel of T, defined by $\ker T = \{a \in \mathbf{A} \mid T(a) = 0\}$, is an ideal in $\mathbf{A}$. [This is an exercise for the reader.]

Ex. Consider the map $T : \mathbf{Z} \to \mathbf{Z}_n$ given by $T(m) = \overline{m} \in \mathbf{Z}_n$. Then $T(m_1 + m_2) = \overline{m_1 + m_2} = \overline{m}_1 + \overline{m}_2 = T(m_1) + T(m_2)$; $T(m_1 \cdot m_2) = \overline{m_1 \cdot m_2} = \overline{m}_1 \cdot \overline{m}_2 = T(m_1) \cdot T(m_2)$; $T(1) = \overline{1}$. Hence T is a ring homomorphism. Note that $\mathrm{Im}(T) = \mathbf{Z}_n$ and that $\ker T = \{m \in \mathbf{Z} \mid T(m) = \overline{0}\} = \{m \in \mathbf{Z} \mid n|m\} = (n)$.

Ex. Let $\mathbf{A} = \mathbf{Z}_2 = \{\overline{0}, \overline{1}\}$, $\mathbf{B} = 5\mathbf{Z}_{10} = \{\overline{0}, \overline{5}\}$. Recall that both $\mathbf{A}$ and $\mathbf{B}$ are fields. Consider the map $T : \mathbf{A} \to \mathbf{B}$ given by $T(\overline{0}) = \overline{0}$, $T(\overline{1}) = \overline{5}$. Then T is a ring homomorphism (in fact an isomorphism, as will be defined below). [Note that $\mathrm{Im}(T) = 5\mathbf{Z}_5$ and $\ker T = \overline{0}$.]

Ex. Let $\mathbf{A} = \mathbf{Q}[x]$, $\mathbf{B} = \mathbf{Q}$. Consider the map $T : \mathbf{Q}[x] \to \mathbf{Q}$ given by $T(p(x)) = p(1) \in \mathbf{Q}$. Then T is a ring homomorphism. [Reason: $T\big(f(x)+g(x)\big) = \big(f(x)+g(x)\big)(1) = f(1) + g(1) = T(f(x)) + T(g(x))$; $T\big(f(x) \cdot g(x)\big) = \big(f(x) \cdot g(x)\big)(1) = f(1) \cdot g(1) = T(f(x)) \cdot T(g(x))$; $T(1) = 1$.] Since $T(r) = r$ for all $r \in \mathbf{Q}$, it follows that $\mathrm{Im}(T) = \mathbf{Q}$. Note that $\ker T = \{p(x) \in \mathbf{Q}[x] \mid p(1) = 0\} = \{p(x) \in \mathbf{Q}[x] \mid (x-1)|p(x)\} = \{q(x) \cdot (x-1) \mid q(x) \in \mathbf{Q}[x]\} = \big((x-1)\big)$.

For the next example, we need the following result:

Claim. A ring $\mathbf{A}$ with unity $1 \neq 0$ is a field $\Leftrightarrow$ the only ideals in $\mathbf{A}$ are (0) and $(1) = \mathbf{A}$.

Reason: First, suppose $\mathbf{A}$ is a field, and $\mathcal{U} \neq (0)$ is an ideal. Then there is an $x \in \mathcal{U}$ such that $x \neq 0$. Since $\mathbf{A}$ is a field, it follows that $x^{-1} \in \mathbf{A}$, and therefore $1 = x^{-1} \cdot x \in \mathcal{U}$,

by definition of an ideal. Hence $\mathcal{U} = (1) = \mathbf{A}$. Conversely, suppose that the only ideals in $\mathbf{A}$ are (0) and $\mathbf{A}$, and let $x \in \mathbf{A}$ be given, with $x \neq 0$. The $(x) := \{y \cdot x \mid y \in \mathbf{A}\}$ is an ideal in $\mathbf{A}$. Since $x = 1 \cdot x \in (x)$, it follows that $(x) \neq (0)$. Thus $(x) = (1) = \mathbf{A}$. Hence $y \cdot x = 1$ for some $y \in \mathbf{A}$. Therefore $\mathbf{A}$ is a field.

Ex. Let $\mathbf{F}$ be a field, $\mathbf{B}$ a ring with unity $1 \neq 0$, and $T : \mathbf{F} \to \mathbf{B}$ a ring homomorphism. Then $\ker T = 0$. [Reason: Since $T(1) = 1$, it follows that $\ker T \neq \mathbf{F}$. Since $\ker T$ is an ideal in $\mathbf{F}$, it follows that $\ker T = (0) = 0$.]

Definition-Claim. Assume given $\mathbf{A}$, $\mathbf{B}$ rings with unity, and $T : \mathbf{A} \to \mathbf{B}$ a ring homomorphism. Then T is $1-1$ (or injective), if either of the two equivalent conditions hold:

1) $T(a) = T(b) \Rightarrow a = b$, $(a, b \in \mathbf{A})$.

2) $\ker T = 0$.

[Reason: This is based on the observation that $T(a) = T(b) \Leftrightarrow T(a) - T(b) = 0 \Leftrightarrow T(a-b) = 0 \Leftrightarrow a - b \in \ker T$.] The notation for a $1-1$ map is $T : \mathbf{A} \hookrightarrow \mathbf{B}$, or $T : \mathbf{A} >\!\!\to \mathbf{B}$.

Definition. A ring homomorphism $T : \mathbf{A} \to \mathbf{B}$ is onto (or surjective), if $\mathrm{Im}(T) = \mathbf{B}$. Notation: $T : \mathbf{A} \to\!\!> \mathbf{B}$.

Definition-Claim. A ring homomorphism $T : \mathbf{A} \to \mathbf{B}$ is said to be bijective (or an isomorphism) if either of the following two equivalent conditions hold:

1) T is $1-1$ and onto. [Written $T : \mathbf{A} >\!\!\to\!\!> \mathbf{B}$, or as in 2) below.]

2) There is a ring homomorphism $S : \mathbf{B} \to \mathbf{A}$ such that $T(S(b)) = b$ for all $b \in \mathbf{B}$ and $S(T(a)) = a$ for all $a \in \mathbf{A}$. [Written $T : \mathbf{A} \xrightarrow{\sim} \mathbf{B}$, or as in 1) above.]

[The equivalence of 1) and 2) is an exercise[†] for the reader.]

Ex. Any ring homomorphism $T : \mathbf{F} \to \mathbf{B}$, where $\mathbf{F}$ is a field, is injective.

Ex. A homomorphism $T : \mathbf{A} \to \mathbf{A}$ is called an endomorphism. An isomorphism $T : \mathbf{A} \xrightarrow{\sim} \mathbf{A}$ is called an automorphism.

Preimages of homomorphisms. Let $T : \mathbf{A} \to \mathbf{B}$ be a ring homomorphism. Let $\mathcal{U}_B$ be an ideal in $\mathbf{B}$, and put

$$\mathcal{U}_A = T^{-1}(\mathcal{U}_B) := \{a \in \mathbf{A} \mid T(a) \in \mathcal{U}_B\}.$$

[†] For example, assumimg 1), it is easy to construct $S : \mathbf{B} \to \mathbf{A}$, namely, for $b \in \mathbf{B}$, there exists a unique $a \in \mathbf{A}$ such that $T(a) = b$. Define $S(b) = a$. S is a homomorphism, since $T(1_A) = 1_B$ $(\Rightarrow S(1_B) = 1_A)$, and if $b_1 = T(a_1)$, $b_2 = T(a_2)$, then $T(a_1 + a_2) = T(a_1) + T(a_2) = b_1 + b_2$ and $T(a_1 \cdot a_2) = T(a_1) \cdot T(a_2) = b_1 \cdot b_2$. Thus $S(b_1 + b_2) = a_1 + a_2 = S(b_1) + S(b_2)$, $S(b_1 \cdot b_2) = a_1 \cdot a_2 = S(b_1) \cdot S(b_2)$.

Claim. $\mathcal{U}_A$ is an ideal in $\mathbf{A}$, called the inverse image ideal (of $\mathcal{U}_B$).

Reason: Since $\mathbf{A}$ (and $\mathbf{B}$) is a ring with unity, it suffices to show that for any $x, y \in \mathcal{U}_A$, and $z \in \mathbf{A}$, $x+y,\ z\cdot x \in \mathcal{U}_A$. But $T(x),\ T(y) \in \mathcal{U}_B$, hence $T(x+y) = T(x)+T(y) \in \mathcal{U}_B$, and $T(z\cdot x) = T(z)\cdot T(x) \in \mathcal{U}_B$. Thus $x+y,\ z\cdot x \in \mathcal{U}_A$.

Ex. Put $\mathcal{U}_B = (0) \subset \mathbf{B}$. Then $\mathcal{U}_A = \ker T$, hence $\ker T$ is an ideal in $\mathbf{A}$.

Quotient Rings

Given a ring $\mathbf{A}$ and an ideal $\mathcal{U} \subset \mathbf{A}$, we introduce a relation $\sim$ on $\mathbf{A}$ as follows:

$$a \sim b \Leftrightarrow a - b \in \mathcal{U}.$$

Claim. $\sim$ is an equivalence relation on $\mathbf{A}$.

Reason: First, $a - a = 0 \in \mathcal{U} \Rightarrow a \sim a$. Secondly $a \sim b \Leftrightarrow a - b \in \mathcal{U} \Rightarrow b - a = -(a-b) \in \mathcal{U} \Rightarrow b \sim a$. Thirdly, if $a \sim b$ and $b \sim c$, then $a-b,\ b-c \in \mathcal{U}$, hence $a - c = (a-b)+(b-c) \in \mathcal{U}$, i.e. $a \sim c$.

Definition-Claim. Let $\mathbf{A}$ be a ring and $\mathcal{U} \subset \mathbf{A}$ an ideal. The quotient ring of $\mathbf{A}$ by $\mathcal{U}$ is given by:

$$\mathbf{A}/\mathcal{U} = \{\overline{a} \mid a \in \mathbf{A} \ \&\ \text{where } \overline{a} = \overline{b} \Leftrightarrow a \sim b,\ \text{i.e. } a - b \in \mathcal{U}\},$$

and where $+, \bullet$ on $\mathbf{A}/\mathcal{U}$ is induced from the corresponding $+, \bullet$ on $\mathbf{A}$.

Ex. $\mathbf{A} = \mathbf{Z}$ and $\mathcal{U} = (n)$, for some given integer $n \geq 2$. Then $\mathbf{A}/\mathcal{U} = \mathbf{Z}/(n) = \mathbf{Z}_n$.

Ex. $\mathcal{U} = (0) \subset \mathbf{A}$. $\mathbf{A}/\mathcal{U} = \mathbf{A}/(0) = \mathbf{A}$.

Ex. $\mathcal{U} = \mathbf{A}$. $\mathbf{A}/\mathcal{U} = \mathbf{A}/\mathbf{A} = \{0\}$.

Details of the Claim: First observe that there is a map $\mathbf{A} \to \mathbf{A}/\mathcal{U}$, $a \mapsto \overline{a}$. The definition of $+, \bullet$ on $\mathbf{A}/\mathcal{U}$ is governed by the "commutative" diagram below:

$$\begin{array}{ccccc}
(x,y) & & \mapsto & & x+y,\ x\cdot y \\
 & \mathbf{A}\times\mathbf{A} & \xrightarrow{+,\bullet} & \mathbf{A} & \\
\downarrow & \downarrow & & \downarrow & \downarrow \\
 & \mathbf{A}/\mathcal{U}\times\mathbf{A}/\mathcal{U} & \xrightarrow{+,\bullet} & \mathbf{A}/\mathcal{U} & \\
(\overline{x},\overline{y}) & & \mapsto & & \overline{x+y},\ \overline{x\cdot y}
\end{array}$$

Namely $\overline{x} + \overline{y} := \overline{x+y}$, $\overline{x}\cdot\overline{y} := \overline{x\cdot y}$. We must verify that $+, \bullet$ on $\mathbf{A}/\mathcal{U}$ is well-defined. That is, if $\overline{x}_1 = \overline{x}_2$ and $\overline{y}_1 = \overline{y}_2$, then $\overline{x}_1 + \overline{y}_1 = \overline{x}_2 + \overline{y}_2$ and $\overline{x}_1 \cdot \overline{y}_1 = \overline{x}_2 \cdot \overline{y}_2$. Put more

explicitly, if $x_1 - x_2,\ y_1 - y_2 \in \mathcal{U}$, must show that $(x_1 + y_1) - (x_2 + y_2),\ x_1 \cdot y_1 - x_2 \cdot y_2 \in \mathcal{U}$. But

$$(x_1 + y_1) - (x_2 + y_2) = \underbrace{(x_1 - x_2)}_{\in \mathcal{U}} + \underbrace{(y_1 - y_2)}_{\in \mathcal{U}} \in \mathcal{U}.$$

Next, if $x_1 = x_2 + u$, $y_1 = y_2 + v$, for some $u, v \in \mathcal{U}$, then:

$$x_1 x_2 = x_2 y_2 + \underbrace{x_2 \cdot v + y_2 \cdot u + u \cdot v}_{\in \mathcal{U}}.$$

Therefore $x_1 y_1 - x_2 y_2 \in \mathcal{U}$. Next, since $+, \bullet$ on $\mathbf{A}/\mathcal{U}$ is induced from $+, \bullet$ on $\mathbf{A}$, it follows that the associative, commutative and distributive laws hold for $\mathbf{A}/\mathcal{U}$ (since they hold for $\mathbf{A}$). Likewise, we have $\overline{0}$ and additive inverses $-\overline{x} = \overline{(-x)}$. Thus $\mathbf{A}/\mathcal{U}$ is a ring. Note that if $\mathcal{U} \neq \mathbf{A}$, then $\mathbf{A}/\mathcal{U}$ is a ring with unity $\overline{1} \in \mathbf{A}$, provided that $\mathbf{A}$ has unity $1 \in \mathbf{A}$.

Remark. It is instructive to describe the equivalence relation for the ring $\mathbf{A}$ above (with ideal $\mathcal{U} \subset \mathbf{A}$) in terms of coset decompositions. Recall that $x \sim y \Leftrightarrow x - y \in \mathcal{U}$, equivalently, $x \in y + \mathcal{U} := \{y + u \mid u \in \mathcal{U}\}$. That is, $\{x \in \mathbf{A} \mid x \sim y\} = y + \mathcal{U}$. Note that for $x, y \in \mathbf{A}$, either $x + \mathcal{U} = y + \mathcal{U}$ (in which case $x \sim y$), or $\{x + \mathcal{U}\} \cap \{y + \mathcal{U}\} = \emptyset$ (in which case $x \not\sim y$). Moreover, for some subset $I \subset \mathbf{A}$:

$$\mathbf{A} = \bigcup_{x \in \mathbf{A}} \{x + \mathcal{U}\} = \coprod_{x \in I} \{x + \mathcal{U}\}.$$

Claim. Let $\mathbf{A}$ be a ring with unity $1 \in \mathbf{A}$, and $\mathcal{U} \subset \mathbf{A}$ an ideal such that $\mathcal{U} \neq \mathbf{A}$. Then the natural map $T : \mathbf{A} \to \mathbf{A}/\mathcal{U}$, given by $T(x) = \overline{x} \in \mathbf{A}/\mathcal{U}$ is a ring homomorphism; moreover $\ker T = \mathcal{U}$.

Reason: First of all, by definition $T(1) = \overline{1}$, i.e. T preserves unity. Next:

$$T(x + y) \stackrel{\text{def}}{=} \overline{x + y} = \overline{x} + \overline{y} \stackrel{\text{def}}{=} T(x) + T(y).$$

$$T(x \cdot y) \stackrel{\text{def}}{=} \overline{x \cdot y} = \overline{x} \cdot \overline{y} \stackrel{\text{def}}{=} = T(x) \cdot T(y).$$

Thus T is a ring homomorphism. The statement $\ker T = \mathcal{U}$ is easy to prove, and is left for the reader.

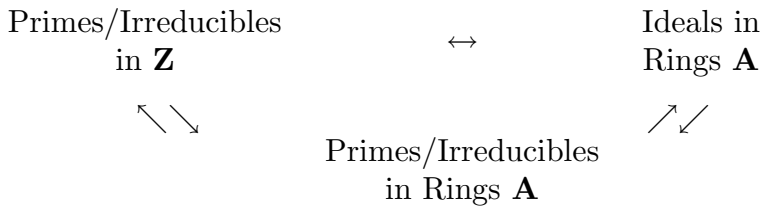
Exercise. Assume given a ring homomorphism $T : \mathbf{A} \to \mathbf{B}$. Show that T can be factored in the diagram below:

$$\begin{array}{ccc} \mathbf{A} & \stackrel{T}{\longrightarrow} & \mathbf{A} \\ (\text{onto}) \downarrow & & \uparrow (1-1) \\ \mathbf{A}/\ker T & \stackrel{\overline{T}}{\xrightarrow{\sim}} & \text{Im}(T), \end{array}$$

where $\overline{T}$ is an isomorphism.

From Primes to Ideals in Rings

We want to explain a natural progression from primes to ideals in rings, as indicated in the diagram below:



Definition-Claim. Let $\mathbf{A}$ be a ring with unity $1 \neq 0$. An ideal $\mathcal{P} \subset \mathbf{A}$ is said to be prime, if $\mathcal{P} \neq (1)$ and either of the two equivalent conditions hold:

1) $\mathbf{A}/\mathcal{P}$ is an integral domain.

2) Given $x, y \in \mathbf{A}$, then $x \cdot y \in \mathcal{P} \Rightarrow x \in \mathcal{P}$ or $y \in \mathcal{P}$.

Reason: [Note that $\overline{1} \neq \overline{0}$ in $\mathbf{A}/\mathcal{P} \Leftrightarrow \mathcal{P} \neq (1)$, which is the case for a prime ideal.] For $x \in \mathbf{A}$, let $\overline{x} \in \mathbf{A}/\mathcal{P}$ be the corresponding element. Lets assume that $\mathbf{A}/\mathcal{P}$ is an integral domain, and that $x, y \in \mathbf{A}$ are given such that $x \cdot y \in \mathcal{P}$. Then $\overline{0} = \overline{x \cdot y} = \overline{x} \cdot \overline{y}$. But

$$\overline{x} \cdot \overline{y} = \overline{0} \Rightarrow \overline{x} = \overline{0} \ (\Rightarrow x \in \mathcal{P}), \text{ or } \overline{y} = \overline{0} \ (\Rightarrow y \in \mathcal{P}).$$

Thus we have shown that 1) $\Rightarrow$ 2). Next, suppose that 2) holds and that $\overline{x} \cdot \overline{y} = \overline{0}$. Then $x \cdot y \in \mathcal{P}$. Thus either $x \in \mathcal{P} \ \Rightarrow \overline{x} = \overline{0}$ or $y \in \mathcal{P} \ \Rightarrow \overline{y} = \overline{0}$. Thus 2) $\Rightarrow$ 1), and we're done.

Ex. A. Let $\mathcal{U} \subset \mathbf{Z}$ be an ideal. Recall that $\mathcal{U} = (n)$ for some integer $n \geq 0$. Then $\mathcal{U}$ is prime $\Leftrightarrow$ either $n = 0$, or $n = p$ is prime. This is because $\mathbf{Z}/(0) = \mathbf{Z}$, and that for $n \geq 2$, $\mathbf{Z}_n$ is an integral domain $\Leftrightarrow n = p$ is prime.

Definition-Claim. Let $\mathbf{A}$ be a ring with unity $1 \neq 0$. An ideal $\mathcal{M} \subset \mathbf{A}$ is said to be maximal, if $\mathcal{M} \neq (1)$ and either of the two equivalent conditions hold:

1) $\mathbf{A}/\mathcal{M}$ is a field.

2) For any ideal $\mathcal{U} \subset \mathbf{A}$ with $\mathcal{M} \subset \mathcal{U}$, either $\mathcal{U} = \mathcal{M}$ or $\mathcal{U} = \mathbf{A}$.

Reason: [Note that $\overline{1} \neq \overline{0}$ in $\mathbf{A}/\mathcal{M} \Leftrightarrow \mathcal{M} \neq (1)$, which is the case for a maximal ideal.] Suppose that 1) holds and that $\mathcal{U}$ is an ideal with $\mathcal{M} \subset \mathcal{U}$, but $\mathcal{U} \neq \mathcal{M}$. Choose $x \in \mathcal{U}$ such that $x \notin \mathcal{M}$. Then $\overline{x} \neq \overline{0}$ in $\mathbf{A}/\mathcal{M}$. Thus there exists $\overline{y} \in \mathbf{A}/\mathcal{M}$ such that $\overline{y} \cdot \overline{x} = \overline{1} \in \mathbf{A}/\mathcal{M}$. This is the same as saying that $1 - y \cdot x \in \mathcal{M}$. Thus $1 \in y \cdot x + \mathcal{M} \subset \mathcal{U}$. Hence $\mathcal{U} = (1) = \mathbf{A}$. We have just shown that 1) $\Rightarrow$ 2). Conversely, suppose that 2) holds, and let $\overline{x} \in \mathbf{A}/\mathcal{M}$ be given such that $\overline{x} \neq \overline{0} \in \mathbf{A}/\mathcal{M}$ ($\Rightarrow x \notin \mathcal{M}$). Put $\mathcal{U} = \{y \cdot x + m \mid y \in \mathbf{A}, \ m \in \mathcal{M}\}$. Then one can easily verify that $\mathcal{U}$ is an ideal, with $\mathcal{M} \subset \mathcal{U}$ (since $0 \cdot x + m \in \mathcal{U}$ for all $m \in \mathcal{M}$),

and with $x = 1 \cdot x + 0 \in \mathcal{U}$. Thus $\mathcal{U} \neq \mathcal{M}$, and hence $\mathcal{U} = \mathbf{A}$. Therefore $1 = y \cdot x + m$ for some $y \in \mathbf{A}$ and $m \in \mathcal{M}$. Therefore modulo $\mathcal{M}$, $\overline{y} \cdot \overline{x} + \overline{m} = \overline{1} \in \mathbf{A}/\mathcal{M}$. But $\overline{m} = \overline{0}$ in $\mathbf{A}/\mathcal{M}$, hence $\overline{y} \cdot \overline{x} = \overline{1}$, i.e. $\mathbf{A}/\mathcal{M}$ is a field. Thus 2) $\Rightarrow$ 1), and we're done.

Remark. Since every field is an integral domain, it follows that any maximal ideal is prime. However, not every prime ideal is maximal. [Compare Ex. A above with Ex. B below.]

Ex. B. The maximal ideals in $\mathbf{Z}$ are the ideals of the form (p) where p is prime. This is because for $n \geq 2$, $\mathbf{Z}_n$ is a field $\Leftrightarrow n = p$ is prime.

The Ring $\mathbf{F}[x]$

Let $\mathbf{F}$ be a field, and $\mathcal{U} \subset \mathbf{F}[x]$ an ideal. Recall that $\mathbf{F}[x]$ is a PID, and hence $\mathcal{U} = \big(f(x)\big)$ for some $f(x) \in \mathbf{F}[x]$.

Claim. (1) $\mathcal{U}$ is prime $\Leftrightarrow$ either $\mathcal{U} = (0)$, or $\mathcal{U} = \big(p(x)\big)$, where $p(x)$ is prime (= irreducible).

(2) $\mathcal{U}$ is maximal $\Leftrightarrow \mathcal{U} = \big(p(x)\big)$, where $p(x)$ is prime (= irreducible).

Reason: First, since $\mathbf{F}[x]$ is an integral domain, and that $\mathbf{F}[x]/(0) = \mathbf{F}[x]$, it follows that (0) is a prime ideal. Next ,suppose that $p(x) \in \mathbf{F}[x]$ is prime, and that $h(x) \in \mathbf{F}[x]$ is given such that $\overline{h(x)} \neq \overline{0} \in \mathbf{F}[x]/\big(p(x)\big)$, i.e. $h(x) \notin \big(p(x)\big)$, i.e. $p(x) \not| h(x)$. Then since $p(x)$ is prime and $p(x) \not| h(x)$, it follows that $\big(p(x), h(x)\big) = 1$. Therefore $1 = \ell(x) \cdot p(x) + k(x) \cdot h(x)$ for some $\ell(x), k(x) \in \mathbf{F}[x]$. Thus modulo $\big(p(x)\big)$,

$$\overline{1} = \overline{k(x)} \cdot \overline{h(x)},$$

i.e. $\overline{h(x)}^{-1} = \overline{k(x)} \in \mathbf{F}[x]/\big(p(x)\big)$. Therefore $\mathbf{F}[x]/\big(p(x)\big)$ is a field, and hence $\big(p(x)\big)$ is maximal. Note that if $\mathcal{U} = \big(f(x)\big)$, where $f(x)$ is not prime (hence not irreducible), then $f(x) = g(x) \cdot h(x)$, where $f(x) \not| g(x)$ and $f(x) \not| h(x)$. Therefore $\overline{g(x)} \neq \overline{0}$ and $\overline{h(x)} \neq \overline{0}$ in $\mathbf{F}[x]/\mathcal{U}$, and yet $\overline{g(x)} \cdot \overline{h(x)} = \overline{f(x)} = \overline{0} \in \mathbf{F}[x]/\mathcal{U}$. Therefore $\mathbf{F}[x]/\mathcal{U}$ has non-zero zero divisors, and hence it is neither an integral domain, nor a field.

Summary

(I) The prime ideals in $\mathbf{Z}$ are:

$$(0), \quad \underbrace{\{(p) \mid p \in \mathbf{N} \text{ prime}\}}_{\text{maximal}}.$$

(II) The prime ideals in $\mathbf{F}[x]$ are:

$$(0), \quad \underbrace{\{\big(p(x)\big) \mid p(x) \in \mathbf{F}[x] \text{ prime}\}}_{\text{maximal}}.$$

Ex. Consider $\mathbf{F} = \mathbf{R}$, and $p(x) = x^2 + 1 \in \mathbf{R}[x]$. Then $p(x)$ is irreducible in $\mathbf{R}[x]$, since it has no real roots, hence $\mathbf{R}[x]/\big(p(x)\big)$ is a field. Let $\overline{x}$ be the image of $x \in \mathbf{R}[x]$ under the map:

$$\mathbf{R}[x] \to \frac{\mathbf{R}[x]}{\big(p(x)\big)} =: \mathbf{R}[\overline{x}] := \{a + b\overline{x} \mid \overline{x}^2 + 1 = 0\}.$$

Consider the map $T : \mathbf{C} \to \mathbf{R}[\overline{x}]$ given by $T(a + b\sqrt{-1}) = a + b\overline{x}$. Then T is in fact an isomorphism. Thus the complex numbers can be reconstructed via quotient rings.

Ex. Let $\mathbf{F} = \mathbf{Z}_2$, and $p(x) = x^2 + x + \overline{1} \in \mathbf{Z}_2[x]$. Then recall that $p(x)$ is irreducible in $\mathbf{Z}_2[x]$ since it has no roots in $\mathbf{Z}_2$. Therefore $\mathbf{Z}_2[x]/\big(p(x)\big)$ is a field. Let α be the image of $x \in \mathbf{Z}_2$ under the natural map:

$$\mathbf{Z}_2[x] \to \frac{\mathbf{Z}_2[x]}{\big(p(x)\big)} =: \mathbf{Z}_2[\alpha], \quad (\text{where } \overline{0} = p(\alpha) = \alpha^2 + \alpha + \overline{1}).$$

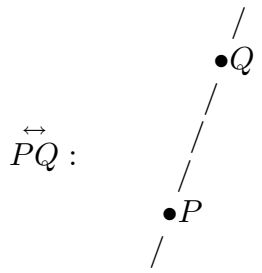
Then $\mathbf{Z}_2[\alpha]$ is the field we discussed earlier regarding solutions of quadratic equations, and here it is reconstructed via quotient rings.

Applications of Algebra to Geometry

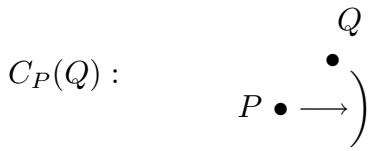
Ruler and Compass Constructions

The Tools

(**I**) Euclidean Ruler: Can draw a line through any two distinct points P and Q in the Euclidean plane $\mathbf{R}^2$.

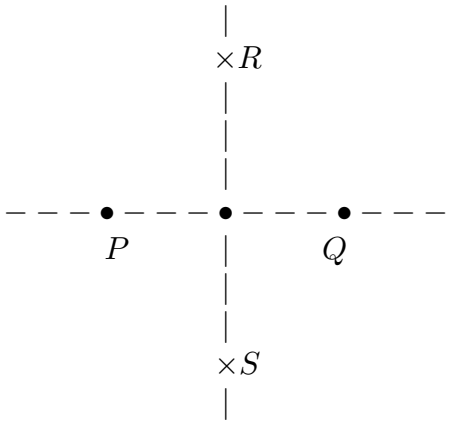


(**II**) Euclidean Compass: Assume given two distinct points P and Q in E. Can draw a circle with center P passing through Q.



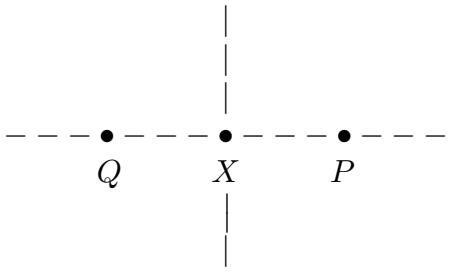
Key Example Constructions

1) *Perpendicular bisector of a line segment* $\overline{PQ}$. Draw $C_P(Q)$ and $C_Q(P)$. Then $C_P(Q) \cap C_Q(P) = \{R, S\}$. Now draw $\overleftrightarrow{RS}$. It intersects $\overline{PQ}$ perpendicularly at the midpoint of this segment. Thus we can bisect a segment using ruler and compass.

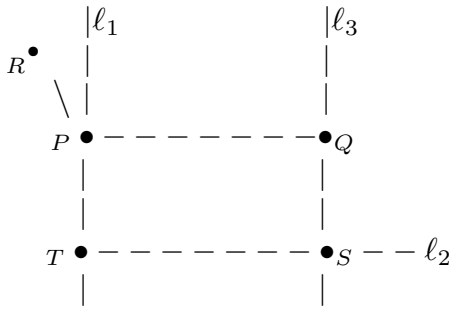


2) *Construct a perpendicular to a given line* ℓ*, through a given point* $X \in \ell$. Choose any $P \in \ell$, with $P \neq X$. Draw $C_X(P)$. Then $C_X(P) \cap \ell = \{P, Q\}$. Now use 1) to construct

a perpendicular bisector of $\overline{PQ}$.

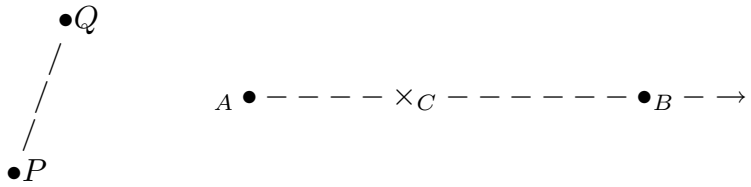


3) *Given three distinct points* $\{P, Q, R\}$*, can construct a rectangle* $\overline{|\ \ |}PQST$*, such that length*$(\overline{PT})$ = *length*$(\overline{PR})$. Construct ℓ_1 perpendicular to $\overleftrightarrow{PQ}$ at P. Draw $C_P(R)$ to arrive at T in the diagram below. Next, draw ℓ_2 perpendicular to $\overleftrightarrow{PT}$ at T, and then draw ℓ_3 perpendicular to $\overleftrightarrow{PQ}$ at Q. Then set $S = \ell_2 \cap \ell_3$.



Exercise. We introduce a relation on the set of line segments in the plane $\mathbf{R}^2$. Namely $\overline{PQ} \cong \overline{TS} \Leftrightarrow \text{length}(\overline{PQ}) = \text{length}(\overline{TS})$. Show that $\cong$ is an equivalence relation.

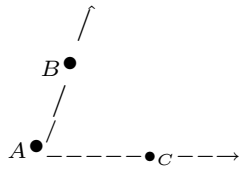
4) *Segment Construction Theorem.* Given a line segment $\overline{PQ}$, and a ray $\vec{AB}$, one can construct a point C on $\vec{AB}$ by ruler and compass, such that $\overline{PQ} \cong \overline{AC}$.



To carry out the construction, do the following: Construct a rectangle $\overline{|\ \ |}PAST$, as in 3), such that $\overline{PT} \cong \overline{PQ}$. Next, draw $C_A(S)$. Then $C_A(S) \cap \vec{AB} = C$.

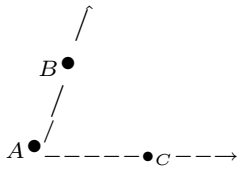
Angles

The notation, $\angle BAC$ is used to describe an angle:

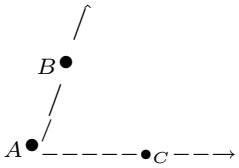


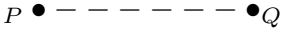
We consider the angle measure map $m : \{\text{Angles} \subset E\} \to [0, 360)$, and say that $\angle BAC \cong \angle DEF \Leftrightarrow m\angle BAC = m\angle DEF$. Again, one argues that $\cong$ is an equivalence relation.

5) *Angle Construction Theorem.* In ruler and compass geometry, there is the following analogue of the segment construction theorem (which we won't prove[†]): Assume given $\angle BAC$ and a ray $\overrightarrow{PQ}$ in $\mathbf{R}^2$. Then by ruler and compass, one can construct a point R in $\mathbf{R}^2$ such that $\angle RPQ \cong \angle BAC$.



For the next part, the following notation is useful. Given the angle and line segment below:

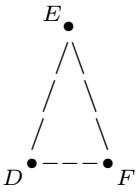




We write $\angle A$ for $\angle BAC$, if there is no possibility of confusion; and write PQ for the length of $\overline{PQ}$.

Congruence of Triangles

Assume given (triangles) $\triangle ABC$ and $\triangle DEF$.



Suppose that the dictionary:

$$\begin{array}{ccc} A & \leftrightarrow & D \\ B & \leftrightarrow & E \\ C & \leftrightarrow & F \end{array}$$

[†] If for simplicity of argument, we consider the case of an *acute* $\angle BAC$, i.e. $m\angle BAC < 90$, then consider this construction: Draw $C_A(B)$ and $C_C(B)$. Then $C_A(B) \cap C_C(B) = \{B, D\}$. Next, draw $\overrightarrow{BD}$. Then $\overrightarrow{BD} \cap \overrightarrow{AC} = T$ say. By segment construction, construct a point M on $\overrightarrow{PQ}$ such that $\overline{PM} \cong \overline{AT}$. Next, construct a line ℓ perpendicular to $\overrightarrow{PQ}$ at M. Construct R on ℓ such that $\overline{RM} \cong \overline{BT}$. Then $\angle RPQ \cong \angle BAC$.

induces the following:

$$\begin{array}{lcl} \angle A & \cong & \angle D \\ \angle B & \cong & \angle E \\ \angle C & \cong & \angle F \end{array} \quad \textit{and} \quad \frac{AB}{DE} = \frac{BC}{EF} = \frac{AC}{DF}.$$

Then we say that $\triangle ABC$ and $\triangle DEF$ are similar triangles, and in this case we write $\triangle ABC \sim \triangle DEF$.

Exercise. Show that $\sim$ is an equivalence relation on the set of triangles in the plane $\mathbf{R}^2$.

There is the following well-known AAA Similarity Theorem: *If the dictionary:*

$$\begin{array}{lcl} A & \leftrightarrow & D \\ B & \leftrightarrow & E \\ C & \leftrightarrow & F \end{array}$$

induces:

$$\begin{array}{lcl} \angle A & \cong & \angle D \\ \angle B & \cong & \angle E\,, \\ \angle C & \cong & \angle F \end{array}$$

then $\triangle ABC \sim \triangle DEF$.

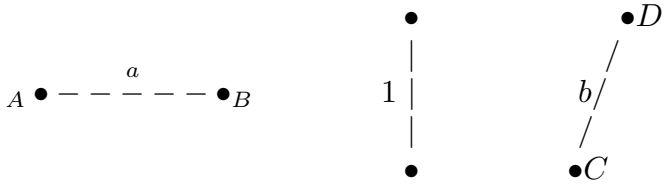
Recall the following well known result, that the sum of the measures of the (interior) angles of a triangle add up to 180. Thus:

$$\begin{array}{lcl} 180 - (m\angle A + m\angle B) & = & m\angle C \\ 180 - (m\angle D + m\angle E) & = & m\angle F\,. \end{array}$$

In particular, this leads to the AA Similarity Theorem: *If two pairs of corresponding angles of two triangles are congruent, then the triangles are similar.*

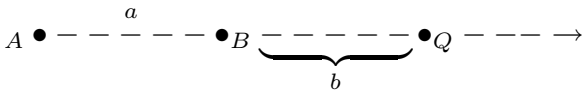
Algebra with Ruler and Compass, Part I

Assume given $a, b \in \mathbf{R}$, with $a > 0$, $b > 0$, and the quantities $a, b, 1$ represented by the lengths of any given line segments, such as below:



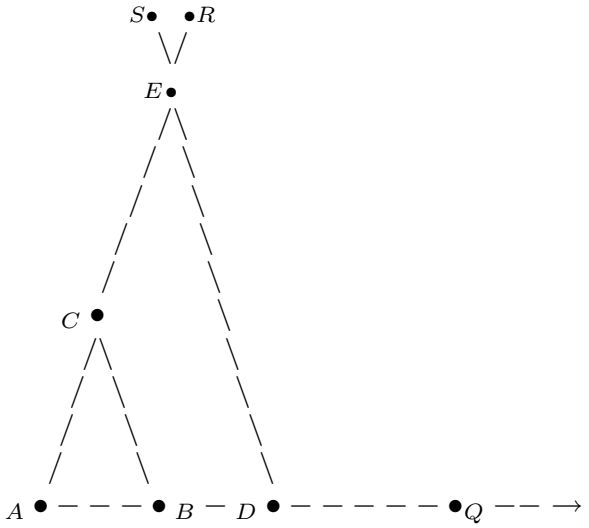
I.e. $AB = a$, $CD = b$.

(a) The sum "$a+b$". Use segment construction to arrive at a point Q on the ray $\overrightarrow{AB}$, such that $BQ = CD$.



Thus $AQ = a + b$, i.e. $\overline{AQ}$ represents "$a + b$".

(b) Multiplicative inverse $\frac{1}{a}$. Choose any $\angle QAR$. Then segment construct B, D on $\overrightarrow{AQ}$, and C on $\overrightarrow{AR}$, such that $AC = AD = 1$ and such that $AB = a$. Duplicate (viz. construct S) $\angle ABC$ to $\angle ADS$ (angle construction theorem). Set $E = \overrightarrow{AR} \cap \overrightarrow{DS}$



Then using the dictionary:

$$\begin{array}{ccc} A & \leftrightarrow & A \\ B & \leftrightarrow & D \\ C & \leftrightarrow & E \end{array}$$

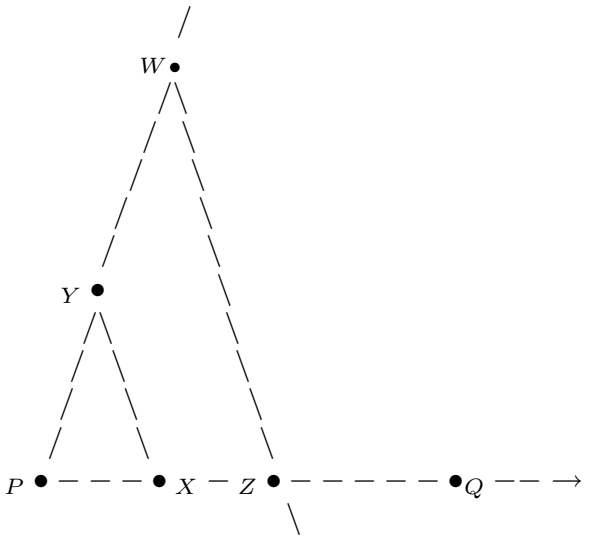
with $\angle A \cong \angle A$, $\angle B \cong \angle D$, it follows by the AA Theorem that $\triangle ABC \sim \triangle ADE$. Thus

$$\frac{1}{a} = \frac{AD}{AB} = \frac{AE}{AC} = \frac{AE}{1} = AE,$$

hence $\overline{AE}$ represents $1/a$.

(c) The product ab. We use essentually the same kind of diagram as in (b), duplicating $\angle PYX$ to $\angle PWZ$ (i.e. constructing the point Z in the process via the angle duplication

theorem process) viz.:



Where $PX = a$, $PY = 1$, $PW = b$. Using the dictionary:

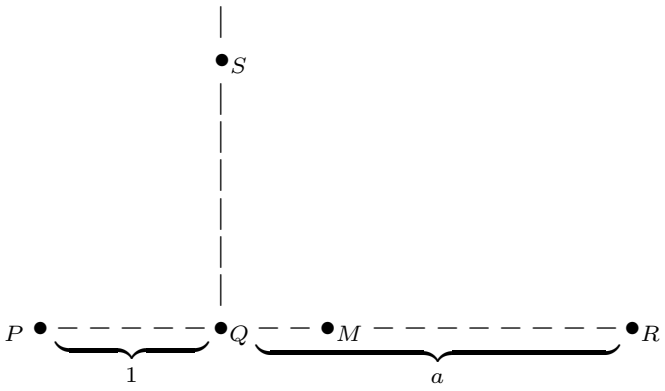
$$\begin{array}{ccc} P & \leftrightarrow & P \\ X & \leftrightarrow & Z \\ Y & \leftrightarrow & W \end{array}$$

to establish the similarity, viz.: $\triangle PXY \sim \triangle PZW$, it follows that:

$$\frac{PZ}{a} = \frac{PZ}{PX} = \frac{PW}{PY} = \frac{b}{1},$$

hence $PZ = ab$, i.e. $\overline{PZ}$ represents ab. Note that $b/a = b \cdot \frac{1}{a}$, and by (b) and (c) above, we can now construct a segment representing b/a.

(d) Square root of $a > 0$. Constructing $\sqrt{a}$:



First construct collinear $P - Q - R$, i.e. Q between P and R, such that $PQ = 1$, $QR = a$. [This involves the segment constructions $\overline{PQ}$ and $\overline{QR}$.] Next, bisect $\overline{PR}$ in a point M.

Thus $2 \cdot PM = 1 + a$, or equivalently $PM = \frac{1+a}{2}$. Draw ℓ perpendicular to $\overleftrightarrow{PR}$ at Q. Draw $C_M(R)$ to arrive at the point S above. Since S is a point on a circle through $\{P, R, S\}$, with diameter line segment $\overline{PR}$, it is well-known that $m\angle RSQ + m\angle PSQ = 90$. Furthermore, since $\triangle PQS$ is a right angle triangle, and the sum of the measures of the (interior) angles of a triangle add up to 180, it follows that $m\angle SPQ + m\angle PSQ = 90$. Therefore

$$\left.\begin{array}{l} m\angle RSQ + m\angle PSQ = 90 \\ m\angle SPQ + m\angle PSQ = 90 \end{array}\right\} \Rightarrow m\angle SPQ = m\angle RSQ.$$

Using the AA Similarity Theorem applied to the dictionary:

$$\begin{array}{ccc} P & \leftrightarrow & S \\ Q & \leftrightarrow & Q \\ S & \leftrightarrow & R \end{array}$$

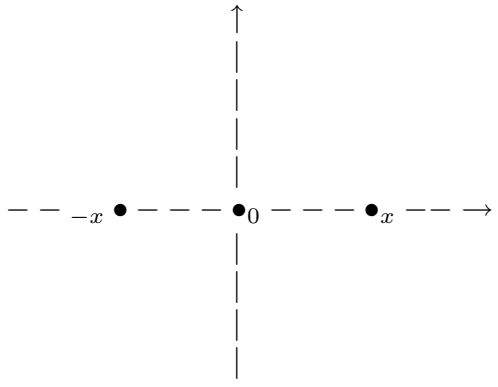
It follows that $\triangle PQS \sim \triangle SQR$. Therefore:

$$\frac{1}{QS} = \frac{PQ}{QS} = \frac{SQ}{QR} = \frac{QS}{a}.$$

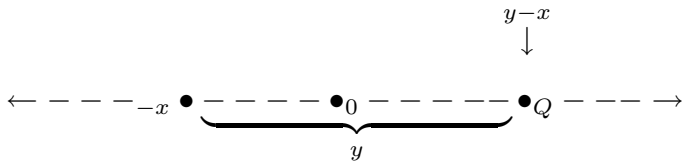
Hence $(QS)^2 = a$, i.e. $QS = \sqrt{a}$, and thus $\overline{QS}$ represents $\sqrt{a}$.

`Algebra with Ruler and Compass, Part II`

Recall that given $a, b \in \mathbf{R}$, $a > 0$, $b > 0$, we can construct segments representing the quantities $a + b$, $\frac{1}{a}$ (and more generally $\frac{b}{a}$), ab, and $\sqrt{a}$, by ruler and compass. By segment construction, these values can be transplanted on the ray $\overrightarrow{01}$, on the x-axis in the Euclidean plane $\mathbf{R}^2$. Now given any $x \in \mathbf{R}$, with $x > 0$, we can view $x \in \overrightarrow{01} \subset \mathbf{R}^2$. Thus we can draw $C_0(x)$ to get "$-x$" on the x-axis $\overleftrightarrow{01} = \mathbf{R}$.



Next, for a given real number $y > 0$, w can find a point Q on the ray $\overrightarrow{-x0}$ such that the length$(\overline{-xQ}) = y$. Thus Q represents "$y - x$" $= y + (-x)$ on $\mathbf{R} = \overleftrightarrow{01}$.



Next, suppose $x, y \in \mathbf{R}$, $x > 0$, $y > 0$. To construct $(-x)y$, do the following on $\mathbf{R} = \overleftrightarrow{01} \subset \mathbf{R}^2$:

$$(-x) \overset{\text{draw } C_0(-x)}{\mapsto} x \overset{\bullet y}{\mapsto} xy \overset{\text{draw } C_0(xy)}{\mapsto} -(xy).$$

Thus the esential idea in doing "algebra" on $\mathbf{R}$ by ruler and compass, is to start with values in $\mathbf{R}$, identified with $\overleftrightarrow{01} \subset \mathbf{R}^2$, and using ruler and compass on $\mathbf{R}^2$, transplant the new values back on $\mathbf{R} = \overleftrightarrow{01}$. In this way, the ruler and compass constructions define $+, \bullet$ operations on $\mathbf{R}$ synthetically, giving $\mathbf{R}$ the structure of a field. Furthermore, we can also construct $\sqrt{a}$ for real $a > 0$. The following picture summarizes what we have just described:

$$\left.\begin{matrix} a, b \in \mathbf{R} \\ a, b > 0 \end{matrix}\right\} \quad \Rightarrow \quad \left[\begin{matrix} \text{Ruler \& Compass} \\ \text{Operations} \\ \text{on } \mathbf{R}^2 \end{matrix}\right] \quad \Rightarrow \quad \left\{\begin{matrix} a+b,\ ab,\ 1/b,\ a/b \\ \sqrt{a},\ -a,\ a-b \end{matrix}\right.$$

A Special Field

Given $0, 1 \in \mathbf{R}$, we construct the subfield of $\mathbf{R}$ generated by $\{0, 1\}$ under the "algebra" of ruler and compass constructions.

Definition. Let $\mathbf{L}$ be the subfield of $\mathbf{R}$ generated by $\{0, 1\}$ under the following operations: $a + b$, $-b$, ab, $1/a$ if $a \neq 0$, and $\sqrt{a}$ if $a > 0$.

Remarks. (1) $\mathbf{Q} \subset \mathbf{L}$ is a subfield.

(2) For example

$$\sqrt{2},\ \sqrt[4]{3} := \sqrt{\sqrt{3}},\ \sqrt[8]{5} := \sqrt{\sqrt{\sqrt{5}}},\ \frac{\sqrt{2}+\sqrt{3}}{10+12(\sqrt[4]{5})},\ \sqrt{\sqrt[4]{3}+\sqrt{8}+5},$$

are elements of $\mathbf{L}$.

(3) Fact: $\pi, e \notin \mathbf{L}$.

We introduce the $\mathbf{L}$-plane $\mathbf{L}^2 := \mathbf{L} \times \mathbf{L} = \{(x, y) \in \mathbf{R}^2 \mid x, y \in \mathbf{L}\}$. We will later see that $\mathbf{L}$ is "much smaller" than $\mathbf{R}$, in the sense that $\mathbf{L}$ is countable, whereas $\mathbf{R}$ is uncountable; however from the "naked eye", $\mathbf{L}$ and $\mathbf{R}$, and similarly $\mathbf{L}^2$ and $\mathbf{R}^2$, "look the same".

Definitions. (i) $(x, y) \in \mathbf{R}^2$ is called an **L**-point if $(x, y) \in \mathbf{L}^2$.

(ii) A line $\ell \subset \mathbf{R}^2$ is called an **L**-line if it contains two distinct **L**-points.

(iii) An **L**-circle is a circle centered at an **L**-point and whose radius $\in \mathbf{L}$.

(iv) An **L**-equation is an equation of the form:

$$Ax + By + C = 0 \quad \text{or} \quad x^2 + y^2 + Dx + Ey + F = 0,$$

where $A, B, C, D, E, F \in \mathbf{L}$.

Claim. $\ell \subset \mathbf{R}^2$ is an **L**-line $\Leftrightarrow$ ℓ is the graph of some **L**-equation of the form $Ax + By + C = 0$, where $(A, B) \neq (0, 0)$.

Reason: Assume ℓ is an **L**-line, and let $P = (p_1, p_2),\ Q = (q_1, q_2) \in \ell \cap \mathbf{L}^2$, with $P \neq Q$. Thus either $p_1 \neq q_1$ or $p_2 \neq q_2$. Lets assume say $p_1 \neq q_1$, and set $m = \frac{p_2 - q_2}{p_1 - q_1}$. Then ℓ is given by $\frac{y - p_2}{x - p_1} = m$, or $y - p_2 = m(x - p_1)$. Thus $Ax + By + C = 0$, where $A = m,\ B = -1,\ C = p_2 - mp_1 \in \mathbf{L}$, i.e. ℓ is the graph of an **L**-equation. Conversely, if ℓ is the graph of an **L**-equation of the form $Ax + By + C = 0$, with $A, B, C \in \mathbf{L}$, and say $B \neq 0$, then $P := (0, -C/B),\ Q := (1, -(C + A)/B) \in \ell \cap \mathbf{L}^2$ are two distinct **L**-points. Thus ℓ is an **L**-line.

Claim. $C \subset \mathbf{R}^2$ is an **L**-circle $\Leftrightarrow$ C is the graph of some **L**-equation of the form $x^2 + y^2 + Dx + Ey + F = 0$, where $D, E, F \in \mathbf{L}$, and $D^2 + E^2 - 4F > 0$.

Reason: Suppose that C is an **L**-circle. Thus C is centered at some $P = (p_1, p_2) \in \mathbf{L}^2$, with radius $r \in \mathbf{L}$, $r > 0$. Thus C is the graph of the equation $(x - p_1)^2 + (y - p_2)^2 = r^2$. Equivalently:

$$x^2 + y^2 + \underbrace{(-2p_1)}_{=:D \in \mathbf{L}} x + \underbrace{(-2p_2)}_{=:E \in \mathbf{L}} y + \underbrace{(p_1^2 + p_2^2 - r^2)}_{=:F \in \mathbf{L}} = 0.$$

Thus C is the graph of an **L**-equation. Conversely, given an **L**-equation of the form:

$$x^2 + y^2 + Dx + Ey + F = 0, \quad D, E, F \in \mathbf{L}, \quad D^2 + E^2 - 4F > 0,$$

we complete the square to get:

$$\big(x - (-D/2)\big)^2 + \big(y - (-E/2)\big)^2 = \frac{D^2 + E^2 - 4F}{4}.$$

Thus C is an **L**-circle, with center $P := (-D/2, -E/2) \in \mathbf{L}^2$, and radius

$$r := \sqrt{\frac{D^2 + E^2 - 4F}{4}} \ \in \ \mathbf{L}.$$

Claim. Let $\ell, \ell_1 \subset \mathbf{R}^2$ be distinct **L**-lines, and let $C, C_1 \subset \mathbf{R}^2$ be distinct **L**-circles. Then, assuming non-empty intersections, we have:

(i) $\ell \cap \ell_1 \in \mathbf{L}^2$.

(ii) $C \cap C_1 \subset \mathbf{L}^2$.

(iii) $\ell \cap C \subset \mathbf{L}^2$.

Reason: Consider the **L**-equations:

$$\begin{array}{ccc} \ell & : & Ax + By + C = 0 \\ \ell_1 & : & A_1x + B_1y + C_1 = 0 \\ C & : & x^2 + y^2 + Dx + Ey + F = 0 \\ C_1 & : & x^2 + y^2 + D_1x + E_1y + F_1 = 0 \end{array}$$

(i) We can assume that

$$\det \begin{bmatrix} A & B \\ A_1 & B_1 \end{bmatrix} \neq 0,$$

so that by Cramer's rule,

$$\ell \cap \ell_1 = \left(\frac{\det \begin{bmatrix} -C & B \\ -C_1 & B_1 \end{bmatrix}}{\det \begin{bmatrix} A & B \\ A_1 & B_1 \end{bmatrix}}, \frac{\det \begin{bmatrix} A & -C \\ A_1 & -C_1 \end{bmatrix}}{\det \begin{bmatrix} A & B \\ A_1 & B_1 \end{bmatrix}} \right) \in \mathbf{L}^2.$$

(ii) Subtracting the equation for C_1 from the equation for C leads to:

$$(D - D_1)x + (E - E_1)y + (F - F_1) = 0,$$

where one can argue that either $D - D_1 \neq 0$ or $E - E_1 \neq 0$. [This is because the circles must have different centers, i.e. $(-D/2, -E/2) \neq (-D_1/2, -E_1/2)$.] Let us suppose that say $D - D_1 \neq 0$. Then we can solve for x, viz.:

$$(\star) \qquad x = \left(\frac{E_1 - E}{D - D_1} \right) y + \left(\frac{F_1 - F}{D - D_1} \right).$$

Substituting this for x in the equation for C yields:

$$\left[\left(\frac{E_1 - E}{D - D_1} \right) y + \left(\frac{F_1 - F}{D - D_1} \right) \right]^2 + y^2 + D \left[\left(\frac{E_1 - E}{D - D_1} \right) y + \left(\frac{F_1 - F}{D - D_1} \right) + Ey \right] + F = 0.$$

Equivalently,

$$\underbrace{\left[\left(\frac{E_1 - E}{D - D_1} \right)^2 + 1 \right]}_{=:a \in \mathbf{L},\ \text{Note: } a > 0} y^2 + \underbrace{\left[2 \left(\frac{E_1 - E}{D - D_1} \right) \left(\frac{F_1 - F}{D - D_1} \right) + D \left(\frac{E_1 - E}{D - D_1} \right) + E \right]}_{=:b \in \mathbf{L}} y$$

$$+\underbrace{\left[\left(\frac{F_1-F}{D-D_1}\right)^2+D\left(\frac{F_1-F}{D-D_1}\right)+F\right]}_{=:c\in\mathbf{L}}=0.$$

We can solve for y in the above quadratic equation, by the quadratic formula. Since $C\cap C_1\neq\emptyset$ is assumed, the two (including multiplicity) y-roots must be real. In particular $\Delta:=b^2-4ac\geq 0$. But the coefficients $a,b,c\in\mathbf{L}$, and hence so is $\sqrt{\Delta}\in\mathbf{L}$. In particular the y-roots $\in\mathbf{L}$, and the corrsponding values of x from $(\star)$ belong to $\mathbf{L}$. Thus $C\cap C_1\in\mathbf{L}^2$.

(iii) Solve for y in terms of x, or x in terms of y, from the equation $Ax+By+C=0$. Then substitute it in for y, or x, in the equation $x^2+y^2+Dx+Ey+F=0$. Now use the quadratic formula, and the fact that $\mathbf{L}$ is closed under $\sqrt{a}$ for $a\in\mathbf{L},\ a>0$, to deduce that $\ell\cap C\in\mathbf{L}^2$. The details are similar to that in (ii) above.

Another way of stating the above claim is this: For any $\mathbf{L}$-line $\ell\subset\mathbf{R}^2$, and $\mathbf{L}$-circle $C\subset\mathbf{R}^2$, put $\underline{\ell}=\ell\cap\mathbf{L}^2$, and $\underline{C}=C\cap\mathbf{L}^2$. Then[†]:

$$\ell\cap\ell_1=\underline{\ell}\cap\underline{\ell}_1,\quad C\cap C_1=\underline{C}\cap\underline{C}_1,\quad \ell\cap C=\underline{\ell}\cap\underline{C}.$$

The upshot is that all ruler and compass constructions in $\mathbf{R}^2$ can be carried out in $\mathbf{L}^2$.

Some Field Theory: Quadratic Extensions

Let $\mathbf{F}\subset\mathbf{R}$ be a subfield, and assume given $k\in\mathbf{F}$ such that $\sqrt{k}\notin\mathbf{F}$.

Ex. $\mathbf{F}:=\mathbf{Q}\subset\mathbf{R}$ is a subfield, $k:=2\in\mathbf{Q}$, and yet $\sqrt{2}\notin\mathbf{Q}$.

Ex. $\mathbf{F}=\mathbf{R}$, $k:=-1\in\mathbf{R}$, and yet $\sqrt{-1}\notin\mathbf{R}$.

We put

$$\mathbf{F}[\sqrt{k}]\stackrel{\text{def}}{=}\{x+y\sqrt{k}\in\mathbf{C}\mid x,y\in\mathbf{F}\}.$$

[We will show that $\mathbf{F}[\sqrt{k}]$ is a field, called a quadratic field extension of $\mathbf{F}$.]

Ex. $\mathbf{R}[\sqrt{-1}]=\mathbf{C}$.

Ex. The subfield $\mathbf{Q}[\sqrt{2}]\subset\mathbf{R}$ was studied earlier.

Claim. $\mathbf{F}[\sqrt{k}]$ is a subfield of $\mathbf{C}$, containing $\mathbf{F}$ as a subfield. [Note: If $k>0$, then likewise $\mathbf{F}[\sqrt{k}]$ is a subfield of $\mathbf{R}$.]

[†] Let $\ell\subset\mathbf{R}^2$ be an $\mathbf{L}$-line, with two distinct $\mathbf{L}$-points $P,Q\in\ell$. Then it follows that $\{P+\lambda\cdot(Q-P)\mid\lambda\in\mathbf{L}\}\subset\ell$. Also, if $C\subset\mathbf{R}^2$ is an $\mathbf{L}$-circle with $\mathbf{L}$-point $P=(p_1,p_2)$ as center, and with radius $0<r\in\mathbf{L}$, then for any $q_1\in\mathbf{L}$ with $|q_1-p_1|\leq r$, there exists $q_2,\tilde{q}_2\in\mathbf{L}$ such that $q_2\leq p_2\leq\tilde{q}_2$ and that $Q:=(q_1,q_2),\ \tilde{Q}:=(q_1,\tilde{q}_2)\in C$. From the point of view of point-set topology, this implies that $\underline{\ell}$ (resp. $\underline{C}$) is dense in ℓ (resp. C).

Reason: It is reasonably clear that the inclusions $\mathbf{F} \subset \mathbf{F}[\sqrt{k}] \subset \mathbf{C}$ are inclusions of subrings [exercise for the reader]. Thus we need only verify the existence of multiplicative inverses for nonzero elements of $\mathbf{F}[\sqrt{k}]$. We first observe that since $\sqrt{k} \notin \mathbf{F}$, the following is true:

1) If $z = x + y\sqrt{k} \in \mathbf{F}[\sqrt{k}]$, then $z = 0 \Leftrightarrow x = y = 0$. [Reason: If $z = 0$ and $y = 0$, then $0 = x + 0\sqrt{k} \Rightarrow x = 0$, *a fortiori* $z = 0$. So assume that $z = 0$, but that $y \neq 0$. Then $\sqrt{k} = -xy^{-1} \in \mathbf{F}$, which violates $\sqrt{k} \notin \mathbf{F}$. Hence $z = 0 \Leftrightarrow x = y = 0$.]

2) For $z = x+y\sqrt{k} \in \mathbf{F}[\sqrt{k}]$, put $\overline{z} = x-y\sqrt{k}$ (conjugate[†] of z). Then conjugation $\overline{(\ )}$ is a well-defined operation on $\mathbf{F}[\sqrt{k}]$. [Reason: Let $z_1 = x_1 + y_1\sqrt{k}, z_2 = x_2 + y_2\sqrt{k} \in \mathbf{F}[\sqrt{k}]$. Then $z_1 = z_2 \Leftrightarrow z_1 - z_2 = 0 \Leftrightarrow (x_1 - x_2) + (y_1 - y_2)\sqrt{k} = 0 \Leftrightarrow x_1 = x_2 \ \& \ y_1 = y_2 \Leftrightarrow \overline{z}_1 = \overline{z}_2$.]

3) We define the norm map $N : \mathbf{F}[\sqrt{k}] \to \mathbf{F}$ by the formula $N(z) = z\overline{z}$. For example, if $z = x+y\sqrt{k}$, then $N(z) = x^2 - ky^2$. Then $N(z) = 0 \Leftrightarrow z = 0$. [Reason: If $N(z) = y = 0$, then $x = 0$, *a fortiori* $z = 0$. So assume that $N(z) = 0$ but that $y \neq 0$. Then $k = (\frac{x}{y})^2$, i.e. $\sqrt{k} = \pm(\frac{x}{y}) \in \mathbf{F}$, which violates $\sqrt{k} \notin \mathbf{F}$. Therefore $N(z) = 0 \Leftrightarrow z = 0$.]

Now assume given $z \in \mathbf{F}[\sqrt{k}]$, with $z \neq 0$. Then $N(z) \in \mathbf{F}$ and $N(z) \neq 0$. Note that $N(z)^{-1} \in \mathbf{F}$, and that $\overline{z} \cdot N(z)^{-1} \in \mathbf{F}[\sqrt{k}]$. Furthermore, $z \cdot \left(\overline{z} \cdot N(z)^{-1}\right) = 1$, hence $z^{-1} = \overline{z} \cdot N(z)^{-1} \in \mathbf{F}[\sqrt{k}]$. Thus $\mathbf{F}[\sqrt{k}]$ is a subfield of $\mathbf{C}$.

Remarks. (a) For a subfield $\mathbf{F} \subset \mathbf{R}$ and $k \in \mathbf{F}$, $k > 0$ given, with $\sqrt{k} \notin \mathbf{F}$, then $\mathbf{F}[\sqrt{k}] \subset \mathbf{R}$ is a subfield of $\mathbf{R}$. This will be the situation regarding subfields of $\mathbf{L}$ from ruler and compass geometry.

(b) Note that $\overline{\overline{z}} = z$, and that $z = \overline{z} \Leftrightarrow z \in \mathbf{F}$. The following properties of conjugation and norm, introduced above, are easy to verify:

(i) For $z_1, z_2 \in \mathbf{F}[\sqrt{k}]$, $\overline{z_1 z_2} = \overline{z}_1 \overline{z}_2$.

(ii) For $z_1, z_2 \in \mathbf{F}[\sqrt{k}]$, $N(z_1 z_2) = N(z_1)N(z_2)$. [Note: This follows from (i) above. $N(z_1 z_2) = \overline{z_1 z_2} z_1 z_2 = \overline{z}_1 \overline{z}_2 z_1 z_2 = (\overline{z}_1 z_1)(\overline{z}_2 z_2) = N(z_1)N(z_2)$.]

The following examples will serve as motivation for the next claim.

Ex. Let $f(x) = x^2 + x + 1 \in \mathbf{R}[x]$ be given. Then

$$f(x) = 0 \Leftrightarrow x = \frac{-1 \pm \sqrt{-3}}{2}.$$

Let $z = \frac{-1+\sqrt{-3}}{2} \in \mathbf{R}[\sqrt{-3}] \in \mathbf{C}$. Then $\overline{z} = \frac{-1-\sqrt{-3}}{2} \in \mathbf{R}[\sqrt{-3}]$, and $f(z) = f(\overline{z}) = 0$.

[†] Note that for $z \in \mathbf{R}[\sqrt{-1}]$, $\overline{z}$ is complex conjugation. For $z \in \mathbf{Q}[\sqrt{2}]$, the conjugate $\overline{z}$ is not complex conjugation.

Ex. Let $f(x) = x^2 + x - \frac{1}{4} \in \mathbf{Q}[x]$. Then

$$f(x) = 0 \Leftrightarrow x = \frac{-1 \pm \sqrt{2}}{2}.$$

Let $z = \frac{-1+\sqrt{2}}{2} \in \mathbf{Q}[\sqrt{2}] \in \mathbf{R}$. Then $\overline{z} = \frac{-1-\sqrt{2}}{2} \in \mathbf{Q}[\sqrt{2}]$, and $f(z) = f(\overline{z}) = 0$.

Claim. Assume given a field $\mathbf{F}$, $k \in \mathbf{F}$, with $\sqrt{k} \notin \mathbf{F}$. Let $f(x) \in \mathbf{F}[x]$, and suppose that $f(z) = 0$ for some $z \in \mathbf{F}[\sqrt{k}]$. Then $f(\overline{z}) = 0$. [Thus $f(z) = 0 \Leftrightarrow f(\overline{z}) = 0$.]

Reason: Write $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, with $a_0, \ldots, a_n \in \mathbf{F}$. Then $\overline{a}_j = a_j$ for all $j = 0, \ldots, n$. Let $z \in \mathbf{F}[\sqrt{k}]$, with $f(z) = 0$. Then:

$$0 = f(z) = \overline{f(z)} = \overline{a_n z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0} = \overline{a}_n \overline{z}^n + \overline{a}_{n-1}\overline{z}^{n-1} + \cdots + \overline{a}_1 \overline{z} + \overline{a}_0$$
$$= a_n \overline{z}^n + a_{n-1}\overline{z}^{n-1} + \cdots + a_1 \overline{z} + a_0 = f(\overline{z}).$$

The Ruler and Compass Field $\mathbf{L}$

Recall that $\mathbf{L} \subset \mathbf{R}$ is the subfield generated by 0 and 1 under the operations:

$$a + b,\ -a,\ \frac{a}{b}\ (b \neq 0),\ ab,\ \sqrt{a}\ (a > 0).$$

Thus, for example $\sqrt{\sqrt{\sqrt{12}}}, \sqrt{\sqrt{2}} - \sqrt{3}, \sqrt{\sqrt{10}} - \sqrt{14} + 15, -\sqrt{2}/\sqrt{3}$ are elements of $\mathbf{L}$.

Definition. Assume given an increasing "tower" of subfields:

$$\mathbf{Q} = \mathbf{F}_0 \underset{\neq}{\subset} \mathbf{F}_1 \underset{\neq}{\subset} \mathbf{F}_2 \underset{\neq}{\subset} \mathbf{F}_3 \underset{\neq}{\subset} \cdots \underset{\neq}{\subset} \mathbf{F}_n \underset{\neq}{\subset} \mathbf{R},$$

where $\mathbf{F}_{j+1} = \mathbf{F}_j[\sqrt{k_{j+1}}]$, $k_{j+1} \in \mathbf{F}_j$, $k_{j+1} > 0$, with $\sqrt{k_{j+1}} \notin \mathbf{F}_j$. We say that $\mathbf{F}_n$ is an $\mathbf{L}$-subfield of order n. [Note that $\mathbf{F}_n \subset \mathbf{L}$.]

Remark. There is only one $\mathbf{F}_0$, namely $\mathbf{F}_0 = \mathbf{Q}$; however there are many possible $\mathbf{F}_n$'s for a given $n \geq 1$. For example, $\mathbf{Q}[\sqrt{2}]$, $\mathbf{Q}[\sqrt{3}]$ represent two different $\mathbf{F}_1$'s.

Examples of Towers:

$$\begin{array}{ccccccccccc}
\mathbf{Q} & \underset{\neq}{\subset} & \mathbf{Q}[\sqrt{2}] & \underset{\neq}{\subset} & \big(\mathbf{Q}[\sqrt{2}]\big)\big[\sqrt{\sqrt{2}}\big] & \underset{\neq}{\subset} & \Big(\big(\mathbf{Q}[\sqrt{2}]\big)[\sqrt{\sqrt{2}}]\Big)\Big[\sqrt{\sqrt{\sqrt{2}}}\Big] & \underset{\neq}{\subset} & \\
|| & & || & & || & & || & & \\
\mathbf{F}_0 & \underset{\neq}{\subset} & \mathbf{F}_1 & \underset{\neq}{\subset} & \begin{array}{c}\mathbf{F}_2 \\ \not|| \\ \mathbf{F}_2\end{array} & \underset{\neq}{\subset} & \begin{array}{c}\mathbf{F}_3 \\ \not|| \\ \mathbf{F}_3\end{array} & & \cdots \\
|| & & || & & || & & || & & \\
\mathbf{Q} & \underset{\neq}{\subset} & \mathbf{Q}[\sqrt{2}] & \underset{\neq}{\subset} & \big(\mathbf{Q}[\sqrt{2}]\big)\big[\sqrt{3}\big] & \underset{\neq}{\subset} & \Big(\big(\mathbf{Q}[\sqrt{2}]\big)[\sqrt{3}]\Big)\Big[\sqrt{\sqrt{3}}\Big] & \underset{\neq}{\subset} &
\end{array}$$

Basic Observation 1: $x \in \mathbf{F}_n \Leftrightarrow x$ is obtained from $\mathbf{Q}$ by applying at most n $\sqrt{\ }$ operations.

Ex. $x = \sqrt{\sqrt{\sqrt{2}}} \in \mathbf{F}_3 := \Big(\big(\mathbf{Q}[\sqrt{2}]\big)\big[\sqrt{\sqrt{2}}]\big) \Big)\Big[\sqrt{\sqrt{\sqrt{2}}}\Big]$

Basic Observation 2: $x \in \mathbf{L} \Rightarrow x \in \mathbf{F}_n$ for some $\mathbf{F}_n$. [Reason: x is obtained from $\{0,1\} \subset \mathbf{Q}$ via a finite number of the operations: $\pm, \bullet, \div, \sqrt{+\text{ve}}$.]

Definition. $x \in \mathbf{L}$ is an $\mathbf{L}$-number of order n if $x \in \mathbf{F}_n$ for some $\mathbf{F}_n$. I.e. x is obtained from $\{0,1\} \subset \mathbf{Q}$ via $\pm, \bullet, \div$ and by at most n applications of $\sqrt{+\text{ve}}$.

Ex. $\frac{\sqrt{2}+5\sqrt{3}}{\sqrt{2}} \in \big(\mathbf{Q}[\sqrt{2}]\big)\big[\sqrt{3}\big]$ has order 2.

Ex. $\sqrt{\sqrt{\sqrt{10}} + \sqrt{10}}$ has order 3.

Key Claim I. Assume given a subfield $\mathbf{F} \subset \mathbf{R}$, and $k \in \mathbf{F}$, with $\sqrt{k} \notin \mathbf{F}$. Let $p(x) = x^3 + ax^2 + bx + c \in \mathbf{F}[x]$ be given, and suppose that $p(z) = 0$ for some $z \in \mathbf{F}[\sqrt{k}]$. Then $p(r) = 0$ for some $r \in \mathbf{F}$.

Reason: Write $z = a + b\sqrt{k}$, $a, b \in \mathbf{F}$, and recall the conjugate $\overline{z} = a - b\sqrt{k}$, the norm $N(z) = z\overline{z} \in \mathbf{F}$, and that $p(z) = 0 \Leftrightarrow p(\overline{z}) = 0$. Note that $z = \overline{z} \Leftrightarrow b = 0 \Leftrightarrow z \in \mathbf{F}$. Thus if $z = \overline{z}$, just set $r = z \in \mathbf{F}$. Therefore we can assume that $z \neq \overline{z}$, and hence $z, \overline{z}$ are two distinct roots of $p(x)$. Put $g(x) = (x-z)(x-\overline{z}) = x^2 - (z+\overline{z})x + z\overline{z} = x^2 + (-2a)x + N(z) \in \mathbf{F}[x]$. By Euclid division, $p(x) = q(x)g(x) + r_0(x)$, where $q(x), r_0(x) \in \mathbf{F}[x]$, and where $\deg r_0(x) \leq 1$. Thus

$$r_0(z) = p(z) - q(z)g(z) = 0 = p(\overline{z}) - q(\overline{z})g(\overline{z}) = r_0(\overline{z}).$$

In particular $r_0(x)$ has two distinct roots, namely z and $\overline{z}$. But recall that $r_0(x) \in \mathbf{F}[x] \subset \big(\mathbf{F}[\sqrt{k}]\big)[x]$ has at most one root in $\mathbf{F}[\sqrt{k}]$, or $r_0 = 0$. Thus it is clear that $r_0 = 0$, hence $p(z) = q(x)g(x)$. Taking degrees, it is clear that $\deg q(x) = 1$. Next, we recall that $q(x) \in \mathbf{F}[x]$ has exactly one root $r \in \mathbf{F}$. Thus $p(r) = q(r)g(r) = 0$, and we're done[†].

As a consequence of the above claim, we arrive at:

Key Claim II. Let $p(x) = x^3 + ax^2 + bx + c \in \mathbf{Q}[x]$ be given. Suppose that $p(z) = 0$ for some $z \in \mathbf{L}$. Then $p(r) = 0$ for some $r \in \mathbf{Q}$.

[†] Another argument, using the Fundamental Theorem of Algebra, goes as follows. First reduce to the case where $z \neq \overline{z}$ are roots of $p(x)$. We can then factor $p(x) = x^3 + ax^2 + bx + c = (x-z)(x-\overline{z})(x-r)$, for some $r \in \mathbf{C}$. But $c = -rN(z)$, where $N(z) = z \cdot \overline{z} \in \mathbf{F}^\times$. Thus $r = -\frac{c}{N(z)} \in \mathbf{F}$.

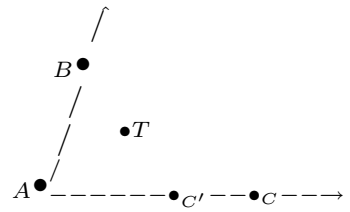
Reason: $z \in \mathbf{L} \Rightarrow z = z_n \in \mathbf{F}_n$ for some $\mathbf{F}_n$ (and some n). But by definition, $\mathbf{F}_n$ comes from a tower:

$$\mathbf{Q} = \mathbf{F}_0 \underset{\neq}{\subset} \mathbf{F}_1 \underset{\neq}{\subset} \mathbf{F}_2 \underset{\neq}{\subset} \cdots \underset{\neq}{\subset} \mathbf{F}_{n-1} \underset{\neq}{\subset} \mathbf{F}_n,$$

where $\mathbf{F}_j = \mathbf{F}_{j-1}[\sqrt{k_j}]$, $(k_j \in \mathbf{F}_{j-1},\ \sqrt{k_j} \notin \mathbf{F}_{j-1})$, $j = 1, \ldots, n$. Thus $p(x) \in \mathbf{Q}[x] \subset \mathbf{F}_n[x]$ and $p(z_n) = 0$, (some $z_n \in \mathbf{F}_n$) $\Rightarrow p(z_{n-1}) = 0$ for some $z_{n-1} \in \mathbf{F}_{n-1}$. This is a consequence of the key claim I above. Applying the claim again, it follows that $p(z_{n-2}) = 0$ for some $z_{n-2} \in \mathbf{F}_{n-2}$ and so on. We eventually arrive at $p(z_0) = 0$ for some $z_0 \in \mathbf{F}_0 = \mathbf{Q}$. Now put $r = z_0$.

Back to Ruler and Compass

Bisecting an Angle

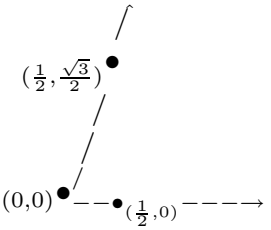


It is easy to bisect any given angle. For example, given $\angle BAC$ in the above picture, draw $C_A(B)$ to get C' on the ray $\overrightarrow{AC}$. Then bisect $\overline{BC'}$ in T. Finally, draw $\overrightarrow{AT}$.

The Impossible Constructions

(I) Trisection. *It is not possible to be able to trisect any angle*[†] *by ruler and compass.* The reasoning goes as follows:

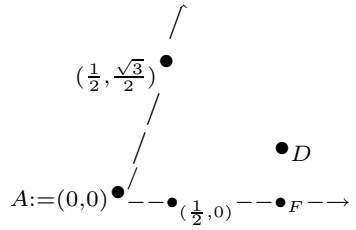
1) Recall that all ruler and compass constructions can be done in the **L**-plane. Further, if it were possible to trisect any angle by ruler and compass, then one could trisect the angle 60°.



Note that $(0,0)$, $(\frac{1}{2},0)$, $(\frac{1}{2},\frac{\sqrt{3}}{2})$ are **L**-points, i.e. belong to $\mathbf{L}^2$. This makes $\angle 60°$ an "**L**-angle", i.e. the union of the two "**L**-rays": $\overrightarrow{(0,0),(\frac{1}{2},0)} \bigcup \overrightarrow{(0,0),(\frac{1}{2},\frac{\sqrt{3}}{2})}$, where by

[†] Certain angles can be trisected by ruler and compass, such as the 90° angle.

definition an **L**-ray is of the form $\overrightarrow{PQ}$, where P, Q are **L**-points. Let $A = (0,0)$. Then ruler and compass construction in the **L**-plane enables us to find **L**-points D and F (with F the projection of D on the horizontal axis), such that $\cos 20^\circ = \frac{AF}{AD}$.



Thus $y := \cos 20^\circ \in \mathbf{L}$. We now need some trig. Recall that:

$$\cos(\alpha \pm \beta) = \cos\alpha\cos\beta \mp \sin\alpha\sin\beta,$$

[Hence: $\cos(2\theta) = \cos^2\theta - \sin^2\theta$ (double angle identity).]

$$\sin(\alpha \pm \beta) = \sin\alpha\cos\beta \pm \cos\alpha\sin\beta$$

[Hence: $\sin(2\theta) = 2\sin\theta\cos\theta$ (double angle identity).]

$$\cos^2\theta + \sin^2\theta = 1. \quad \text{(Pythagorean)}$$

Thus:

$$\cos(3\theta) = \cos(2\theta+\theta) = \cos(2\theta)\cos\theta - \sin(2\theta)\sin\theta = [\cos^2\theta - \sin^2\theta]\cos\theta - 2\sin^2\theta\cos\theta$$

$$= \left[\cos^2\theta - (1-\cos^2\theta)\right]\cos\theta - 2(1-\cos^2\theta)\cos\theta$$

Thus:

$$\cos(3\theta) = 4\cos^3\theta - 3\cos\theta.$$

Next,

$$\frac{1}{2} = \cos 60^\circ = \cos\left(3\times 20^\circ\right) = 4\cos^3(20^\circ) - 3\cos(20^\circ) = 4y^3 - 3y.$$

Hence

$$\frac{1}{2} = 4y^3 - 3y \Rightarrow 8y^3 - 6y - 1 = 0.$$

Now put $w = 2y$, and note that $w^3 - 3w - 1 = 0$. Then $y \in \mathbf{L} \Rightarrow w \in \mathbf{L}$. The upshot is that if we could trisect $\angle 60^\circ$, then $w \in \mathbf{L}$ is a root of $p(x) = x^3 - 3x - 1 \in \mathbf{Z}[x]$. Thus $p(x)$ must have a root in **Q**. But the only candidates for **Q**-roots of $p(x)$ are ± 1, and in this case, neither ± 1 is a root of $p(x)$. Thus it is impossible to trisect $\angle 60^\circ$ by ruler and compass, and hence it is impossible to be able to trisect any angle by ruler and compass!

(II) Duplication of the cube. [†] *Given any line segment $\overline{AB}$ with length $\ell_1 = AB$, is it possible to construct by ruler and compass a line segment $\overline{CD}$ with length $\ell_2 = CD$ such that $\ell_2^3 = 2\ell_1^3$? The answer is NO.*

For if it were possible to duplicate the cube, then we could certainly duplicate the length 1 "**L**-line segment" $\overline{AB} := \overline{(0,0),(0,1)}$, to arrive at another "**L**-line segment" $\overline{CD}$ (i.e. C, D are **L**-points) with length $\ell := CD \in \mathbf{L}$ satisfying $\ell^3 = 2 \cdot 1^3 = 2$. I.e. $\ell \in \mathbf{L}$ is a root of $p(x) := x^3 - 2 \in \mathbf{Z}[x]$. Thus $p(x)$ has a **Q**-root. But the only candidates for **Q**-roots of $p(x)$ are ± 1 and ± 2, and neither of these are roots of $p(x)$. Thus it is impossible to be able to duplicate the cube by ruler and compass!

Key Review Points of this Section

1) Let **F** be a subfield of **R**, and let $k \in \mathbf{F}$ be given such that $\sqrt{k} \notin \mathbf{F}$. Then $\mathbf{F}[\sqrt{k}] := \{a + b\sqrt{k} \mid a, b \in \mathbf{F}\}$ is a subfield of **C** (and a subfield of **R** if $k > 0$). Moreover $\mathbf{F}[\sqrt{k}]$ contains **F** as a subfield.

2) Given the setting in 1), let $p(x) \in \mathbf{F}[x]$ be a degree 3 polynomial. Let $z \in \mathbf{F}[\sqrt{k}]$. Then:

   (i) $p(z) = 0 \Leftrightarrow p(\overline{z}) = 0$ (where if $z = a + b\sqrt{k}$, then $\overline{z} = a - b\sqrt{k}$).

   (ii) $p(z) = 0 \Rightarrow p(r) = 0$ for some $r \in \mathbf{F}$.

3) Recall that $\mathbf{L} \subset \mathbf{R}$ is the subfield of **R** generated from $\{0, 1\}$ by $\pm, \bullet, \div, \sqrt{+\text{ve}}$. Let $p(x) \in \mathbf{Q}[x]$ be a degree 3 polynomial, and suppose that $p(z) = 0$ for some $z \in \mathbf{L}$. Then $p(r) = 0$ for some $r \in \mathbf{Q}$.

[†] The volume of a cube with dimensions $\ell - \ell - \ell$ is ℓ^3. Thus the geometric meaning of this is to be able to duplicate the volume of a cube, namely from dimensions $\ell_1 - \ell_1 - \ell_1$ with volume ℓ_1^3 to dimensions $\ell_2 - \ell_2 - \ell_2$ with volume $\ell_2^3 = 2\ell_1^3$.

Appendix: Countability and Uncountability Results

Definition. A set S is said to be countable, if either it is finite, or there is a bijective map $T : \mathbf{N} \to S$. If we put $x_n = T(n),\ n \in \mathbf{N}$, then S can be enumerated in the form $S = \{x_1, x_2, x_3, \ldots\}$.

Claim. (i) Let S be a countable set, and $W \subset S$ a subset. Then W is likewise countable.

(ii) Let I be a countable set, and assume given for each $i \in I$, a countable set W_i. Then $\bigcup_{i \in I} W_i$ is countable.

Reason: (i) We can assume that $S = \{x_1, x_2, x_3, \ldots\}$. Let $j_1 \in \mathbf{N}$ be the smallest integer for which $x_{j_1} \in W$. Next, let j_2 be the smallest integer $> j_1$ for which $x_{j_2} \in W$, and so on. Then we can write $W = \{x_{j_1}, x_{j_2}, x_{j_3}, \ldots\}$, with $n \in \mathbf{N}$ corresponding to x_{j_n}. Clearly W is countable.

(ii) We can assume that $I = \mathbf{N}$ and write $W_i = \{x_{i_1}, x_{i_2}, x_{i_3}, \ldots\}$. We consider the array:

$$\begin{array}{lccccccc}
W_1: & x_{1_1} & x_{1_2} & x_{1_3} & x_{1_4} & x_{1_5} & \cdots \\
W_2: & x_{2_1} & x_{2_2} & x_{2_3} & x_{2_4} & x_{2_5} & \cdots \\
W_3: & x_{3_1} & x_{3_2} & x_{3_3} & x_{3_4} & x_{3_5} & \cdots \\
W_4: & x_{4_1} & x_{4_2} & x_{4_3} & x_{4_4} & x_{4_5} & \cdots \\
W_5: & x_{5_1} & x_{5_2} & x_{5_3} & x_{5_4} & x_{5_5} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots
\end{array}$$

We count along the diagonals (and throw away repeats):

$$\begin{array}{l}
\nearrow\nearrow\nearrow\nearrow\nearrow\nearrow\cdots \\
\nearrow\nearrow\nearrow\nearrow\nearrow\cdots \\
\nearrow\nearrow\nearrow\nearrow\cdots \\
\nearrow\nearrow\nearrow\cdots \\
\vdots\ \ \vdots
\end{array}$$

Thus:

$$\{y_1, y_2, y_3, y_4, y_5, y_6, \ldots\} = \{x_{1_1}, x_{2_1}, x_{1_2}, x_{3_1}, x_{2_2}, x_{1_3}, \ldots\}$$

Every element x_{i_j} will appear as some y_m for some $m \in \mathbf{N}$. Thus $\bigcup W_i$ is countable.

Consequences: (1) $\mathbf{Z}$ is countable. [Reason: $\mathbf{Z} = -\mathbf{N} \cup \{0\} \cup \mathbf{N}$, a countable union of countable.]

(2) $\mathbf{Q}_+ = \{r \in \mathbf{Q} \mid r > 0\}$ is countable, and hence by the same reasoning as in (1), $\mathbf{Q}$ is countable. [Reason: Consider the array:

$$\begin{array}{ccccccc}
\frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \cdots \\
\frac{2}{1} & \frac{2}{2} & \frac{2}{3} & \frac{2}{4} & \frac{2}{5} & \cdots \\
\frac{3}{1} & \frac{3}{2} & \frac{3}{3} & \frac{3}{4} & \frac{3}{5} & \cdots \\
\frac{4}{1} & \frac{4}{2} & \frac{4}{3} & \frac{4}{4} & \frac{4}{5} & \cdots \\
\frac{5}{1} & \frac{5}{2} & \frac{5}{3} & \frac{5}{4} & \frac{5}{5} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \cdots
\end{array}$$

Again, count along the diagonals (and throw away repeats).]

(3) Let $\overline{\mathbf{Q}} = \{\mathbf{C}\text{-roots of all polynomials } p(x) \in \mathbf{Q}[x]\}$. Then $\overline{\mathbf{Q}}$ is countable. [Note: $\overline{\mathbf{Q}}$ is in fact a subfield of $\mathbf{C}$, called the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$.] [Reason: Using countable unions of countable sets are countable, we can first argue that as a set, $\mathbf{Q}[x]$ is countable. This is because $\left[\mathbf{Q}[x]\right]_n := \{p(x) \in \mathbf{Q}[x] \mid \deg p(x) \leq n\} \simeq \mathbf{Q}^{n+1}$, the bijection given by $(a_0, \ldots, a_n) \in \mathbf{Q}^{n+1} \mapsto p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{Q}[x]$, the fact that $\mathbf{Q}^{n+1}$ is countable (first show that $\mathbf{Q}^2$ is countable as in (5) below, and then use induction on $n \in \mathbf{N}$) and that $\mathbf{Q}[x] = \bigcup_{n=0}^{\infty} \left[\mathbf{Q}[x]\right]_n$ is a countable union. Next, the roots of any $p(x) \in \mathbf{Q}[x]$ is finite (bounded by $\deg p(x)$), hence countable. Thus again $\overline{\mathbf{Q}}$ is a countable union of countable sets, hence itself must be countable!]

(4) $\mathbf{L}$ is countable. [Reason: $\mathbf{L}$ is a subset of the countable $\overline{\mathbf{Q}}$.]

(5) the $\mathbf{L}$-plane $\mathbf{L}^2 \subset \mathbf{R}^2$ is countable. [Reason: $\mathbf{L}^2 = \bigcup_{x \in \mathbf{L}} \{x\} \times L$, a countable union of countable sets!]

In contrast to the above results is:

Claim. $\mathbf{R}$ is uncountable (i.e. not countable).

Reason: Assume to the contrary that $\mathbf{R}$ is countable. Then so is the interval subset $(0,1) \subset \mathbf{R}$. For simplicity, we will work in base 2 where a digit for example of the form 0.11011 is the same as $\frac{1}{2} + \frac{1}{2^2} + \frac{0}{2^3} + \frac{1}{2^4} + \frac{1}{2^5}$. Thus $(0,1)$ assumed countable means that it can be enumerated in the form $(0,1) = \{x_1, x_2, x_3, x_4, \ldots\}$, where:

$$\begin{array}{rcl} x_1: & = & 0.x_{11}x_{12}x_{13}x_{14}\ldots \\ x_1: & = & 0.x_{11}x_{12}x_{13}x_{14}\ldots \\ x_2: & = & 0.x_{21}x_{22}x_{23}x_{24}\ldots \\ x_3: & = & 0.x_{31}x_{32}x_{33}x_{34}\ldots \\ x_4: & = & 0.x_{41}x_{42}x_{43}x_{44}\ldots \\ \vdots & \vdots & \vdots \end{array}$$

and $x_{ij} \in \{0,1\}$. Now set $y = 0.y_1y_2y_3y_4\ldots$, where $y_j = \begin{cases} 1 & \text{if } x_{jj} = 0 \\ 0 & \text{if } x_{jj} = 1 \end{cases}$. Then it is obvious that $y \in (0,1)$ and yet y does not appear in the enumerated description of $(0,1)$ above. Thus $\mathbf{R}$ must be uncountable!

Appendix: Ordered Fields

The real numbers is an example of an ordered field under $<$. The axiomatic properties of $<$ on $\mathbf{R}$ are as follows:

(1) Trichotomy. For any $a, b \in \mathbf{R}$, exactly one of the following holds:

(i) $a < b$
(ii) $a = b$
(iii) $b < a$

(2) Transitivity. $a < b$ and $b < c \Rightarrow a < c$.

Interaction with the binary operations:

(3) $a > 0$ and $b > 0 \Rightarrow ab > 0$.

(4) $a < b \Rightarrow a + c < b + c$ for all $c \in \mathbf{R}$.

Claim. $a < b$ and $c < d \Rightarrow a + c < b + d$

Reason: Applying (4) first, and then (2) above, we have

$$a + c < b + c < b + d, \quad \Rightarrow \ a + c < b + d.$$

Claim. $a < b \Leftrightarrow b - a > 0$.

Reason: By (4) above, $a < b \Leftrightarrow 0 = a + (-a) < b + (-a)$, i.e. $b - a > 0$.

Claim. $a < b$ and $c > 0 \Rightarrow ac < bc$.

Reason: $a < b \Rightarrow b - a > 0$, hence by (3), $c(b - a) > 0$, and thus $ac < bc$.

Claim. $a > 0 \Leftrightarrow -a < 0$.

Reason: Since $-(-a) = 0$, it sufices to show that $a > 0 \Rightarrow -a < 0$. But by (4) above, $a > 0 \Rightarrow 0 = a + (-a) > 0 + (-a) = -a$, i.e. $-a < 0$.

Claim. $1 > 0$.

Reason: Suppose to the contrary that $1 \not> 0$. Then by (1) above, and since $1 \neq 0$ ($\mathbf{R}$ is a field!), we must have $1 < 0$. Hence $-1 > 0$ by the above claim. Thus $1 = (-1)(-1) > 0$ by (3) above, a contradiction to $1 \not> 0$. Thus $1 > 0$.

Claim. $a > 0 \Leftrightarrow a^{-1} > 0$.

Reason: Since $(a^{-1})^{-1} = a$, it suffices to show that $a > 0 \Rightarrow a^{-1} > 0$. Suppose to the contrary that $a > 0$ and yet $a^{-1} < 0$. Then $-a^{-1} > 0$, and hence $-1 = a \cdot \left(-a^{-1}\right) > 0$, i.e. $1 < 0$, which is not the case.

Definition. Let S be a set. An order relation "$<$" on S is a relation[†] satisfying the following:

(1) Trichotomy. For any $a, b \in S$, exactly one of the following holds:

(i) $a < b$
(ii) $a = b$
(iii) $b < a$

(2) Transitivity. $a < b$ and $b < c \Rightarrow a < c$.

Definition. Suppose $\mathbf{F}$ is a field, and assume that as a set $\mathbf{F}$ is ordered with given order relation $<$. Then $[\mathbf{F}; +, \bullet, <]$ is an ordered field if:

(3) $a > 0$ and $b > 0 \Rightarrow ab > 0$.

(4) $a < b \Rightarrow a + c < b + c$ for all $c \in \mathbf{F}$.

Remarks. (a) It is obvious that the above claims for $[\mathbf{R}; +, \bullet, <]$, likewise hold for an ordered field $[\mathbf{F}; +, \bullet, <]$.

(b) Any subset $S \subset \mathbf{R}$ is an ordered set.

(c) Any subfield of $\mathbf{R}$ is an ordered field. [Thus for example, $\mathbf{Q}$, $\mathbf{Q}[\sqrt{2}]$ are ordered fields.]

(d) $\mathbf{Z}_2$ is not an ordered field. [Reason: If $\overline{1} > \overline{0}$, then $\overline{0} = \overline{1} + \overline{1} > \overline{1} + \overline{0}$, i.e. $\overline{1} < \overline{0}$, which violates trichotomy!]

(e) [Generalization of (d).] Any ordered field $\mathbf{F}$ is infinite. More precisely, the characteristic, $\mathrm{Char}(\mathbf{F}) = 0$.

Reason: Since $[\mathbf{F}; +, \bullet, <]$ is ordered, we know that $1 > 0$. Hence $2 := 1+1 > 0+1 = 1$. Likewise $3 := 2 + 1 > 1 + 1 = 2$, $4 := 1 + 3 > 1 + 2 = 3$, and so on. Thus by transitivity,

$$1 < 2 < 3 < 4 < 5 < 6 < 7 < \cdots,$$

is a subset of distinct elements. [In short $\mathbf{N} \hookrightarrow \mathbf{F}$, i.e. one can "count" in $\mathbf{F}$.]

[†] As defined earlier in the notes, around the time we defined equivalence relations.

(f) Not every infinite field is an ordered field[††] For example:

Claim. $\mathbf{C}$ is not an ordered field. [Note that $\mathrm{Char}(\mathbf{C}) = 0$.]

Reason: Suppose to the contrary that $\mathbf{C}$ is ordered, with order relation $<$. Since $\sqrt{-1} \neq 0$, it follows from trichotomy that either $\sqrt{-1} > 0$ or $\sqrt{-1} < 0$. But if $\sqrt{-1} > 0$, then $-1 = (\sqrt{-1})^2 > 0$ by (3) above, which is not the case. On the other hand, if $\sqrt{-1} < 0$, then $-\sqrt{-1} > 0$, and thus $-1 = (-\sqrt{-1})^2 > 0$, which again cannot happen. Therefore trichotomy fails, i.e. $\mathbf{C}$ cannot be ordered.

[††] For example, the class of fields in characteristic $p > 0$ that are "algebraically closed".

MATH 228 SAMPLE MIDTERM EXAM #1

Instructor: James D. Lewis

This is a closed book exam. No calculators.
All questions have equal weight.

---

1. Prove by induction:

$$P(n) : 1 + 3 + 5 + \cdots + (2n - 1) = n^2,$$

for all integers $n \geq 1$.

2. (i) Find all the units in $\mathbf{Z}_8$.

(ii) Find the multiplicative inverse of $\overline{71}$ in $\mathbf{Z}_{88}$.

(iii) Find <u>one</u> zero divisor in $\mathbf{Z}_{142}$.

3. (i) Show that

$$\mathbf{A} \stackrel{\text{def}}{=} \{p + q\sqrt{3} \mid p,\ q \in \mathbf{Q}\},$$

is a subfield of $\mathbf{R}$. [You may assume the class result that $\sqrt{3}$ is irrational.]

4. Consider the subset $3\mathbf{Z}_{12} = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} \subset \mathbf{Z}_{12}$.

(i) Show that $3\mathbf{Z}_{12}$ is a subring of $\mathbf{Z}_{12}$.

(ii) What is the unity element of $3\mathbf{Z}_{12}$?

(iii) Find all units and zero divisors of $3\mathbf{Z}_{12}$.

MATH 228 SAMPLE MIDTERM EXAM #2

Instructor: James D. Lewis

This is a closed book exam. No calculators.
All questions have equal weight.

---

1. Assume given a ring A with unity, consisting of 4 distinct elements: $A = \{a, b, c, d\}$, and where addition and multiplication are given by the tables below.

$+$	a	b	c	d
a	c	d	a	b
b	d	a	b	c
c	a	b	c	d
d	b	c	d	a

$\bullet$	a	b	c	d
a	c	a	c	a
b	a	d	c	b
c	c	c	c	c
d	a	b	c	d

Answer the following:

(i) Which of $\{a, b, c, d\}$ is the zero element?

(ii) Which of $\{a, b, c, d\}$ is the unity?

(iii) Which of $\{a, b, c, d\}$ is the additive inverse of b?

(iv) Find all units in A.

(v) Find all zero divisors in A.

2. (i) Find all the units in $\mathbf{Z}_{14}$.

(ii) Compute $d = \mathrm{GCD}(97, 105)$ and find integers x and y such that $d = x \cdot 97 + y \cdot 105$.

(iii) Find the multiplicative inverse of $\overline{97}$ in $\mathbf{Z}_{105}$.

3. Show that $\sqrt{15}$ is irrational.

4. Let $\mathbf{C} = \{z = x+iy \mid x,\ y \in \mathbf{R}\}$ be the field of complex numbers (and where $i = \sqrt{-1}$), as introduced in class. We also recall the subring $\mathbf{A} \subset \mathbf{C}$ of Gaussian integers given by

$$\mathbf{A} = \{z = x + iy \in \mathbf{C} \mid x,\ y \in \mathbf{Z}\}.$$

We introduce a relation $\sim$ on $\mathbf{C}$ by the rule:

$$z_1 \sim z_2 \text{ if } z_1 - z_2 \in \mathbf{A}.$$

Show that $\sim$ is an equivalence relation on $\mathbf{C}$.

MATH 228 SOLUTIONS TO SAMPLE MIDTERM EXAM #1

---

1. Prove by induction:

$$P(n) : 1 + 3 + 5 + \cdots + (2n-1) = n^2,$$

for all integers $n \geq 1$.

Solution: Case $n = 1$: $1 = 1^2 \Rightarrow P(1)$ is true. Induction Step: Show that $P(n)$ true $\Rightarrow P(n+1)$ true. Simply add $2n + 1 = (2(n+1) - 1)$ to both sides of statement $P(n)$. Thus:

$$1 + 3 + 5 + \cdots + (2n-1) + (2(n+1) - 1) = n^2 + 2n + 1 = (n+1)^2.$$

Thus $P(n)$ true $\Rightarrow P(n+1)$ true, and we're done.

2. (i) Find all the units in $\mathbf{Z}_8$.

Answer: $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$.

(ii) Find the multiplicative inverse of $\overline{71}$ in $\mathbf{Z}_{88}$.

Answer: First, by Euclid,

$$\begin{array}{rcl} 88 &=& 1 \times 71 + 17 \\ 71 &=& 4 \times 17 + 3 \\ 17 &=& 5 \times 3 + 2 \\ 3 &=& 1 \times 2 + 1 \end{array} \quad \Rightarrow \quad \begin{array}{rcl} 1 &=& 3 - 2 = 3 - (17 - 5 \times 3) \\ &=& 6 \times 3 - 17 = 6 \times (71 - 4 \times 17) - 17 \\ &=& 6 \times 71 - 25 \times 17 = 6 \times 71 - 25 \times (88 - 71) \\ &=& 31 \times 71 - 25 \times 88 \end{array}$$

Thus $\overline{71}^{-1} = \overline{31} \in \mathbf{Z}_{88}$

(iii) Find one zero divisor in $\mathbf{Z}_{142}$ (other than $\overline{0}$).

Answer Choose any non-zero $\overline{m} \in \mathbf{Z}_{142}$ such that $(m, 142) > 1$. For example $\overline{71}$ will do. [Note: $\overline{71} \cdot \overline{2} = \overline{142} = \overline{0}$.]

3. (i) Show that

$$\mathbf{A} \stackrel{\text{def}}{=} \{p + q\sqrt{3} \mid p,\ q \in \mathbf{Q}\},$$

is a subfield of $\mathbf{R}$. [You may assume the class result that $\sqrt{3}$ is irrational.]

Solution: Set $z = p + q\sqrt{3}$, $w = a + b\sqrt{3} \in \mathbf{A}$, i.e. where $p, q, a, b \in \mathbf{Q}$. Then:

$$z + w = \underbrace{(p + a)}_{\in \mathbf{Q}} + \underbrace{(q + b)}_{\in \mathbf{Q}} \sqrt{3} \in \mathbf{A}.$$

$$z \cdot w = \underbrace{(p \cdot a + 3q \cdot b)}_{\in \mathbf{Q}} + \underbrace{(p \cdot b + q \cdot a)}_{\in \mathbf{Q}} \sqrt{3} \in \mathbf{A}.$$

Thus $\mathbf{A}$ is closed under $+, \bullet$ from $\mathbf{R}$, and hence the associative, commutative and distributive laws hold for $\mathbf{A}$, since the same laws hold for $\mathbf{R}$. Note that $\mathbf{Q} = \{p + 0 \cdot \sqrt{3} \mid p \in \mathbf{Q}\} \subset \mathbf{A}$. Thus $0, 1 \in \mathbf{A}$ and $1 \neq 0$. Also we have additive inverses: $-z = (-p) + (-q)\sqrt{3} \in \mathbf{A}$. Finally, since $\sqrt{3} \notin \mathbf{Q}$, it follows that

$$z = p + q\sqrt{3} = 0 \Leftrightarrow p = q = 0 \Leftrightarrow p^2 - 3q^2 = 0.$$

Thus if $z = p + q\sqrt{3} \neq 0$, then from the formal calculation:

$$\frac{1}{z} = \left(\frac{1}{p + q\sqrt{3}}\right)\left(\frac{p - q\sqrt{3}}{p - q\sqrt{3}}\right) = \left(\frac{p}{p^2 - 3q^2}\right) + \left(\frac{-q}{p^2 - 3q^2}\right)\sqrt{3},$$

it follows that z^{-1} is given by the formula:

$$z^{-1} = \left(\frac{p}{p^2 - 3q^2}\right) + \left(\frac{-q}{p^2 - 3q^2}\right)\sqrt{3} \in \mathbf{A}.$$

Thus $\mathbf{A}$ is a subfield of $\mathbf{R}$.

4. Consider the subset $3\mathbf{Z}_{12} = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} \subset \mathbf{Z}_{12}$.

(i) Show that $3\mathbf{Z}_{12}$ is a subring of $\mathbf{Z}_{12}$.

Solution: The $+, \bullet$ tables are:

$+$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$
$\overline{0}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$
$\overline{3}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{0}$
$\overline{6}$	$\overline{6}$	$\overline{9}$	$\overline{0}$	$\overline{3}$
$\overline{9}$	$\overline{9}$	$\overline{0}$	$\overline{3}$	$\overline{6}$

$\bullet$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{3}$	$\overline{0}$	$\overline{9}$	$\overline{6}$	$\overline{3}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$
$\overline{9}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$

Since the values in the tables belongs to $3\mathbf{Z}_{12}$, it follows that $3\mathbf{Z}_{12}$ is closed under $+, \bullet$ from $\mathbf{Z}_{12}$ Thus the associative, commutative and distributive laws hold for $3\mathbf{Z}_{12}$, since they hold for $\mathbf{Z}_{12}$. Obviously $\overline{0} \in 3\mathbf{Z}_{12}$ is the zero element, and there are additive inverses. [E.g. $-\overline{3} = \overline{9},\ -\overline{6} = \overline{6}$, etc.] Thus $3\mathbf{Z}_{12}$ is a subring of $\mathbf{Z}_{12}$

(ii) What is the unity element of $3\mathbf{Z}_{12}$?

Answer: From the $(\bullet)$ table, $\overline{9}$ is the unity.

(iii) Find all units and zero divisors of $3\mathbf{Z}_{12}$.

Answer: From the $(\bullet)$ table, $\left(3\mathbf{Z}_{12}\right)^* = \{\overline{3}, \overline{9}\}$. The zero divisors are $\{\overline{0}, \overline{6}\}$.

MATH 228 SOLUTIONS TO SAMPLE MIDTERM EXAM #2

---

1. Assume given a ring A with unity, consisting of 4 distinct elements: $A = \{a, b, c, d\}$, and where addition and multiplication are given by the tables below.

$+$	$\|\|$	a	b	c	d
a	$\|\|$	c	d	a	b
b	$\|\|$	d	a	b	c
c	$\|\|$	a	b	c	d
d	$\|\|$	b	c	d	a

$\bullet$	$\|\|$	a	b	c	d
a	$\|\|$	c	a	c	a
b	$\|\|$	a	d	c	b
c	$\|\|$	c	c	c	c
d	$\|\|$	a	b	c	d

Answer the following:

(i) Which of $\{a, b, c, d\}$ is the zero element?

Answer: c

(ii) Which of $\{a, b, c, d\}$ is the unity?

Answer: d

(iii) Which of $\{a, b, c, d\}$ is the additive inverse of b?

Answer: d

(iv) Find all units in A.

Answer: $\{b, d\}$

(v) Find all zero divisors in A.

Answer: $\{c, a\}$

2. (i) Find all the units in $\mathbf{Z}_{14}$.

Answer: $\{\overline{1}, \overline{3}, \overline{5}, \overline{9}, \overline{11}, \overline{13}\}$.

(ii) Compute $d = \mathrm{GCD}(97, 105)$ and find integers x and y such that $d = x \cdot 97 + y \cdot 105$.

Solution: By Euclid:

$$\left.\begin{array}{rcl} 105 & = & 1 \times 97 + 8 \\ 97 & = & 12 \times 8 + 1 \end{array}\right\} \Rightarrow (105, 97) = 1.$$

Next, by back substitution:

$$1 = 97 - 12 \times (105 - 97) = 13 \times 97 + (-12) \times 105.$$

Thus $x = 13$ and $y = -12$ will do.

(iii) Find the multiplicative inverse of $\overline{97}$ in $\mathbf{Z}_{105}$.

Answer: By the previous part, $\overline{97}^{-1} = \overline{13}$.

3. Show that $\sqrt{15}$ is irrational.

Solution: Suppose to the contrary that $\sqrt{15} \in \mathbf{Q}$. Then we can write $\sqrt{15} = p/q$, where $p, q \in \mathbf{N}$, and $(p, q) = 1$. Thus $15q^2 = p^2$. Next, $15 = 3 \cdot 5$, and hence $3|p$ and $5|p$. Therefore by the Fundamental Theorem of Arithmetic $15|p$, and so $p = 15 \cdot p_1$. Thus $15q^2 = (15)^2 p_1^2$, i.e. $q^2 = 15p_1^2$. By the same reasoning, $15|q$, and hence $(p, q) \geq 15$, which violates $(p, q) = 1$. Therefore $\sqrt{15} \notin \mathbf{Q}$.

4. Let $\mathbf{C} = \{z = x + iy \mid x,\ y \in \mathbf{R}\}$ be the field of complex numbers (and where $i = \sqrt{-1}$), as introduced in class. We also recall the subring $\mathbf{A} \subset \mathbf{C}$ of Gaussian integers given by

$$\mathbf{A} = \{z = x + iy \in \mathbf{C} \mid x,\ y \in \mathbf{Z}\}.$$

We introduce a relation $\sim$ on $\mathbf{C}$ by the rule:

$$z_1 \sim z_2 \text{ if } z_1 - z_2 \in \mathbf{A}.$$

Show that $\sim$ is an equivalence relation on $\mathbf{C}$.

Solution: Let $z \in \mathbf{C}$. Then $z - z = 0 + i0 \in \mathbf{A}$, hence $z \sim z$. Next, for $z, w \in \mathbf{C}$,

$$z \sim w \Leftrightarrow z - w \in \mathbf{A} \Leftrightarrow w - z = -(z - w) \in \mathbf{A} \Leftrightarrow w \sim z.$$

Finally, for $z, w, v \in \mathbf{C}$, $z \sim w$ and $w \sim v \Rightarrow z - w \in \mathbf{A}$ and $w - v \in \mathbf{A}$. Thus

$$z - v = \underbrace{(z - w)}_{\in \mathbf{A}} + \underbrace{(w - v)}_{\in \mathbf{A}} \in \mathbf{A}.$$

Hence $z \sim v$, and we're done.

Sample Problems 1

In the exercises below you may assume $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ are fields.

1. Consider the 3 element set $\mathbf{F}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ with binary operations $+$, $\bullet$ given by the tables below.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Verify that $[\mathbf{F}_3, +, \bullet]$ is a field. [Note: For the associative and distributive laws, just do a couple sample calculations for each.]

2. Verify that $\mathbf{A} \stackrel{\text{def}}{=} \{a + b\sqrt{-1} \mid a, b \in \mathbf{Q}\}$ is a subfield of the complex numbers $\mathbf{C}$.

3. Let $\mathbf{A} = \{\frac{p}{2^q} \mid p, q \in \mathbf{Z} \text{ and } q \geq 0\}$. Recall that $\mathbf{A}$ is a subring (with unity) of $\mathbf{Q}$. Compute the group of units $\mathbf{A}^*$.

4. Prove by induction that

$$1 + 5 + 9 + \cdots + (4n + 1) = (2n + 1)(n + 1)$$

for all integers $n \geq 0$.

5. Prove by induction that

$$1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n} = \frac{2^{n+1} - 1}{2^n}$$

for all integers $n \geq 0$.

Sample Problems 2

---

1. Compute the GCD $(750, 495)$ by the Euclidean division algorithm method done in class.

2. Compute the GCD $(11232, 2268)$ by the Euclidean division algorithm method done in class.

3. Compute GCD $(144, 756)$ and LCM $[144, 756]$ by factoring into products of primes.

4. If $a,\ b \in \mathbf{N}$ are relatively prime, show that

$$[a, b] = a \cdot b.$$

[Hint: This is easier than it looks.]

5. Find integers x and y for which $d = (19, 7)$ is a combination of the form

$$d = x \cdot 7 + y \cdot 19.$$

6. Without factoring into primes, compute $[192, 66]$.

Sample Problems 3

---

1. Consider the ring $\mathbf{A} = \{0, a, b, c\}$ of 4 distinct elements, with multiplication table below:

$\bullet$	0	a	b	c
0	0	0	0	0
a	0	0	b	a
b	0	b	c	b
c	0	a	b	c

Answer the following:

(i) Is there a unity for $\mathbf{A}$? [If so, what element is it?]

(ii) If the answer to (i) is yes, compute the group of units $\mathbf{A}^*$.

(iii) Compute the zero divisors in $\mathbf{A}$.

(iv) Is $\mathbf{A}$ an integral domain? [State your reasons.]

(v) Is $\mathbf{A}$ a field? [State your reasons.]

2. (i) Compute the group of units, and zero divisors in $\mathbf{Z}_{15}$.

(ii) Find the multiplicative inverse of $\overline{23}$ in $\mathbf{Z}_{30}$.

(iii) By first showing that $3\mathbf{Z}_{15} \stackrel{\text{def}}{=} \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}\} \subset \mathbf{Z}_{15}$ is a subring of $\mathbf{Z}_{15}$, show that $3\mathbf{Z}_{15}$ is a field.

3. Define a relation $\sim$ on the real numbers $\mathbf{R}$ as follows: $x \sim y \Leftrightarrow x = 2^q y$ for some integer $q \in \mathbf{Z}$. Verify that $\sim$ is an equivalence relation.

4. Find all values $\overline{x}$ in $\mathbf{Z}_8$ which satisfy the equation $\overline{x}^2 = \overline{1}$.

5. Show that $\sqrt{30}$ is irrational.

Sample Problems 4

Find all solutions of the given equations in the given field $\mathbf{Z}_p$.

1. $\overline{5}x + \overline{66} = \overline{0}$ in $\mathbf{Z}_{101}$.

2. $x^2 + \overline{3}x + \overline{2} = \overline{0}$ in $\mathbf{Z}_5$.

3. $x^2 + \overline{10}x + \overline{24} = \overline{0}$ in $\mathbf{Z}_{101}$.

4. $x^2 = \overline{2}$ in $\mathbf{Z}_7$.

5. $x^2 = \overline{18}$ in $\mathbf{Z}_{31}$.

Perform the indicated operation.

6. $(\overline{4}x + \overline{3})(\overline{5}x + \overline{6})$ in $\mathbf{Z}_7[x]$.

7. $(\overline{2}x^3 + \overline{3}x^2 - \overline{5}x + \overline{1})/(x + \overline{4})$ in $\mathbf{Z}_7[x]$ (long division).

8. $(\overline{4}x^2 + \overline{7}x + \overline{3}) + (\overline{8}x^2 + \overline{5}x + \overline{11})$ in $\mathbf{Z}_{12}[x]$.

Factor completely into a product of irreducibles.

9. $x^2 + \overline{6}x + \overline{1}$ in $\mathbf{Z}_7[x]$.

10. $x^4 + \overline{9}x^2 + \overline{7}$ in $\mathbf{Z}_{11}[x]$.

---

11. Explain why $x^3 + \overline{3}x + \overline{2}$ is irreducible in $\mathbf{Z}_5[x]$.

Sample Problems 5

[1.] (i) Show that $2x^3 + 3x^2 + x - 1$ has no rational roots.

(ii) Show that $x^3 - 3x - 1$ has no rational roots.

(iii) Determine the rational root(s) of $p(x) = x^4 + 3x^3 - 3x^2 - 10x - 3$ and factor $p(x)$ as a product of irreducibles in $\mathbf{Q}[x]$. [Hint: Use (ii).]

[2.] Let $\mathbf{F}$ be a field, and $f(x) \in \mathbf{F}[x]$ a polynomial of degree 1. Prove that $f(x)$ is irreducible.

[3.] (i) Let $T : \mathbf{Q}[x] \to \mathbf{Q}$ be the map given by $p(x) \in \mathbf{Q}[x] \mapsto T(p(x)) := p(0) \in \mathbf{Q}$. Show that T is a ring homomorphism. Describe the kernel, $\ker T$. Also, what is the image of T?

(ii) Explain why the map $g : \mathbf{R} \to \mathbf{R}$ given by $g(t) = t^2$, is not a ring homomorphism.

[4.] Let A be a ring, and fix $a \in A$. Show that $(a) := \{ba \mid b \in A\}$ is an ideal in A.

[5.] Give an example of a ring A, and a non-zero element $a \in A$ for which $(a) = 0$. [Hint: Choose A to be a suitable subring of $\mathbf{Z}_4$.]

[6.] Let $f : \mathbf{Z}_{12} \to \mathbf{Z}_4$ be given by the prescription $f(\overline{x}_{12}) = \overline{x}_4$.

(i) Show that f is a well defined ring homomorphism.

(ii) Compute the kernel, $\ker f$.

[7.] Give an example of the following: An integral domain A and an ideal $\mathcal{U} \subset A$ such that the quotient ring $A/\mathcal{U}$ is not an integral domain.

Solutions to Sample Problems 1

In the exercises below you may assume $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ are fields.

1. Consider the 3 element set $\mathbf{F}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ with binary operations $+$, $\bullet$ given by the tables below.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Verify that $[\mathbf{F}_3, +, \bullet]$ is a field. [Note: For the associative and distributive laws, just do a couple sample calculations for each.]

Solution: We must verify the 9 properties for a field. The values in the tables belong to the set $\mathbf{F}_3$, hence $\mathbf{F}_3$ is closed under $+, \bullet$. Also, the tables are symmetric about the diagonal, hence commutivity holds as well. Since the set has 3 elements, it follows that $\overline{1} \neq \overline{0}$. Of course all elements of $\mathbf{F}_3$ are preserved under multiplication by $\overline{1}$, and addition by $\overline{0}$. Thus $\overline{1}$ is the unity and $\overline{0}$ is the zero element. Next, "$-\overline{0}$" $= \overline{0}$, "$-\overline{1}$" $= \overline{2}$, and "$-\overline{2}$" $= \overline{1}$. Hence we have additive inverses. Also "$\overline{1}^{-1}$" $= \overline{1}$ and "$\overline{2}^{-1}$" $= \overline{2}$, and so we have multiplicative inverses for non-zero elements. The only thing left to check are the associative and distributive laws. We just do a sample of calculations here:

Associativity. $(\overline{1} + \overline{2}) + \overline{1} = \overline{0} + \overline{1} \quad = \quad \overline{1} \quad = \quad \overline{1} + \overline{0} = \overline{1} + (\overline{2} + \overline{1})$.

$(\overline{1} \bullet \overline{2}) \bullet \overline{1} = \overline{2} \bullet \overline{1} \quad = \quad \overline{2} \quad = \quad \overline{1} \bullet \overline{2} = \overline{1} \bullet (\overline{2} \bullet \overline{1})$.

Distributive. $\overline{2} \bullet (\overline{1} + \overline{2}) = \overline{2} \bullet \overline{0} \quad = \quad \overline{0} \quad = \quad \overline{2} + \overline{1} = \overline{2} \bullet \overline{1} + \overline{2} \bullet \overline{2}$.

2. Verify that $\mathbf{A} \stackrel{\text{def}}{=} \{a + b\sqrt{-1} \mid a, b \in \mathbf{Q}\}$ is a subfield of the complex numbers $\mathbf{C}$.

Solution: We first check closure of $\mathbf{A}$ under $+, \bullet$ from $\mathbf{C}$. Let $z = a + b\sqrt{-1}$, $w = c + d\sqrt{-1} \in \mathbf{A}$. Note that $a, b, c, d \in \mathbf{Q}$, hence $(a + c), (b + d), (ac - bd), (ad + bc) \in \mathbf{Q}$. Therefore

$$z + w = (a + c) + (b + d)\sqrt{-1} \in \mathbf{A},$$

$$zw = (ac - bd) + (ad + bc)\sqrt{-1} \in \mathbf{A}.$$

Thus $\mathbf{A}$ is closed under $+, \bullet$ from $\mathbf{C}$, and since the commutative, associative and distributive laws hold for $\mathbf{C}$, the same laws must hold for $\mathbf{A}$. Note that $\mathbf{Q} \subset \mathbf{A}$, where $r \in \mathbf{Q}$ is the same as $r + 0\sqrt{-1} \in \mathbf{A}$. Thus $1, 0 \in \mathbf{A}$ and $1 \neq 0$. So we have a unity and zero element. Next, $z = a + b\sqrt{-1} \in \mathbf{A} \Rightarrow -z := (-a) + (-b)\sqrt{-1} \in \mathbf{A}$. Hence we have additive inverses. Finally, we must show that we have multiplicative inverses of non-zero elements. We recall from class notes, that given $z = a + b\sqrt{-1} \in \mathbf{A}$, it is the case that $z = 0 \Leftrightarrow a = b = 0$. Further, it is clear that $z \neq 0 \Rightarrow a^2 + b^2 \neq 0$. Now assume that $z \neq 0$. Then from the formal calculation:

$$\frac{1}{z} = \frac{1}{a + b\sqrt{-1}} = \left(\frac{1}{a + b\sqrt{-1}}\right)\left(\frac{a - b\sqrt{-1}}{a - b\sqrt{-1}}\right) = \left(\frac{a - b\sqrt{-1}}{a^2 + b^2}\right),$$

we arrive at the formula for z^{-1}, namely:

$$z^{-1} = \left(\frac{a}{a^2 + b^2}\right) \; + \; \left(\frac{-b}{a^2 + b^2}\right)\sqrt{-1} \in \mathbf{A}.$$

3. Let $\mathbf{A} = \{\frac{p}{2^q} \mid p, q \in \mathbf{Z} \text{ and } q \geq 0\}$. Recall that $\mathbf{A}$ is a subring (with unity) of $\mathbf{Q}$. Compute the group of units $\mathbf{A}^*$.

Solution: Let $x \in \mathbf{A}$. Recall that x is a unit if there exists $y \in \mathbf{A}$ such that $xy = 1$. If we write $x = \frac{p_1}{2^{q_1}}$ and $y = \frac{p_2}{2^{q_2}}$, then:

$$xy = 1 \Leftrightarrow \frac{p_1 p_2}{2^{q_1 + q_2}} = 1 \Leftrightarrow p_1 p_2 = 2^{q_1 + q_2}.$$

But $p_1, p_2, p_1 p_2$ are integers, and $2^{q_1+q_2}$ is the prime decomposition of $p_1 p_2$. Hence p_1 (and p_2) must be a power of 2. What that means is that $x = \pm 2^q$ for some $q \in \mathbf{Z}$. Thus:

$$\mathbf{A}^* = \{\pm 2^q \mid q \in \mathbf{Z}\} = \{\ldots, \pm\frac{1}{16}, \pm\frac{1}{8}, \pm\frac{1}{4}, \pm\frac{1}{2}, \pm 1, \pm 2, \pm 4, \pm 8, \pm 16, \ldots\}.$$

4. Prove by induction that

$$1 + 5 + 9 + \cdots + (4n + 1) = (2n + 1)(n + 1)$$

for all integers $n \geq 0$.

Solution: Let $P(n)$ be the statement

$$\underbrace{1 + 5 + 9 + \cdots + (4n + 1)}_{\text{LHS}} = \underbrace{(2n + 1)(n + 1)}_{\text{RHS}}, \quad n = 0, 1, 2, \ldots.$$

Case $n = 0$: LHS $= 4 \cdot 0 + 1 = 1 = (2 \cdot 0 + 1)(0 + 1)$, hence $P(0)$ is true.

Induction Step ($P(n)$ true $\Rightarrow P(n+1)$ true): We assume given that $P(n)$ is true, and add $\big(4(n+1)+1\big)$ to both LHS and RHS. Thus:

$$1+5+9+\cdots+\big(4(n+1)+1\big) = (2n+1)(n+1)+\big(4(n+1)+1\big),$$

i.e.

$$1+5+9+\cdots+\big(4(n+1)+1\big) = 2n^2+7n+6 = (2n+3)(n+2) = \big(2(n+1)+1\big)\big((n+1)+1\big).$$

Hence $P(n+1)$ is true. This completes the induction step, and hence the proof.

5. Prove by induction that

$$1+\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{2^n} = \frac{2^{n+1}-1}{2^n}$$

for all integers $n \geq 0$.

Solution: Let $P(n)$ be the statement

$$\underbrace{1+\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{2^n}}_{\text{LHS}} = \underbrace{\frac{2^{n+1}-1}{2^n}}_{\text{RHS}}, \quad n = 0, 1, 2, \ldots.$$

Case $n=0$: LHS $= \frac{1}{2^0} = 1 = \frac{2^{1-0}-1}{2^0}$, hence $P(0)$ is true.

Induction Step ($P(n)$ true $\Rightarrow P(n+1)$ true): We assume given that $P(n)$ is true, and add $\frac{1}{2^{n+1}}$ to both LHS and RHS. Thus:

$$1+\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{2^{n+1}} = \frac{2^{n+1}-1}{2^n}+\frac{1}{2^{n+1}},$$

i.e.

$$1+\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{2^{n+1}} = \frac{2^{n+1}-1}{2^n}+\frac{1}{2^{n+1}}$$

$$= \frac{2\cdot(2^{n+1}-1)+1}{2^{n+1}} = \frac{2^{n+2}-2+1}{2^{n+1}} = \frac{2^{(n+1)+1}-1}{2^{(n+1)}}.$$

Hence $P(n+1)$ is true. This completes the induction step, and hence the proof.

Solutions to Sample Problems 2

---

1. Compute the GCD $(750, 495)$ by the Euclidean division algorithm method done in class.

Solution: By Euclidean division,

$$\left\{\begin{array}{rcrcrcr} 750 & = & 1 & \times & 495 & + & 255 \\ 495 & = & 1 & \times & 255 & + & 240 \\ 255 & = & 1 & \times & 240 & + & 15 \\ 240 & = & 16 & \times & 15 & + & 0 \end{array}\right\} \Rightarrow (750, 495) = 15.$$

2. Compute the GCD $(11232, 2268)$ by the Euclidean division algorithm method done in class.

Solution: By Euclidean division,

$$\left\{\begin{array}{rcrcrcr} 11232 & = & 4 & \times & 2268 & + & 2160 \\ 2268 & = & 1 & \times & 2160 & + & 108 \\ 2160 & = & 20 & \times & 108 & + & 0 \end{array}\right\} \Rightarrow (11232, 2268) = 108.$$

3. Compute GCD $(144, 756)$ and LCM $[144, 756]$ by factoring into products of primes.

Solution: By factoring into primes, we have:

$$\left.\begin{array}{rcl} 144 & = & 2^4 3^2 7^0 \\ 756 & = & 2^2 3^3 7^1 \end{array}\right\} \Rightarrow \begin{array}{rcrcr} (144, 756) & = & 2^2 3^2 7^0 & = & 36 \\ [144, 756] & = & 2^4 3^3 7^1 & = & 3024 \end{array}$$

4. If $a,\ b \in \mathbf{N}$ are relatively prime, show that

$$[a, b] = a \cdot b.$$

[Hint: This is easier than it looks.]

Solution: Recall that a, b are relatively prime $\Leftrightarrow (a, b) = 1$. Therefore, from the formula in class, we have:

$$[a, b] = \frac{a \cdot b}{(a, b)} = a \cdot b.$$

5. Find integers x and y for which $d = (19, 7)$ is a combination of the form

$$d = x \cdot 7 + y \cdot 19.$$

Solution: By Euclidean division,

$$\left\{ \begin{array}{rcrcrcr} 19 & = & 2 & \times & 7 & + & 5 \\ 7 & = & 1 & \times & 5 & + & 2 \\ 5 & = & 2 & \times & 2 & + & 1 \end{array} \right\} \Rightarrow (19, 7) = 1.$$

We now back substitute:

$$1 = 5 - 2 \times \big[2 = 7 - 1 \times 5\big] = (-2) \times 7 \ + \ 3 \times \big[5 = 19 - 2 \times 7\big] = (-8) \times 7 + 3 \times 19.$$

Thus $x = -8$ and $y = 3$ will work.

6. Without factoring into primes, compute $[192, 66]$.

Solution: From the formula in class, we have:

$$[192, 66] = \frac{192 \times 66}{(192, 66)}.$$

By Euclid,

$$\left\{ \begin{array}{rcrcrcr} 192 & = & 2 & \times & 66 & + & 60 \\ 66 & = & 1 & \times & 60 & + & 6 \\ 60 & = & 10 & \times & 6 & + & 0 \end{array} \right\} \Rightarrow (192, 66) = 6.$$

Thus

$$[192, 66] = \frac{192 \times 66}{6} = 11 \times 192 = 2112.$$

Solutions to Sample Problems 3

---

1. Consider the ring $\mathbf{A} = \{0, a, b, c\}$ of 4 distinct elements, with multiplication table below:

$\bullet$	0	a	b	c
0	0	0	0	0
a	0	0	b	a
b	0	b	c	b
c	0	a	b	c

Answer the following:

(i) Is there a unity for $\mathbf{A}$? [If so, what element is it?]

YES: The element c.

(ii) If the answer to (i) is yes, compute the group of units $\mathbf{A}^*$.

$\mathbf{A}^* = \{c, b\}$.

(iii) Compute the zero divisors in $\mathbf{A}$.

Zero divisors $= \{0, a\}$.

(iv) Is $\mathbf{A}$ an integral domain? [State your reasons.]

NO, since $\mathbf{A}$ has a zero divisor $\neq 0$, namely a.

(v) Is $\mathbf{A}$ a field? [State your reasons.]

NO, since any field is necessarily an integral domain.

2. (i) Compute the group of units, and zero divisors in $\mathbf{Z}_{15}$.

$\mathbf{Z}_{15}^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$. Zero divisors $= \{\overline{0}, \overline{3}, \overline{5}, \overline{6}, \overline{9}, \overline{10}, \overline{12}\}$.

(ii) Find the multiplicative inverse of $\overline{23}$ in $\mathbf{Z}_{30}$.

First of all, we use Euclid and back substitution to express $1 = (23, 30)$ in terms of a linear combination of 23 and 30.

$$\left.\begin{array}{rcrcr} 30 & = & 1 \times 23 & + & 7 \\ 23 & = & 3 \times 7 & + & 2 \\ 7 & = & 3 \times 2 & + & 1 \end{array}\right\} \Rightarrow \begin{array}{rcl} 1 & = & 7 - 3 \times 2 \\ & = & 7 - 3 \times (23 - 3 \times 7) \\ & = & 10 \times 7 - 3 \times 23 \\ & = & 10 \times (30 - 23) - 3 \times 23 \\ & = & (-13) \times 23 + 10 \times 30 \end{array}$$

Thus $\overline{23}^{-1} = \overline{(-13)} = \overline{(-13+30)} = \overline{17}$.

(iii) By first showing that $3\mathbf{Z}_{15} \stackrel{\text{def}}{=} \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}\} \subset \mathbf{Z}_{15}$ is a subring of $\mathbf{Z}_{15}$, show that $3\mathbf{Z}_{15}$ is a field.

From the $+, \bullet$ tables below:

$+$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{12}$
$\overline{0}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{12}$
$\overline{3}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{12}$	$\overline{0}$
$\overline{6}$	$\overline{6}$	$\overline{9}$	$\overline{12}$	$\overline{0}$	$\overline{3}$
$\overline{9}$	$\overline{9}$	$\overline{12}$	$\overline{0}$	$\overline{3}$	$\overline{6}$
$\overline{12}$	$\overline{12}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$

$\bullet$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{12}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{3}$	$\overline{0}$	$\overline{9}$	$\overline{3}$	$\overline{12}$	$\overline{6}$
$\overline{6}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{12}$
$\overline{9}$	$\overline{0}$	$\overline{12}$	$\overline{9}$	$\overline{6}$	$\overline{3}$
$\overline{12}$	$\overline{0}$	$\overline{6}$	$\overline{12}$	$\overline{3}$	$\overline{9}$

It is clear that $3\mathbf{Z}_{15}$ is closed under $+, \bullet$ from $\mathbf{Z}_{15}$ (since all values in the tables are elements in $3\mathbf{Z}_{15}$). Therefore since the associative, commutative and distributive laws hold for $\mathbf{Z}_{15}$, the same laws also hold for $3\mathbf{Z}_{15}$. [Note that symmetry about diagonals also implies commutivity.] It is clear that $\overline{0}$ is the zero element, and that there are additive inverses [e.g. $-\overline{3} = \overline{12}$, $-\overline{6} = \overline{9}$, etc.]. Finally, from the $(\bullet)$ table, $\overline{6} \neq \overline{0}$ is the unity. Moreover multiplicative inverses for non-zero elements follows from the fact that $\overline{6}$ appears in every $(\bullet)$ column corresponding to a non-zero element. Thus $3\mathbf{Z}_{15}$ is a field.

3. Define a relation $\sim$ on the real numbers $\mathbf{R}$ as follows: $x \sim y \Leftrightarrow x = 2^q y$ for some integer $q \in \mathbf{Z}$. Verify that $\sim$ is an equivalence relation.

First, $x = 2^0 \cdot x \Rightarrow x \sim x$. Next, $x = 2^q y \Leftrightarrow y = 2^{-q} x$; moreover $q \in \mathbf{Z} \Leftrightarrow -q \in \mathbf{Z}$. Therefore $x \sim y \Leftrightarrow y \sim x$. Finally, suppose that $x \sim y$ and $y \sim z$. Then $x = 2^{q_1} y$ and $y = 2^{q_2} z$, for some $q_1, q_2 \in \mathbf{Z}$. Therefore $x = 2^{q_1+q_2} z$, hence $x \sim z$.

4. Find all values $\overline{x}$ in $\mathbf{Z}_8$ which satisfy the equation $\overline{x}^2 = \overline{1}$.

From the table of values:

$\overline{x}$	$\overline{x}^2$
$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{1}$
$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{1}$
$\overline{4}$	$\overline{0}$
$\overline{5}$	$\overline{1}$
$\overline{6}$	$\overline{4}$
$\overline{7}$	$\overline{1}$

It follows that $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ satisfies the equation $\overline{x}^2 = \overline{1}$.

5. Show that $\sqrt{30}$ is irrational.

Suppose to the contrary that $\sqrt{30} \in \mathbf{Q}$. Then we can write $\sqrt{30} = p/q$, where $p, q \in \mathbf{N}$, and where $\text{GCD}(p, q) = 1$. Thus $30 \cdot q^2 = p^2$, and $30 = 2 \cdot 3 \cdot 5$ is a product of distinct primes (multiplicity 1). By the Fundamental Theorem of Arithmetic, $2, 3, 5$ must be prime factors of p, hence $30|p$, i.e. $p = 30 \cdot p_1$ for some $p_1 \in \mathbf{N}$. Thus $30 \cdot q^2 = p^2 = 30^2 p_1^2$, hence $q^2 = 30 \cdot p_1$. By the same reasoning, $30|q$, hence $\text{GCD}(p, q) \geq 30$, which violates $\text{GCD}(p, q) = 1$. Thus $\sqrt{30} \notin \mathbf{Q}$.

Solutions to Sample Problems 4

Find all solutions of the given equations in the given field $\mathbf{Z}_p$.

1. $\overline{5}x + \overline{66} = \overline{0}$ in $\mathbf{Z}_{101}$.

Solution: There will be only one solution. Observe that $101 - 20 \cdot 5 = 1$, hence $\overline{5}^{-1} = -\overline{20}$. Thus $x = (-\overline{20}) \cdot (-\overline{66}) = \overline{1320} = \overline{1320 - 13 \cdot 101} = \overline{7}$. [Alternatively, $\overline{5}x = -\overline{66} = \overline{101 - 66} = \overline{35}$. Thus $x = \overline{7}$.]

2. $x^2 + \overline{3}x + \overline{2} = \overline{0}$ in $\mathbf{Z}_5$.

Solution: $\Delta = \overline{3}^2 - 4 \cdot \overline{2} = \overline{1}$, and $\overline{2}^{-1} = \overline{3}$, since $\overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$. Thus by the quadratic formula, $x = \overline{3}(-\overline{3} \pm \overline{1}) = \{-\overline{6}, -\overline{12}\} = \{\overline{4}, \overline{3}\}$.

3. $x^2 + \overline{10}x + \overline{24} = \overline{0}$ in $\mathbf{Z}_{101}$.

Solution: $\Delta = \overline{100} - 4 \cdot \overline{24} = \overline{4}$, and $\overline{2}^{-1} = \overline{51}$, since $\overline{2} \cdot \overline{51} = \overline{102} = \overline{1}$. Thus by the quadratic formula, $x = \overline{51}(-\overline{10} \pm \overline{2}) = \{-\overline{408}, -\overline{612}\} = \{\overline{97}, \overline{95}\}$.

4. $x^2 = \overline{2}$ in $\mathbf{Z}_7$.

Solution: $\Delta = \overline{1}$. Further $\overline{2}^{-1} = \overline{4}$, since $\overline{2} \cdot \overline{4} = \overline{8} = \overline{1}$. Thus by the quadratic formula, $x = \{\overline{4}, -\overline{4}\} = \{\overline{4}, \overline{3}\}$.

5. $x^2 = \overline{18}$ in $\mathbf{Z}_{31}$.

Solution: $\Delta = 4 \cdot \overline{18} = \overline{72} = \overline{10}$. In this case, solving $x^2 = \overline{10}$, viz. $\sqrt{\overline{10}}$ seems no easier than solving the original equation $x^2 = \overline{18}$. Note that $\overline{7}^2 = \overline{49} = \overline{18}$, hence the two roots (which are guaranteed by the quadratic formula) are $\{\overline{7}, -\overline{7}\} = \{\overline{7}, \overline{22}\}$.

Perform the indicated operation.

6. $(\overline{4}x + \overline{3})(\overline{5}x + \overline{6})$ in $\mathbf{Z}_7[x]$.

Solution: $(\overline{4}x+\overline{3})(\overline{5}x+\overline{6}) = \overline{20}x^2+\overline{39}x+\overline{18} = \overline{6}x^2+\overline{4}x+\overline{4}$.

7. $(\overline{2}x^3+\overline{3}x^2-\overline{5}x+\overline{1})/(x+\overline{4})$ in $\mathbf{Z}_7[x]$ (long division).

$$
\begin{array}{rl}
 & \overline{2}x^2 + \overline{2}x + \overline{4} \\
 & -- - -- - -- - -- - -- \\
x+\overline{4} \;\big)\; & \overline{2}x^3 + \overline{3}x^2 - \overline{5}x + \overline{1} \\
 & 2\overline{x}^3 + x^2 \\
 & -- - -- - -- - -- - -- \\
 & \quad \overline{2}x^2 - \overline{5}x + \overline{1} \\
 & \quad \overline{2}x^2 + x \\
 & \quad\quad -- - -- - -- \\
 & \quad\quad \overline{4}x + \overline{1} \\
 & \quad\quad \overline{4}x + \overline{2} \\
 & \quad\quad\quad -- - -- \\
 & \quad\quad\quad \overline{6}
\end{array}
$$

Thus

$$(\overline{2}x^3+\overline{3}x^2-\overline{5}x+\overline{1}) = (x+\overline{4})(\overline{2}x^2+\overline{2}x+\overline{4}) \;+\; \overline{6}.$$

8. $(\overline{4}x^2+\overline{7}x+\overline{3})+(\overline{8}x^2+\overline{5}x+\overline{11})$ in $\mathbf{Z}_{12}[x]$.

Solution: $(\overline{4}x^2+\overline{7}x+\overline{3})+(\overline{8}x^2+\overline{5}x+\overline{11}) = \overline{12}x^2+\overline{12}x+\overline{14} = \overline{2}$.

Factor completely into a product of irreducibles.

9. $x^2+\overline{6}x+\overline{1}$ in $\mathbf{Z}_7[x]$.

Solution: The trick is to find a root of this polynomial in $\mathbf{Z}_7$, either by the quadratic formula, or by a good guess. Note that $\Delta = \overline{36}-\overline{4} = \overline{32} = \overline{4}$, and that $\overline{2}^{-1} = \overline{4}$. By the quadratic formula, the roots are $\overline{4}\cdot(-\overline{6}\pm\overline{2}) = \{-\overline{16}, -\overline{32}\} = \{\overline{5},\overline{3}\}$. Thus

$$x^2+\overline{6}x+\overline{1} = (x-\overline{5})(x-\overline{3})$$

gives the factorization into irreducibles.

10. $x^4+\overline{9}x^2+\overline{7}$ in $\mathbf{Z}_{11}[x]$.

Solution: First, replace x^2 by y, and solve the quadratic equation $y^2+\overline{9}y+\overline{7} = \overline{0}$. In this case $\Delta = \overline{81}-\overline{28} = \overline{53} = \overline{9}$, and $\overline{2}^{-1} = \overline{6}$, since $\overline{2}\cdot\overline{6} = \overline{12} = \overline{1}$. Thus by the quadratic

formula, $y = \overline{6}\cdot(-\overline{9}\pm\overline{3}) = \{-\overline{36}, -\overline{72}\} = \{\overline{8}, \overline{5}\}$. Thus so far $x^4+\overline{9}x^2+\overline{7} = (x^2-\overline{8})(x^2-\overline{5})$. Note the following table of values:

x	x^2
$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{1}$
$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{9}$
$\overline{4}$	$\overline{5}$
$\overline{5}$	$\overline{9}$
$\overline{6}$	$\overline{3}$
$\overline{7}$	$\overline{5}$
$\overline{8}$	$\overline{9}$
$\overline{9}$	$\overline{4}$
$\overline{10}$	$\overline{1}$

From the table, it is obvious that $x^2 - \overline{8}$ has no root in $\mathbf{Z}_{11}$, hence being of degree 2, it must be irreducible. On the other hand, the table implies that $x^2 - \overline{5}$ has roots $\{\overline{4}, \overline{7}\}$, hence factors into $(x - \overline{4})(x - \overline{7})$. Thus:

$$x^4 + \overline{9}x^2 + \overline{7} = (x^2 - \overline{8})(x - \overline{4})(x - \overline{7})$$

is the factorization into irreducibles.

---

11. Explain why $x^3 + \overline{3}x + \overline{2}$ is irreducible in $\mathbf{Z}_5[x]$.

Solution: Since we are dealing with a degree three polynomial, it suffices to show that $f(x) := x^3 + \overline{3}x + \overline{2}$ has no root in $\mathbf{Z}_5$. This is clear from the table of values:

x	$f(x)$
$\overline{0}$	$\overline{2}$
$\overline{1}$	$\overline{1}$
$\overline{2}$	$\overline{1}$
$\overline{3}$	$\overline{3}$
$\overline{4}$	$\overline{3}$

Solutions to Sample Problems 5

[1.] (i) Show that $2x^3 + 3x^2 + x - 1$ has no rational roots.

Solution: Set $f(x) := 2x^3+3x^2+x-1$. The only candidates for $\mathbf{Q}$-roots are $\{\pm 1, \pm\frac{1}{2}\}$. We evaluate: $f(1) = 5$, $f(-1) = -1$, $f(1/2) = 1/2$, $f(-1/2) = -1$. Thus f has no $\mathbf{Q}$-roots.

(ii) Show that $x^3 - 3x - 1$ has no rational roots.

Solution: The only candidates for $\mathbf{Q}$-roots are ± 1, and neither of these are roots of $x^3 - 3x - 1$.

(iii) Determine the rational root(s) of $p(x) = x^4 + 3x^3 - 3x^2 - 10x - 3$ and factor $p(x)$ as a product of irreducibles in $\mathbf{Q}[x]$. [Hint: Use (ii).]

Solution: The only candidates for $\mathbf{Q}$-roots are $\pm 1, \pm 3$. It is easy to check that $p(-3) = 0$, and hence $x + 3 = (x - (-3))$ is a factor of $p(x)$. Since none of the other candidates turn out to be roots, we long divide:

$$
\begin{array}{rcl}
 & x^3 - 3x - 1 & \\
 & -- \quad -- \quad -- \quad -- & \\
x+3 \;\big)\; & x^4 + 3x^3 - 3x^2 - 10x - 3 & \\
 & x^4 + 3x^3 & \\
 & -- \quad -- \quad -- \quad -- & \\
 & -3x^2 - 10x - 3 & \\
 & -3x^2 - 9x & \\
 & -- \quad -- \quad -- & \\
 & -x - 3 & \\
 & -x - 3 & \\
 & -- \quad -- & \\
 & 0 &
\end{array}
$$

Thus $p(x) = (x + 3)(x^3 - 3x - 1)$ gives the decomposition into irreducibles, using the fact that the degree 3 polynomial $x^3 - 3x - 1$ has no $\mathbf{Q}$-roots by (ii) above, hence is irreducible.

[2.] Let $\mathbf{F}$ be a field, and $f(x) \in \mathbf{F}[x]$ a polynomial of degree 1. Prove that $f(x)$ is irreducible.

Solution: Suppose that $f = h \cdot g$. then $1 = \deg f = \deg h + \deg g$. Thus either $(\deg h, \deg g) = (1, 0)$ (hence $g \in \mathbf{F}^*$), or $(\deg h, \deg g) = (0, 1)$ (hence $h \in \mathbf{F}^*$). Thus f is irreducible.

[3.] (i) Let $T : \mathbf{Q}[x] \to \mathbf{Q}$ be the map given by $p(x) \in \mathbf{Q}[x] \mapsto T(p(x)) := p(0) \in \mathbf{Q}$. Show that T is a ring homomorphism. Describe the kernel, $\ker T$. Also, what is the image of T?

Solution: If $p(x) = p \in \mathbf{Q}$, then $p(0) = p$, hence $T(1) = 1$, and $\mathrm{Im}(T) = \mathbf{Q}$. Next, $T(f+g) := (f+g)(0) = f(0)+g(0) = T(f)+T(g)$, and $T(f \cdot g) := (f \cdot g)(0) = f(0) \cdot g(0) = T(f) \cdot T(g)$. Thus T is a ring homomorphism. Finally, $T(f) = 0 \Leftrightarrow f(0) = 0 \Leftrightarrow x = (x-0)$ is a factor of f. Thus $\ker T = (x) \subset \mathbf{Q}[x]$.

(ii) Explain why the map $g : \mathbf{R} \to \mathbf{R}$ given by $g(t) = t^2$, is not a ring homomorphism.

Solution: For example $g(1+1) = g(2) = 4 \neq 2 = g(1) + g(1)$. Thus g is not a ring homomorphism.

[4.] Let A be a ring, and fix $a \in A$. Show that $(a) := \{ba \mid b \in A\}$ is an ideal in A.

Solution: First of all, if $b_1a, b_2a \in (a)$, and $c \in \mathbf{A}$, then $b_1a+b_2a = (b_1+b_2)a \in (a)$ and $c(b_1a) = (cb_1)a \in (a)$. Thus (a) is closed under multiplication by elements in $\mathbf{A}$, and closed under addition from $\mathbf{A}$. In particular, the associative, commutative, and distributive laws, which hold for $\mathbf{A}$, must likewise hold for (a). Also $ba \in (a) \Rightarrow -(ba) = (-b)a \in (a)$, and $0 = 0 \cdot a \in (a)$. Hence (a) has a zero element, and additive inverses. In particular, (a) is a subring of $\mathbf{A}$ for which $\mathbf{A} \cdot (a) \subset (a)$. This makes (a) an ideal in $\mathbf{A}$.

[5.] Give an example of a ring A, and a non-zero element $a \in A$ for which $(a) = 0$. [Hint: Choose A to be a suitable subring of $\mathbf{Z}_4$.]

Solution: Put $\mathbf{A} = 2\mathbf{Z}_4 = \{\overline{0}, \overline{2}\} \subset \mathbf{Z}_4$, and let $a = \overline{2}$. Then $(\overline{2}) = (\overline{0})$ in $\mathbf{A}$.

[6.] Let $f : \mathbf{Z}_{12} \to \mathbf{Z}_4$ be given by the prescription $f(\overline{x}_{12}) = \overline{x}_4$.

(i) Show that f is a well defined ring homomorphism.

Solution: Suppose that $\overline{y}_{12} = \overline{x}_{12}$. We must show that $f(\overline{y}_{12}) = f(\overline{x}_{12})$, i.e. $\overline{y}_4 = \overline{x}_4$. But $\overline{y}_{12} = \overline{x}_{12} \Leftrightarrow 12|(y-x) \Rightarrow 4|(y-x) \Rightarrow \overline{y}_4 = \overline{x}_4$. Thus f is well-defined.

(ii) Compute the kernel, $\ker f$.

Solution: $\ker f = \{\overline{x}_{12} \mid \overline{x}_4 = \overline{0}\} = \{\overline{x}_{12} \mid 4|x\} = 4 \cdot \mathbf{Z}_{12} = \{\overline{0}, \overline{4}, \overline{8}\} \subset \mathbf{Z}_{12}$.

[7.] Give an example of the following: An integral domain A and an ideal $\mathcal{U} \subset A$ such that the quotient ring $A/\mathcal{U}$ is not an integral domain.

Solution: Choose any $n \in \mathbf{N}$ with n not prime, say $n = 4$. Set $\mathcal{U} = (n)$ and $\mathbf{A} = \mathbf{Z}$. then $\mathbf{A}$ is an integral domain, and yet $\mathbf{A}/\mathcal{U} = \mathbf{Z}_n = \mathbf{Z}_4$ is not an integral domain.

SAMPLE FINAL EXAM #1

Time: 2 hours Instructor: James D. Lewis

$\mathbf{Z} =$ integers, $\mathbf{Q} =$ rationals, $\mathbf{R} =$ reals, $\mathbf{C} =$ complex numbers

---

[1.] Factor

$$f(x) = x^4 + \overline{2}x^3 + \overline{2}x^2 + \overline{2}x + \overline{1} \in \mathbf{Z}_3[x]$$

into a product of irreducibles.

[2.] Find all irreducible polynomials of degree 3 in $\mathbf{Z}_2[x]$.

[3.] Consider the map $T : \mathbf{Q}[x] \to \mathbf{R}$ given by $T(f(x)) = f(\sqrt{2}) \in \mathbf{R}$.

(i) Verify that T is a ring homomorphism.

(ii) Find $\ker(T)$, i.e. find a $d(x) \in \mathbf{Q}[x]$ such that $\ker(T) = (d(x)) \stackrel{\text{def}}{=} \{h(x) \cdot d(x) \mid h(x) \in \mathbf{Q}[x]\}$.

(iii) Find $\text{Im}(T)$.

[4.] (i) Find all units in $\mathbf{Z}_{18}$.

(ii) Compute $\overline{31}^{-1}$ in $\mathbf{Z}_{60}$.

[5.] Let

$$f(x) = 2x^5 + 5x^4 + 4x^3 + 7x^2 + 7x + 2 \in \mathbf{Q}[x].$$

Factor $f(x)$ into a product of irreducibles.

[6] Let $\mathbf{A} = \{a + b\sqrt{5} \mid a,\ b \in \mathbf{Z}\}$. Verify that $\mathbf{A}$ is a subring of $\mathbf{R}$. Is $\mathbf{A}$ a field? [You must explain your reasoning.]

[7.] Let $f(x) = x^3 + 2x^2 + x + 3 \in \mathbf{Q}[x]$. Explain why no combination of the form $a + b\sqrt{2} + c\sqrt{3},\ a,\ b,\ c \in \mathbf{Q}$, can be a root of $f(x)$.

[8.] Consider the quotient ring

$$\mathbf{A} = \frac{\mathbf{Z}_2[x]}{(x^2 + \overline{1})},$$

and where we write $\overline{x}$ for the image of x in $\mathbf{A}$ via the homomorphism $\mathbf{Z}_2[x] \to \mathbf{A}$. Compute all units and all zero divisors of $\mathbf{A}$.

SAMPLE FINAL EXAM #2

Time: 2 hours Instructor: James D. Lewis

$\mathbf{Z} =$ integers, $\mathbf{Q} =$ rationals, $\mathbf{R} =$ reals, $\mathbf{C} =$ complex numbers

---

[1.] (i) Explain why $x^2 + x + \overline{1}$ is the *only* irreducible polynomial of degree 2 in $\mathbf{Z}_2[x]$. [Hint: First list all the polynomials of degree 2 in $\mathbf{Z}_2[x]$.]

(ii) Factor $p(x) = x^6 + x^4 + x + \overline{1} \in \mathbf{Z}_2[x]$ into a product of irreducibles. [Hint: First divide $p(x)$ by the polynomial in (i).]

[2.] Let $p(x) = 2x^3 + 21x^2 - 5 \in \mathbf{Q}[x]$. Factor $p(x)$ as a product of irreducibles in $\mathbf{Q}[x]$.

[3.] Let $i = \sqrt{-1} \in \mathbf{C}$, and consider the map $T : \mathbf{R}[x] \to \mathbf{C}$ given by $T(p(x)) = p(i) \in \mathbf{C}$.

(i) Verify that T is a ring homomorphism.

(ii) Find $\ker(T)$, i.e. find a $d(x) \in \mathbf{R}[x]$ such that $\ker(T) = (d(x)) \stackrel{\text{def}}{=} \{h(x) \cdot d(x) \mid h(x) \in \mathbf{R}[x]\}$.

(iii) Find $\text{Im}(T)$.

[4.] Let $T : A \to B$ be a ring homomorphism, and let $\mathcal{U} \subset B$ be an ideal. [Here A and B are rings with unity.] Show that $T^{-1}(\mathcal{U})$ is an ideal in B. [Recall $T^{-1}(\mathcal{U}) = \{a \in A \mid T(a) \in \mathcal{U}\}$.]

[5.] Let $A = \{a + b\sqrt{2} \mid a,\ b \in \mathbf{Z}\}$.

(i) Explain why A is a subring of $\mathbf{R}$.

(ii) Find the units A^* in A.

(iii) Is A a field? An integral domain? [Please explain.]

(iv) Find the units $(A[x])^*$ in $A[x]$.

[6.] Consider the polynomial $p(x) = x^3 - 3x^2 + 2x - 1 \in \mathbf{Q}[x]$.

(i) Explain why $p(x)$ is irreducible in $\mathbf{Q}[x]$.

(ii) Is $\mathbf{Q}[x]/(p(x))$ a field?

(iii) For any $g \in \mathbf{Q}[x]$, let $\overline{g} \in \mathbf{Q}[x]/(p(x))$ be the corresponding class. Find the multiplicative inverse of $\overline{x}$ in $\mathbf{Q}[x]/(p(x))$.

[7.] (i) Find all units $\mathbf{Z}_{25}^*$ in $\mathbf{Z}_{25}$.

(ii) Find all zero divisors in $\mathbf{Z}_{14}$.

(iii) Find $\overline{29}^{-1}$ in $\mathbf{Z}_{147}$.

[8.] (i) Compute GCD$(66, 220)$.

(ii) Let $\mathcal{U} = \{n66 + m220 \mid n,\ m \in \mathbf{Z}\}$. Show that $\mathcal{U}$ is an ideal in $\mathbf{Z}$.

(iii) Let $\mathcal{U}$ be given in (ii). Find a positive integer d such that $\mathcal{U} = (d)$.

SOLUTIONS TO SAMPLE FINAL EXAM #1

[1.] Factor

$$f(x) = x^4 + \overline{2}x^3 + \overline{2}x^2 + \overline{2}x + \overline{1} \in \mathbf{Z}_3[x]$$

into a product of irreducibles.

Solution: Note that $f(\overline{0}) = \overline{1}$, $f(\overline{1}) = \overline{2}$, $f(\overline{2}) = \overline{0}$, and therefore $(x - \overline{2})$ is a factor of $f(x)$. Long division gives us

$$f(x) = (x - \overline{2}) \underbrace{(x^3 + x^2 + x + \overline{1})}_{q(x)}.$$

But $q(\overline{2}) = \overline{0}$, and hence $(x - \overline{2})$ is a factor of $q(x)$. [Alternatively, $f'(x) = x^3 + x + \overline{2} \Rightarrow f'(\overline{2}) = \overline{0}$, $f''(\overline{2}) = \overline{2} \neq \overline{0}$, hence $(x - \overline{2})$ is a double root.] Again, by long division, $q(x) = (x + \overline{2})(x^2 + \overline{1})$. Note that $x^2 + \overline{1}$ has no root in $\mathbf{Z}_3$, hence $x^2 + \overline{1}$ is irreducible in $\mathbf{Z}_3[x]$. Thus

$$f(x) = (x + \overline{2})^2(x^2 + \overline{1})$$

gives the irreducible decomposition.

[2.] Find all irreducible polynomials of degree 3 in $\mathbf{Z}_2[x]$.

Solution: The degree 3 polynomials in $\mathbf{Z}_2[x]$ are $x^3 + x^2 + x + \overline{1}$, $x^3 + x + \overline{1}$, $x^3 + x^2 + x$, $x^3 + x^2 + \overline{1}$, $x^3 + \overline{1}$, $x^3 + x^2$, $x^3 + x$, and x^3. Among this list, only $x^3 + x + \overline{1}$ and $x^3 + x^2 + \overline{1}$ don't have a root in $\mathbf{Z}_2$. Thus $x^3 + x + \overline{1}$ and $x^3 + x^2 + \overline{1}$ are the only degree three irreducible polynomials in $\mathbf{Z}_2[x]$.

[3.] Consider the map $T : \mathbf{Q}[x] \to \mathbf{R}$ given by $T(f(x)) = f(\sqrt{2}) \in \mathbf{R}$.

(i) Verify that T is a ring homomorphism.

Solution: Clearly $T(r) = r$ for any $r \in \mathbf{Q}$. Thus $T(1) = 1$, i.e. preserves unities. Next, $T(f + g) = (f + g)(\sqrt{2}) = f(\sqrt{2}) + g(\sqrt{2}) = T(f) + T(g)$. Finally, $T(f \cdot g) = (f \cdot g)(\sqrt{2}) = f(\sqrt{2})g(\sqrt{2}) = T(f)T(g)$.

(ii) Find $\ker(T)$, i.e. find a $d(x) \in \mathbf{Q}[x]$ such that $\ker(T) = (d(x)) \stackrel{\text{def}}{=} \{h(x) \cdot d(x) \mid h(x) \in \mathbf{Q}[x]\}$.

Solution: Note that $\sqrt{2} \notin \mathbf{Q} \Rightarrow \deg d(x) \geq 2$. If we put $d(x) = x^2 - 2$, then it is obvious that $d(\sqrt{2}) = 0$, hence $d(x) \in \ker T$, and that for any $h(x) \in \ker T$, $h(x) = q(x)d(x) + r(x)$, where $\deg r(x) \leq 1$. But $r(\sqrt{2}) = h(\sqrt{2}) - q(\sqrt{2})d(\sqrt{2}) = 0$, hence $r(x) = 0$. Thus $\ker T = (d(x))$, where $d(x) = x^2 - 2$.

(iii) Find $\mathrm{Im}(T)$.

Solution: $\mathrm{Im}(T) = \mathbf{Q}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$.

[4.] (i) Find all units in $\mathbf{Z}_{18}$.

Solution: $\mathbf{Z}_{18}^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}\}$.

(ii) Compute $\overline{31}^{-1}$ in $\mathbf{Z}_{60}$.

Solution: By applying Euclidean division and back substitution, we arrive at $1 = 15 \times 60 - 29 \times 31$. Thus $\overline{31}^{-1} = \overline{-29} = \overline{60 - 29} = \overline{31}$.

[5.] Let

$$f(x) = 2x^5 + 5x^4 + 4x^3 + 7x^2 + 7x + 2 \in \mathbf{Q}[x].$$

Factor $f(x)$ into a product of irreducibles.

Solution: We first look for $\mathbf{Q}$-roots of $f(x)$, the candidates being $\{\pm 1, \pm 2, \pm\frac{1}{2}\}$. It is obvious that $f(+\text{ve}) > 0$, so we evaluate f on the negative candidates. In this case $f(-2) = f(-\frac{1}{2}) = 0$. Long division gives us

$$f(x) = (x+2)(2x^4 + x^3 + 2x^2 + 3x + 1) = (x+2)(x + \frac{1}{2})(2x^2 + 2x + 2).$$

$$= (x+1)(2x+1)(x^2 + x + 1).$$

Note that $\{\pm 1, \pm 2, \pm\frac{1}{2}\}$ are not roots of x^2+x+1, and therefore x^2+x+1 has no $\mathbf{Q}$-roots. Thus $x^2 + x + 1$ is irreducible in $\mathbf{Q}[x]$, and hence $f(x) = (x+1)(2x+1)(x^2+x+1)$ gives the irreducible decomposition.

[6] Let $\mathbf{A} = \{a + b\sqrt{5} \mid a,\ b \in \mathbf{Z}\}$. Verify that $\mathbf{A}$ is a subring of $\mathbf{R}$. Is $\mathbf{A}$ a field? [You must explain your reasoning.]

Solution: Set $z = p + q\sqrt{5}$, $w = a + b\sqrt{5} \in \mathbf{A}$, i.e. where $p, q, a, b \in \mathbf{Z}$. Then:

$$z + w = \underbrace{(p+a)}_{\in \mathbf{Z}} + \underbrace{(q+b)}_{\in \mathbf{Z}}\sqrt{5} \in \mathbf{A}.$$

$$z \cdot w = \underbrace{(p \cdot a + 5q \cdot b)}_{\in \mathbf{Z}} + \underbrace{(p \cdot b + q \cdot a)}_{\in \mathbf{Z}}\sqrt{5} \in \mathbf{A}.$$

Thus $\mathbf{A}$ is closed under $+, \bullet$ from $\mathbf{R}$, and hence the associative, commutative and distributive laws hold for $\mathbf{A}$, since the same laws hold for $\mathbf{R}$. Note that $\mathbf{Z} = \{p + 0\cdot\sqrt{5} \mid p \in \mathbf{Z}\} \subset \mathbf{A}$. Thus $0, 1 \in \mathbf{A}$ and $1 \neq 0$. Also we have additive inverses: $-z = (-p) + (-q)\sqrt{5} \in \mathbf{A}$. Thus $\mathbf{A}$ is a subring of $\mathbf{R}$. It is not a subfield though. For example, if we let $z = p + q\sqrt{5} \in \mathbf{A}$, and consider the conjugate $\overline{z} = p - q\sqrt{5}$, and put $N(z) = z \cdot \overline{z} = p^2 - 5q^2 \in \mathbf{Z}$, then $zw = 1 \Rightarrow N(zw) = N(z)N(w) = N(1) = 1$. Thus $N(z) = N(w) = \pm 1$. In other words,

if $z \in \mathbf{A}^*$, then $N(z) = \pm 1$. So for example $2 \notin \mathbf{A}^*$, since $N(2) = 4 \neq \pm 1$. Thus $\mathbf{A}$ is a subring, but not a subfield of $\mathbf{R}$.

[7.] Let $f(x) = x^3 + 2x^2 + x + 3 \in \mathbf{Q}[x]$. Explain why no combination of the form $a + b\sqrt{2} + c\sqrt{3},\ a,\ b,\ c \in \mathbf{Q}$, can be a root of $f(x)$.

Solution: If $z := a + b\sqrt{2} + c\sqrt{3}$ is a root of $f(x)$ for some $a, b, c \in \mathbf{Q}$, then such a z belongs to the subfield $\mathbf{L} \subset \mathbf{R}$ introduced in the rule and compass constructions. Therefore $f(x)$ would have to have a $\mathbf{Q}$-root. But the only candidates of $\mathbf{Q}$-roots of $f(x)$ are $\pm 1, \pm 3$, and neither of these turn out to be roots of $f(x)$. Thus such a root z above cannot exist.

[8.] Consider the quotient ring

$$\mathbf{A} = \frac{\mathbf{Z}_2[x]}{\left(x^2 + \overline{1}\right)},$$

and where we write $\overline{x}$ for the image of x in $\mathbf{A}$ via the homomorphism $\mathbf{Z}_2[x] \to \mathbf{A}$. Compute all units and all zero divisors of $\mathbf{A}$.

Solution: All the elements of $\mathbf{A} = \mathbf{Z}[\overline{x}]$ are given by $\{\overline{0}, \overline{1}, \overline{x}, \overline{x} + \overline{1}\}$. Note that $\overline{x}^2 = -\overline{1} = \overline{1}$. The multiplication table is given below:

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x}+\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x}+\overline{1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{1}$	$\overline{x}+\overline{1}$
$\overline{x}+\overline{1}$	$\overline{0}$	$\overline{x}+\overline{1}$	$\overline{x}+\overline{1}$	$\overline{0}$

Thus it is clear that the units $\mathbf{A}^* = \{\overline{1}, \overline{x}\}$ and the zero divisors are $\{\overline{0}, \overline{x} + \overline{1}\}$.

SOLUTIONS TO SAMPLE FINAL EXAM #2

[1.] (i) Explain why $x^2 + x + \overline{1}$ is the *only* irreducible polynomial of degree 2 in $\mathbf{Z}_2[x]$. [Hint: First list all the polynomials of degree 2 in $\mathbf{Z}_2[x]$.]

Solution: All polynomials in $\mathbf{Z}_2[x]$ of degree 2 are: $x^2 + x + \overline{1}, x^2 + x, x^2 + \overline{1}, x^2$, and all except $x^2 + x + \overline{1}$ have a root in $\mathbf{Z}_2$. Thus $x^2 + x + \overline{1}$ is the only irreducible degree 2 polynomial in $\mathbf{Z}_2[x]$.

(ii) Factor $p(x) = x^6 + x^4 + x + \overline{1} \in \mathbf{Z}_2[x]$ into a product of irreducibles. [Hint: First divide $p(x)$ by the polynomial in (i).]

Solution: By long division, $p(x) = (x^4 + x^3 + x^2 + \overline{1})(x^2 + x + \overline{1})$. But $x^4 + x^3 + x^2 + \overline{1}$ has $\overline{1}$ as root, hence $x + \overline{1}$ is a factor. Again, by long division:

$$p(x) = (x^2 + x + \overline{1})(x + \overline{1})(x^3 + x + \overline{1}).$$

This is a decomposition into irreducibles, since $x^3 + x + \overline{1}$ has no root in $\mathbf{Z}_2$.

[2.] Let $p(x) = 2x^3 + 21x^2 - 5 \in \mathbf{Q}[x]$. Factor $p(x)$ as a product of irreducibles in $\mathbf{Q}[x]$.

Solution: The candidates for $\mathbf{Q}$-roots of $p(x)$ are $\{\pm 1, \pm 5, \pm\frac{1}{2}, \pm\frac{5}{2}\}$. Among these candidates, one sees that $p(-\frac{1}{2}) = 0$, and thus $x + \frac{1}{2}$ is a factor of $p(x)$. By long division:

$$p(x) = (x + \frac{1}{2})(2x^2 + 20x - 10) = (2x + 1)(x^2 + 10x - 5).$$

But the only candidates for $\mathbf{Q}$-roots of $x^2 + 10x - 5$ are $\pm 1, \pm 5$ and neither of these are roots. Thus $x^2 + 10x - 5$ is irreducible, and hence the above is an irreducible decomposition.

[3.] Let $i = \sqrt{-1} \in \mathbf{C}$, and consider the map $T : \mathbf{R}[x] \to \mathbf{C}$ given by $T(p(x)) = p(i) \in \mathbf{C}$.

(i) Verify that T is a ring homomorphism.

Solution: Clearly $T(r) = r$ for any $r \in \mathbf{R}$. Thus $T(1) = 1$, i.e. preserves unities. Next, $T(f + g) = (f + g)(\sqrt{-1}) = f(\sqrt{-1}) + g(\sqrt{-1}) = T(f) + T(g)$. Finally, $T(f \cdot g) = (f \cdot g)(\sqrt{-1}) = f(\sqrt{-1})g(\sqrt{-1}) = T(f)T(g)$.

(ii) Find $\ker(T)$, i.e. find a $d(x) \in \mathbf{R}[x]$ such that $\ker(T) = (d(x)) \stackrel{\text{def}}{=} \{h(x) \cdot d(x) \mid h(x) \in \mathbf{R}[x]\}$.

Solution: $d(x) = x^2 + 1$.

(iii) Find $\mathrm{Im}(T)$.

Solution: $\mathrm{Im}(T) = \mathbf{C}$.

[4.] Let $T : A \to B$ be a ring homomorphism, and let $\mathcal{U} \subset B$ be an ideal. [Here A and B are rings with unity.] Show that $T^{-1}(\mathcal{U})$ is an ideal in B. [Recall $T^{-1}(\mathcal{U}) = \{a \in A \mid T(a) \in \mathcal{U}\}$.]

Solution: Let $a, b \in T^{-1}(\mathcal{U})$, and $c \in A$ be given. Then $T(a+b) = T(a) + T(b) \in \mathcal{U}$, and $T(ca) = T(c)T(a) \in \mathcal{U}$. Thus $T^{-1}(\mathcal{U})$ is an ideal in A.

[5.] Let $A = \{a + b\sqrt{2} \mid a,\ b \in \mathbf{Z}\}$.

(i) Explain why A is a subring of $\mathbf{R}$.

Solution: Set $z = p + q\sqrt{2}$, $w = a + b\sqrt{2} \in \mathbf{A}$, i.e. where $p, q, a, b \in \mathbf{Z}$. Then:

$$z + w = \underbrace{(p+a)}_{\in \mathbf{Z}} + \underbrace{(q+b)}_{\in \mathbf{Z}}\sqrt{2} \in \mathbf{A}.$$

$$z \cdot w = \underbrace{(p \cdot a + 2q \cdot b)}_{\in \mathbf{Z}} + \underbrace{(p \cdot b + q \cdot a)}_{\in \mathbf{Z}}\sqrt{2} \in \mathbf{A}.$$

Thus $\mathbf{A}$ is closed under $+, \bullet$ from $\mathbf{R}$, and hence the associative, commutative and distributive laws hold for $\mathbf{A}$, since the same laws hold for $\mathbf{R}$. Note that $\mathbf{Z} = \{p + 0 \cdot \sqrt{2} \mid p \in \mathbf{Z}\} \subset \mathbf{A}$. Thus $0, 1 \in \mathbf{A}$ and $1 \neq 0$. Also we have additive inverses: $-z = (-p) + (-q)\sqrt{2} \in \mathbf{A}$. Thus $\mathbf{A} \subset \mathbf{R}$ is a subring (with unity $1 \neq 0$).

(ii) Find the units A^* in A.

Solution: For $z = p + q\sqrt{2}$, define $\overline{z} = p - q\sqrt{2}$, and the norm $N(z) = z \cdot \overline{z} = p^2 - 2q^2 \in \mathbf{Z}$. Then for $z, w \in \mathbf{A}$, $zw = 1 \Rightarrow N(z)N(w) = N(zw) = N(1) = 1$, hence $N(z) = N(w) = \pm 1$. Thus $z \in \mathbf{A}^* \Rightarrow N(z) = \pm 1$. Conversely, if $N(z) = \pm 1$, then $z^{-1} = \pm\overline{z} \in \mathbf{A}$. Thus

$$\mathbf{A}^* = \{z \in \mathbf{A} \mid N(z) = \pm 1\} = \{p + q\sqrt{2} \mid p^2 - 2q^2 = \pm 1,\ p, q \in \mathbf{Z}\}.$$

(iii) Is A a field? An integral domain? [Please explain.]

Solution: By the decription of $\mathbf{A}^*$ in (ii) above, $\sqrt{2} \notin \mathbf{A}^*$, and therefore $\mathbf{A}$ is not a field. However, by (i), $\mathbf{A}$ is a subring of $\mathbf{R}$, with unity $1 \neq 0$. Thus $\mathbf{A}$ cannot have any non-zero zero divisors (being a subring of $\mathbf{R}$). Thus $\mathbf{A}$ is an integral domain.

(iv) Find the units $(A[x])^*$ in $A[x]$.

Solution: $(\mathbf{A}[x])^* = \mathbf{A}^*$, since $\mathbf{A}$ is an integral domain.

[6.] Consider the polynomial $p(x) = x^3 - 3x^2 + 2x - 1 \in \mathbf{Q}[x]$.

(i) Explain why $p(x)$ is irreducible in $\mathbf{Q}[x]$.

Solution: The only candidates for $\mathbf{Q}$-roots of $p(x)$ are ± 1, and neither are roots. Hence $p(x)$, being of degree 3, must be irreducible.

(ii) Is $\mathbf{Q}[x]/(p(x))$ a field?

Solution: YES, since from class notes, $p(x)$ being irreducible implies that $(p(x))$ is a maximal ideal, hence $\mathbf{Q}[x]/(p(x))$ a field.

(iii) For any $g \in \mathbf{Q}[x]$, let $\overline{g} \in \mathbf{Q}[x]/(p(x))$ be the corresponding class. Find the multiplicative inverse of $\overline{x}$ in $\mathbf{Q}[x]/(p(x))$.

Solution: In $\mathbf{Q}[x]/(p(x))$, $\overline{p(x)} = \overline{x}^3 - 3\overline{x}^2 + 2\overline{x} - 1 = 0$. Equivalently, $\overline{x}^3 - 3\overline{x}^2 + 2\overline{x} = 1$. Factoring out an $\overline{x}$-term gives us: $\overline{x}(\overline{x}^2 - 3\overline{x} + 2) = 1$. Thus $\overline{x}^{-1} = \overline{x^2 - 2x + 2}$.

[7.] (i) Find all units $\mathbf{Z}_{25}^*$ in $\mathbf{Z}_{25}$.

Solution: $\mathbf{Z}_{25}^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{11}, \overline{12}, \overline{13}, \overline{14}, \overline{16}, \overline{17}, \overline{18}, \overline{19}, \overline{21}, \overline{22}, \overline{23}, \overline{24}\}$.

(ii) Find all zero divisors in $\mathbf{Z}_{14}$.

Solution: $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{7}, \overline{8}, \overline{10}, \overline{12}\}$.

(iii) Find $\overline{29}^{-1}$ in $\mathbf{Z}_{147}$.

Solution: By Euclidean division and back substitution, $1 = 71 \times 29 - 14 \times 147$. Thus $\overline{29}^{-1} = \overline{71}$.

[8.] (i) Compute GCD$(66, 220)$.

Solution: $66 = 2 \times 3 \times 11$, $220 = 2^2 \times 5 \times 11$. Thus GCD$(66, 220) = 2 \times 11 = 22$.

(ii) Let $\mathcal{U} = \{n66 + m220 \mid n,\ m \in \mathbf{Z}\}$. Show that $\mathcal{U}$ is an ideal in $\mathbf{Z}$.

Solution: Let $z = n66 + m220$, $z_1 = n_1 66 + m220$, $z_2 = n_2 66 + m_2 220 \in \mathcal{U}$, and $k \in \mathbf{Z}$ be given. Then $z_1 + z_2 = (n_1 + n_2)66 + (m_1 + m_2)220 \in \mathcal{U}$ and $kz = (kn)66 + (km)220 \in \mathcal{U}$. Thus $\mathcal{U}$ is an ideal.

(iii) Let $\mathcal{U}$ be given in (ii). Find a positive integer d such that $\mathcal{U} = (d)$.

Solution: From class notes, $\mathcal{U} = \{n66 + m220 \mid n,\ m \in \mathbf{Z}\} = \big(\text{GCD}(66, 220)\big) = (22)$, i.e. $d = 22$.

MATH 228 (A1) MIDTERM EXAM

Instructor: James D. Lewis

Wednesday, November 1, 2000

$\star\star\star\star\star\star\star\star\star\star$ Closed Book. No Calculators. $\star\star\star\star\star\star\star\star\star\star$

$\mathbf{N} = \{1, 2, 3, \ldots\}$; $\mathbf{Z} =$ Integers ; $\mathbf{C} =$ Complex Numbers

---

1. Prove by induction on $n \in \mathbf{N}$ that

$$1 + 4 + 7 + \cdots + (3n - 2) = \frac{(3n^2 - n)}{2}.$$

2. (i) Find all the units in $\mathbf{Z}_{30}$.

(ii) Find the multiplicative inverse of $\overline{92}$ in $\mathbf{Z}_{201}$.

(iii) Given that $5\mathbf{Z}_{20} = \{\overline{0}, \overline{5}, \overline{10}, \overline{15}\}$ is a subring of $\mathbf{Z}_{20}$, find all units and zero divisors in $5\mathbf{Z}_{20}$.

3. (i) Show that

$$\mathbf{A} \stackrel{\text{def}}{=} \{p + q\sqrt{-2} \mid p, q \in \mathbf{Z}\},$$

is a subring of $\mathbf{C}$. [Note that $\mathbf{A}$ is contained in $\mathbf{C}$, since $\sqrt{-2} = \sqrt{2} \cdot \sqrt{-1} \in \mathbf{C}$.]

(ii) Compute the units $\mathbf{A}^*$ for the ring $\mathbf{A}$ in (i). Is $\mathbf{A}$ a subfield of $\mathbf{C}$? (Please explain.)

4. Consider the relation $\sim$ on the set $\mathbf{N} \times \mathbf{N}$, given by the prescription:

$$(a, b) \sim (c, d) \Leftrightarrow a \cdot b = c \cdot d.$$

(i) Show that $\sim$ is an equivalence relation.

(ii) Find all elements $(a, b) \in \mathbf{N} \times \mathbf{N}$ such that $(a, b) \sim (2, 2)$.

MATH 228 (A1) MIDTERM EXAM SOLUTIONS

Instructor: James D. Lewis

Wednesday, November 1, 2000

⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆ Closed Book. No Calculators. ⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆

$\mathbf{N} = \{1, 2, 3, \ldots\}$; $\mathbf{Z} =$ Integers ; $\mathbf{C} =$ Complex Numbers

---

[10] **1.** Prove by induction on $n \in \mathbf{N}$ that

$$1 + 4 + 7 + \cdots + (3n - 2) = \frac{(3n^2 - n)}{2}.$$

Solution: Let $P(n)$ be te statement:

$$\underbrace{1 + 4 + 7 + \cdots + (3n - 2)}_{\text{LHS}} = \underbrace{\frac{(3n^2 - n)}{2}}_{\text{RHS}}.$$

Then for $n = 1$, we have LHS $= (3 \cdot 1 - 2) = 1$ and RHS $= \frac{(3 \cdot 1^2 - 1)}{2} = 1$. Thus $P(1)$ is true. We now show that $P(n)$ true $\Rightarrow P(n+1)$ true. If we add $(3(n+1) - 2) = 3n + 1$ to both sides of $P(n)$, then the new LHS becomes $1 + 4 + 7 + \cdots + (3(n+1) - 2)$ and the new RHS becomes $\frac{(3n^2 - n)}{2} + 3n + 1 = \frac{3n^2 - n + 6n + 2}{2} = \frac{3n^2 + 5n + 2}{2} = \frac{3(n+1)^2 - (n+1)}{2}$. Thus we arrive at:

$$1 + 4 + 7 + \cdots + (3(n+1) - 2) = \frac{(3(n+1)^2 - (n+1))}{2},$$

i.e. $P(n+1)$ holds.

[10] **2.** (i)[3/3] Find all the units in $\mathbf{Z}_{30}$.

Solution: [Note that $30 = 2 \cdot 3 \cdot 5$, and hence the Euler-Phi function value is $\varphi(30) = 2 \cdot 4 = 8$. Thus there will be 8 units in all.]

$$\mathbf{Z}_{30}^* = \{\overline{x} \mid (x, 30) = 1\} = \{\overline{1}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{29}\}.$$

(ii)[4/4] Find the multiplicative inverse of $\overline{92}$ in $\mathbf{Z}_{201}$.

Solution: By Euclidean division, we have:

$$\begin{aligned} 201 &= 2 \times 92 + 17 \\ 92 &= 5 \times 17 + 7 \\ 17 &= 2 \times 7 + 3 \\ 7 &= 2 \times 3 + 1 \end{aligned}$$

Thus by back substitution, we have:

$$1 = 7 - 2 \times 3 = 7 - 2 \times (17 - 2 \times 7) = 5 \times 7 - 2 \times 17 = 5 \times (92 - 5 \times 17) - 2 \times 17$$

$$= 5 \times 92 - 27 \times 17 = 5 \times 92 - 27 \times (201 - 2 \times 92) = 59 \times 92 - 27 \times 201.$$

Thus $\overline{92}^{-1} = \overline{59}$.

(iii)[3/3] Given that $5\mathbf{Z}_{20} = \{\overline{0}, \overline{5}, \overline{10}, \overline{15}\}$ is a subring of $\mathbf{Z}_{20}$, find all units and zero divisors in $5\mathbf{Z}_{20}$.

Solution: The multiplication table is given below:

$\bullet$	$\overline{0}$	$\overline{5}$	$\overline{10}$	$\overline{15}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{10}$	$\overline{15}$
$\overline{10}$	$\overline{0}$	$\overline{10}$	$\overline{0}$	$\overline{10}$
$\overline{15}$	$\overline{0}$	$\overline{15}$	$\overline{10}$	$\overline{5}$

It it obvious from the table that $\overline{5}$ is the unity, and that the units are $\{\overline{5}, \overline{15}\}$, and zero divisors are $\{\overline{0}, \overline{10}\}$.

[10] **3.** (i)[5/5] Show that

$$\mathbf{A} \stackrel{\text{def}}{=} \{p + q\sqrt{-2} \mid p, q \in \mathbf{Z}\},$$

is a subring of $\mathbf{C}$. [Note that $\mathbf{A}$ is contained in $\mathbf{C}$, since $\sqrt{-2} = \sqrt{2} \cdot \sqrt{-1} \in \mathbf{C}$.]

Solution: Let $z_1 = p_1 + q_1\sqrt{-2}$, $z_2 = p_2 + q_2\sqrt{-2} \in \mathbf{A}$. Then:

$$z_1 + z_2 = \underbrace{(p_1 + p_2)}_{\in \mathbf{Z}} + \underbrace{(q_1 + q_2)}_{\in \mathbf{Z}}\sqrt{-2} \in \mathbf{A},$$

$$z_1 \cdot z_2 = \underbrace{(p_1p_2 - 2q_1q_2)}_{\in \mathbf{Z}} + \underbrace{(p_1q_2 + p_2q_1)}_{\in \mathbf{Z}}\sqrt{-2} \in \mathbf{A}.$$

Thus $\mathbf{A}$ closed under $+, \bullet$ from $\mathbf{C}$, and the associative, commutative, distributive laws holding for $\mathbf{C}$, implies that the same laws must hold for $\mathbf{A}$. Note that $\mathbf{Z} \subset \mathbf{A}$, by the identification $p \in \mathbf{Z} \mapsto p + 0\sqrt{-2} \in \mathbf{A}$. Thus for example $0, 1 \in \mathbf{A}$. Also $z = p + q\sqrt{-2} \in \mathbf{A} \Rightarrow -z = (-p) + (-q)\sqrt{-2} \in \mathbf{A}$. Thus $\mathbf{A} \subset \mathbf{C}$ is a subring (with unity as well).

(ii)[5/5] Compute the units $\mathbf{A}^*$ for the ring $\mathbf{A}$ in (i). Is $\mathbf{A}$ a subfield of $\mathbf{C}$? (Please explain.)

Solution: For $z = p + q\sqrt{-2}$, set $N(z) = z \cdot \overline{z} = p^2 + 2q^2$. Note that $N(z)$ is an integer ≥ 0. Recall from class notes that $N(z_1 z_2) = N(z_1)N(z_2)$, for any $z_1, z_2 \in \mathbf{A}$. Thus if $z_1 z_2 = 1$, it follows that $N(z_1)N(z_2) = N(z_1 z_2) = N(1) = 1$, hence $N(z_1) = N(z_2) = 1$. Thus $z \in \mathbf{A}^* \Leftrightarrow N(z) = 1 \Leftrightarrow z = \pm 1$. In particular $\mathbf{A}^* = \{1, -1\}$. Thus for example $\sqrt{-2} \in \mathbf{A}$ has no multiplicative inverse, and hence $\mathbf{A}$ is not a subfield of $\mathbf{C}$.

[10] **4.** Consider the relation $\sim$ on the set $\mathbf{N} \times \mathbf{N}$, given by the prescription:

$$(a, b) \sim (c, d) \Leftrightarrow a \cdot b = c \cdot d.$$

(i)[6/6] Show that $\sim$ is an equivalence relation.

Solution: Since $a \cdot b = a \cdot b$ it follows that $(a, b) \sim (a, b)$ [$\Rightarrow$ reflexivity]. Next $(a, b) \sim (c, d) \Leftrightarrow a \cdot b = c \cdot d \Leftrightarrow c \cdot d = a \cdot b \Leftrightarrow (c, d) \sim (a, b)$ [$\Rightarrow$ symmetry holds]. Finally, $(a, b) \sim (c, d)$ & $(c, d) \sim (e, f) \Leftrightarrow a \cdot b = c \cdot d$ & $c \cdot d = e \cdot f \Rightarrow a \cdot b = e \cdot f \Rightarrow (a, b) \sim (e, f)$ [$\Rightarrow$ transitivity holds].

(ii)[4/4] Find all elements $(a, b) \in \mathbf{N} \times \mathbf{N}$ such that $(a, b) \sim (2, 2)$.

Solution: We are looking at $\{(a, b) \in \mathbf{N} \times \mathbf{N} \mid a \cdot b = 4\}$. This gives us $(4, 1)$, $(2, 2)$ and $(1, 4)$.

MATH 228 FINAL EXAM December, 2000

⋆⋆⋆⋆⋆⋆ [This is a closed book exam. No Calculators.]⋆⋆⋆⋆⋆⋆

$\mathbf{Z}=$ integers, $\mathbf{Q}=$ rationals, $\mathbf{R}=$ reals, $\mathbf{C}=$ complex numbers
$\mathbf{A}^*=$ units in a ring $\mathbf{A}$

[1. (15 pts)] (i) Find all the units $\big(\mathbf{Z}_7[x]\big)^*$ in $\mathbf{Z}_7[x]$.
(ii) Find all the zero divisors in $\mathbf{Z}_{10}$.
(iii) Let $\mathbf{A}=\mathbf{Z}[y]$. Find all the units $\big(\mathbf{A}[x]\big)^*$ in $\mathbf{A}[x]$. [Here x, y are variables.]

[2. (10 pts)] Find all values $\overline{a},\ \overline{b}\in\mathbf{Z}_3$ for which the polynomial

$$p(x)=x^3+\overline{a}x+\overline{b}\in\mathbf{Z}_3[x]$$

is irreducible.

[3. (10 pts)] Let

$$\mathcal{U}=\{756\cdot x\ +\ 232\cdot y\mid x,y\in\mathbf{Z}\}.$$

(i) Show that $\mathcal{U}$ is an ideal in $\mathbf{Z}$.
(ii) Find $d\in\mathbf{N}$ such that $\mathcal{U}=(d)$.

[4. (10 pts)] Factor $p(x)=2x^5-3x^4-x^2-5x-2$ into a product of irreducibles in $\mathbf{Q}[x]$.

[5. (10 pts)] Consider the quotient ring $\mathbf{Q}[\overline{x}]:=\mathbf{Q}[x]/\big(p(x)\big)$, where $p(x)=x^3-x^2+x-1$.
(i) Find the multiplicative inverse of $\overline{x}$ in $\mathbf{Q}[\overline{x}]$.
(ii) Find two non-zero zero divisors in $\mathbf{Q}[\overline{x}]$.

[6. (10 pts)] Show that $\sqrt{3}+\sqrt{5}\notin\mathbf{Q}$. [Hint: First verify the identity: $\big[(\sqrt{5}+\sqrt{3})^2-8\big]^2-60=0$.]

[7. (15 pts)] Let $\mathbf{A}$ and $\mathbf{B}$ be rings with unity, and assume given a ring homomorphism $T:\mathbf{A}\to\mathbf{B}$.

(i) Show that if $a\in\mathbf{A}^*$, then $T(a)\in\mathbf{B}^*$.
(ii) Show that $\ker T$ is an ideal in $\mathbf{A}$.

[8. (20 pts)] Let n, m be integers ≥ 2, and consider the ring $\mathbf{A}=\mathbf{Z}_n\times\mathbf{Z}_m$, with componentwise addition and multiplication given by

$$(\overline{x}_n,\overline{y}_m)+(\overline{u}_n,\overline{v}_m)=(\overline{(x+u)}_n,\overline{(y+v)}_m)$$

$$(\overline{x}_n,\overline{y}_m)\bullet(\overline{u}_n,\overline{v}_m)=(\overline{(xu)}_n,\overline{(yv)}_m),$$

and with unity $(\overline{1}_n,\overline{1}_m)\in\mathbf{A}$, and zero element $(\overline{0}_n,\overline{0}_m)\in\mathbf{A}$. Let $T:\mathbf{Z}_{nm}\to\mathbf{A}$ be the map given by

$$T(\overline{x}_{nm})=(\overline{x}_n,\overline{x}_m).$$

(i) Show that T is well-defined.
(ii) Show that T is a ring homomorphism.
(iii) Show that $\ker T=(\overline{k}):=\{\overline{q}\cdot\overline{k}\mid\overline{q}\in\mathbf{Z}_{nm}\}$, where $k=\mathrm{LCM}(n,m)$ (= least common multiple).
(iv) Explain why T is an isomorphism (i.e. $\ker T=0$ and the image $\mathrm{Im}(T)=\mathbf{A}$) in the case that $(m,n)=1$.

MATH 228 FINAL EXAM SOLUTIONS December, 2000

⋆⋆⋆⋆⋆⋆ [This is a closed book exam. No Calculators.]⋆⋆⋆⋆⋆⋆

$\mathbf{Z} =$ integers, $\mathbf{Q} =$ rationals, $\mathbf{R} =$ reals, $\mathbf{C} =$ complex numbers
$\mathbf{A}^* =$ units in a ring $\mathbf{A}$

[1.] (i) Find all the units $\big(\mathbf{Z}_7[x]\big)^*$ in $\mathbf{Z}_7[x]$. [Solution: $\big(\mathbf{Z}_7[x]\big)^* = \mathbf{Z}_7^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$.]
(ii) Find all the zero divisors in $\mathbf{Z}_{10}$. [Solution: $\{\overline{0}, \overline{2}, \overline{4}, \overline{5}, \overline{6}, \overline{8}\}$.]
(iii) Let $\mathbf{A} = \mathbf{Z}[y]$. Find all the units $\big(\mathbf{A}[x]\big)^*$ in $\mathbf{A}[x]$. [Here x, y are variables.]
[Solution: $\big(\mathbf{A}[x]\big)^* = \mathbf{A}^* = \big(\mathbf{Z}[y]\big)^* = \mathbf{Z}^* = \{1, -1\}$.]

[2.] Find all values $\overline{a},\ \overline{b} \in \mathbf{Z}_3$ for which the polynomial

$$p(x) = x^3 + \overline{a}x + \overline{b} \in \mathbf{Z}_3[x]$$

is irreducible. [Solution: There are 9 polynomials to consider. Among those, only $x^3+\overline{2}x+\overline{1}$ and $x^3+\overline{2}x+\overline{2}$ are the polynomials with no roots in $\mathbf{Z}_3$. Hence $(\overline{a}, \overline{b}) = (\overline{2}, \overline{1})$, $(\overline{2}, \overline{2})$ are the only values of $\overline{a}$ and $\overline{b}$ for which $p(x)$ is irreducible.]

[3.] Let

$$\mathcal{U} = \{756 \cdot x \ + \ 232 \cdot y \mid x, y \in \mathbf{Z}\}.$$

(i) Show that $\mathcal{U}$ is an ideal in $\mathbf{Z}$. [Solution: For $x, y, x_1, y_1, x_2, y_2, z \in \mathbf{Z}$, we have $(756x_1+232y_1)+(756x_2+232y_2) = 756(x_1+x_2)+232(y_1+y_2) \in \mathcal{U}$. $z(756x+232y) = 756(zx) + 232(zy) \in \mathcal{U}$.]
(ii) Find $d \in \mathbf{N}$ such that $\mathcal{U} = (d)$. [Solution: $d = (756, 232) = 4$.]

[4.] Factor $p(x) = 2x^5 - 3x^4 - x^2 - 5x - 2$ into a product of irreducibles in $\mathbf{Q}[x]$. [Solution: The only candidates for $\mathbf{Q}$-roots are $\{\pm 1, \pm 2, \pm\frac{1}{2}\}$, and one checks that 1 and $-\frac{1}{2}$ are roots. By long division, $p(x) = (2x+1)(x-2)(x^3+x+1)$. Note that x^3+x+1 has no $\mathbf{Q}$-roots, since the only candidates are ± 1. Thus this gives the irreducible decomposition.]

[5.] Consider the quotient ring $\mathbf{Q}[\overline{x}] := \mathbf{Q}[x]/\big(p(x)\big)$, where $p(x) = x^3 - x^2 + x - 1$.
(i) Find the multiplicative inverse of $\overline{x}$ in $\mathbf{Q}[\overline{x}]$. [Solution: We have $\overline{x}(\overline{x}^2 - \overline{x} + 1) = \overline{x}^3 - \overline{x}^2 + \overline{x} = 1$. Thus $\overline{x}^{-1} = (\overline{x}^2 - \overline{x} + 1)$.]
(ii) Find two non-zero zero divisors in $\mathbf{Q}[\overline{x}]$. [Solution: Note that $p(1) = 0$, thus $(x-1)$ is a factor of $p(x)$. In particular, by long division, $p(x) = (x-1)(x^2+1)$. Thus $(\overline{x}-1)(\overline{x}^2+1) = 0 \in \mathbf{Q}[\overline{x}]$. Hence $\overline{x}-1,\ \overline{x}^2+1$ are zero divisors.]

[6.] Show that $\sqrt{3}+\sqrt{5} \notin \mathbf{Q}$. [Hint: First verify the identity: $\big[(\sqrt{5}+\sqrt{3})^2 - 8\big]^2 - 60 = 0$.] [Solution: Set $p(x) = (x^2-8)^2 - 60 = x^4 - 16x^2 + 4$. Then the only candidates for $\mathbf{Q}$-roots of $p(x)$ are $\{\pm 1, \pm 2, \pm 4\}$. It is obvious that $\sqrt{5}+\sqrt{3}$ is not equal to any of these. Alternatively, none of these candidate roots turn out to be roots of $p(x)$.]

[7.] Let $\mathbf{A}$ and $\mathbf{B}$ be rings with unity, and assume given a ring homomorphism $T : \mathbf{A} \to \mathbf{B}$.

(i) Show that if $a \in \mathbf{A}^*$, then $T(a) \in \mathbf{B}^*$. [Solution: Let $a, b \in \mathbf{A}$ be given such that $ab = 1_A$. Then $1_B = T(1_A) = T(ab) = T(a)T(b)$. Thus $T(\mathbf{A}^*) \subset \mathbf{B}^*$.]
(ii) Show that $\ker T$ is an ideal in $\mathbf{A}$. [Solution: Let $a, b \in \ker T$ and $c \in \mathbf{A}$. Then $T(a+b) = T(a) + T(b) = 0 + 0 = 0 \Rightarrow a + b \in \ker T$. Next, $T(ca) = T(c)T(a) = T(c) \cdot 0 = 0 \Rightarrow ca \in \ker T$.]

[8.] Let n, m be integers ≥ 2, and consider the ring $\mathbf{A} = \mathbf{Z}_n \times \mathbf{Z}_m$, with componentwise addition and multiplication given by

$$(\overline{x}_n, \overline{y}_m) + (\overline{u}_n, \overline{v}_m) = (\overline{(x+u)}_n, \overline{(y+v)}_m)$$

$$(\overline{x}_n, \overline{y}_m) \bullet (\overline{u}_n, \overline{v}_m) = (\overline{(xu)}_n, \overline{(yv)}_m),$$

and with unity $(\overline{1}_n, \overline{1}_m) \in \mathbf{A}$, and zero element $(\overline{0}_n, \overline{0}_m) \in \mathbf{A}$. Let $T : \mathbf{Z}_{nm} \to \mathbf{A}$ be the map given by

$$T(\overline{x}_{nm}) = (\overline{x}_n, \overline{x}_m).$$

(i) Show that T is well-defined. [Solution: We observe that $\overline{x}_{nm} = \overline{y}_{nm} \Leftrightarrow (nm)|(x-y) \Rightarrow n|(x-y)$ & $m|(x-y) \Rightarrow T(\overline{x}_{nm}) = (\overline{x}_n, \overline{x}_m) = (\overline{y}_n, \overline{y}_m) = T(\overline{y}_{nm})$.]
(ii) Show that T is a ring homomorphism. [Solution: $T(\overline{x}_{nm}\overline{y}_{nm}) = T(\overline{(xy)}_{nm}) = (\overline{(xy)}_n, \overline{(xy)}_m) = (\overline{x}_n, \overline{x}_m) \bullet (\overline{y}_n, \overline{y}_m) = T(\overline{x}_{nm})T(\overline{y}_{nm})$; $T(\overline{x}_{nm} + \overline{y}_{nm}) = T(\overline{(x+y)}_{nm}) = (\overline{(x+y)}_n, \overline{(x+y)}_m) = (\overline{x}_n, \overline{x}_m) + (\overline{y}_n, \overline{y}_m) = T(\overline{x}_{nm}) + T(\overline{y}_{nm})$; $T(\overline{1}_{nm}) = (\overline{1}_n, \overline{1}_m)$.]
(iii) Show that $\ker T = (\overline{k}) := \{\overline{q} \cdot \overline{k} \mid \overline{q} \in \mathbf{Z}_{nm}\}$, where $k = \mathrm{LCM}(n, m)$ (= least common multiple). [Solution: Let $k = \mathrm{LCM}(n, m)$. Since $n|k$ and $m|k$, it is obvious that $T(\overline{k}_{nm}) = (\overline{k}_n, \overline{k}_m) = (\overline{0}_n, \overline{0}_m)$, hence $(\overline{k}) \subset \ker T$. On the other hand, if $T(\overline{q}_{nm}) = (\overline{0}_n, \overline{0}_m)$, then $n|q$ and $m|q$. Thus $k|q$, by definition of LCM. Hence $\ker T \subset (\overline{k})$, i.e. $\ker T = (\overline{k})$.]
(iv) Explain why T is an isomorphism (i.e. $\ker T = 0$ and the image $\mathrm{Im}(T) = \mathbf{A}$) in the case that $(m, n) = 1$. [Solution: By (iii), $\ker T = \overline{\mathrm{LCM}(n, m)} = \overline{nm} = \overline{0} \in \mathbf{Z}_{nm}$, where we use the fact that $(m, n) = 1 \Rightarrow \mathrm{LCM}(n, m) = nm$. Thus T is one-to-one. But $\mathbf{A}$ and $\mathbf{Z}_{nm}$ have the same number of elements. Thus T must be onto as well.]

INDEX

[Students are encouraged to supply the appropriate page numbers of the following index topics, for quick reference]

INDEX OF NOTATION

$\subset$	:	Subset, contained in or equal to
$\subset$ $\neq$	:	Contained in but not equal to
(n, m)	:	$=$ GCD(m, n), greatest common divisor
$[m, n]$	:	$=$ LCM$[m, n]$, least common multiple
$a \vert b$	:	a divides b, a is a factor of b
$\mathbf{F}$	:	Field
$\mathbf{N}$	:	Natural numbers $\{1, 2, 3, \ldots\}$
$\mathbf{Z}$	:	Integers $\{0, \pm 1, \pm 2, \pm 3, \ldots\}$
$\mathbf{Q}$	:	Rational numbers
$\mathbf{R}$	:	Real numbers
$\mathbf{C}$	:	Complex numbers
$\mathbf{F}[\sqrt{k}]$	:	Quadratic extension of the field $\mathbf{F}$ given by $\{a + b\sqrt{k} \mid a, b \in \mathbf{F}\}$
$\mathbf{Z}_n$	:	Integers mod n
$\mathbf{A}^*$	:	(Group of) units
(a)	:	Ideal generated by $a \in \mathbf{A}$, $(a) = \{b \cdot a \mid b \in \mathbf{A}\}$
$\mathbf{A}[x]$	:	Polynomial ring over $\mathbf{A}$
$\mathbf{F}[x]$	:	Polynomial ring over the field $\mathbf{F}$
$\mathbf{F}(x)$	:	Rational function field
Quot$(\mathbf{A})$	:	Quotient field of an integral domain $\mathbf{A}$
$\mathbf{A}/\mathcal{U}$	:	Quotient ring
PID	:	Principal ideal domain
UFD	:	Unique factorization domain
$\bigcup, \cup$	:	Union
$\coprod$	:	Disjoint union
$\bigcap, \cap$	:	Intersection
ker	:	Kernel
Char$(\mathbf{F})$	:	Characteristic of a field