Chapter 21

MSMXP5 Polynomials & Rings

(21.1) Binary Operations & Equivalence Relations

(21.1.1) Binary Operations

Definition 1 *A binary operation '+' on a set S is a function $+ \colon S \times S \longrightarrow S$. This is written $(S, +)$.*

Definition 2 *Let $(S, +)$ be a binary operation. The subset $T \subseteq S$ is closed under + if $+|_{T \times T} : T \times T \longrightarrow T$.*

The usual definitions of associativity and commutativity are taken. Note that associativity makes the expression $a + b + c$ meaningful. It is a trivial matter to write down binary operations, however, to write down associative and commutative ones is rather more taxing.

It is sometimes the case that two binary operations "look the same". Even though they may act on completely different sets in completely different ways, it is quite possible that when elements of the sets are labelled in some way, both binary operations produce the same multiplication tables.

Definition 3 *Let $(S, +)$ and $(T, *)$ be sets with binary operations defined upon them. $(S, +)$ is isomorphic to $(T, *)$ provided there exists a bijective function $\theta \colon S \longrightarrow T$ such that $\forall a, b \in S$, $\theta(a + b) = \theta(a) * \theta(b)$. In this case θ is called an isomorphism and it is said that "S is isomorphic to T", written $(S, +) \cong (T, *)$.*

(21.1.2) Equivalence Relations

Although equivalence relations are mentioned elsewhere, they are done so without their proper foundations. Equivalence relations are a special kind of a more general concept—the relation.

Definition 4 *A relation ρ on a set S is a subset of $S \times S$ such that for $a, b \in S$, a is related to B (written $a \, \rho \, b$) if $(a, b) \in \rho$.*

Definition 5 *Suppose that ρ is a relation on a set S then*

1. *If $\forall a \in S$ and $a \, \rho \, a$, then ρ is reflexive.*
2. *If $\forall a, b \in S$, $a \, \rho \, b \Rightarrow b \, \rho \, a$ then ρ is symmetric.*
3. *If $\forall a, b, c \in S$, $a \, \rho \, b$ and $b \, \rho \, c \Rightarrow a \, \rho \, c$ then ρ is transitive.*
4. *A symmetric, reflexive, and transitive relation is called an equivalence relation.*

Lemma 6 *Suppose Ω is a set. Let $\{\Omega_i \mid i \in I\}$ be a set of subsets of Ω such that $\Omega = \bigcup_{i \in I} \Omega_i$ and $\Omega_i \cap \Omega_j = \varnothing$ $\forall i \neq j$. Define now the relation ρ by*

$$\rho = \Big\{ (a, b) \in \Omega \times \Omega \mid \exists j \in I \text{ such that } \{a, b\} \subseteq \Omega_j \Big\}$$

Then rho is an equivalence relation

Proof. $\circlearrowright$ Let $a \in \Omega$, then since the Ω_i form a partition, $\exists j$ for which $a \in \Omega_j$. Since $a \in \Omega_j$ clearly $\{a, a\} \subseteq \Omega_j$ and hence $a \,\rho\, a$.

$\leftrightarrows$ Suppose $a \,\rho\, b$ then for some j, $\Omega_j \supseteq \{a, b\} = \{b, a\}$ so $b \,\rho\, a$.

$\rightrightarrows$ Suppose $a \,\rho\, b$ and $b \,\rho\, c$.
Then $\exists j, k \in I$ such that $\{a, b\} \subseteq \Omega_j$ and $\{b, c\} \subseteq \Omega_k$. Hence

$$\{b\} \subseteq \{a, b\} \cap \{b, c\} \subseteq \Omega_j \cap \Omega_k$$

But by hypothesis, $\Omega_j \cap \Omega_k = \emptyset$ unless $j = k$. Hence $\{a, b, c\} \subseteq \Omega_j = \Omega_k$. In particular $\{a, c\} \subseteq \Omega_j$ so that $a \,\rho\, c$. □

Definition 7 *Let ρ be an equivalence relation on a set Ω. For $a \in \Omega$ define*

$$\Omega_a = [a] = \{b \in \Omega \mid a \,\rho\, b\}$$

This is the equivalence class of a.

Lemma 8 *Let ρ be an equivalence relation on a set Ω and let I be the set of all equivalence classes of ρ on Ω. Then*

1. $\displaystyle\bigcup_{i \in I} i = \Omega$
2. $\forall a, b \in \Omega \quad \Omega_a \cap \Omega_b = \emptyset$ *or* Ω_a

(21.2) Rings, Fields & Vector Spaces

(21.2.1) Rings

Definition 9 *Let R be a non-empty set and let $+ \colon R \times R \to T$ and $\cdot \colon R \times R \to R$ be two binary operations. $(R, +, \cdot)$ is a ring provided that*

(R1) $(R, +)$ *is associative*

(R2) $(R, +)$ *is commutative*

(R3) $\exists 0_R \in R$ *such that* $r + 0_R = r \;\forall r \in R$

(R4) $\forall r \in R \exists r' \in R$ *such that* $r + r' = 0_R$

(R5) $(R, \cdot)$ *is associative*

(R6) The left and right distributivity laws hold. i.e.

$$\forall a, b, c \in R \begin{cases} (a + b)c = ac + bc \\ a(b + c) = ab + ac \end{cases}$$

Definition 10 *Let R be a ring. If $\exists 1_R \in R$ such that $1_R x = x 1_R = x \;\forall x \in R$ then R is called a ring with a 1.*

It is common to refer to a ring without a 1 as a 'rng'. Clearly a ring behaves in many ways similarly to a group or a vector space. It is now possible to prove the usual results of uniqueness and commutativity of identities and inverses.

Lemma 11 *Let R be a ring, and let $r, s, t \in R$. If $r + s = r + t$ then $s = t$.*

Proof. Let $r' \in R$ be such that $r + r' = 0_R$. Then by commutativity $r' + r = 0$. Hence

$$\begin{aligned} r' + (r+s) &= r' + (r+t) \\ (r'+r) + s &= (r'+r) + t \quad \text{by associativity} \\ 0_R + s &= 0_R + t \quad \text{property of } 0_R \\ s + 0_R &= t + 0_R \quad \text{by commutativity} \\ s &= t \quad \text{property of } 0_R \end{aligned}$$ □

Observe the form of the proof: it uses only the axioms as they are stated. Although what is being proved is in most cases blatantly obvious, the point of the proof is to show that the axioms admit the property being proved.

Lemma 12 *Let R be a ring and $r, s \in R$. Then the linear equation $r + x = s$ has a unique solution in R.*

Proof. Let $x = r' + s$, then

$$r + (r' + s) = (r + r') + s = 0_R + s = s$$

Hence this is verified as a solution. It now remains to show this solution to be unique. Let $x_1, x_2 \in R$ be two solutions, so

$$r + x_1 = s \quad \text{and} \quad r + x_2 = s \quad \text{hence} \quad r + x_1 = r + x_2$$

by Lemma 11 $x_1 = x_2$. □

This lemma shows two other important results

- Putting $s = 0_R$ shows that r' is the unique inverse of r with respect to $+$. It is now meaningful to write $r' = -r$.
- Putting $s = r$ and $x = 0_R$ shows that 0_R is unique, so that it is now meaningful to write $0_R = 0$.

Lemma 13 *Let R be a ring with a 1, then 1_R is the unique element of R with the property $x1_R = 1_R x = x \ \forall x \in R$.*

Proof. Suppose $\exists 1'_R \in R$ with the same property. Then

$$1'_R = 1'_R 1_R = 1_R$$

using first the fact that 1_R is a 1 and then that $1'_R$ is a 1. □

Lemma 14 *Let R be a ring and $r, s \in R$ then*

1. *$r0 = 0r = 0$*
2. *$r(-s) = (-r)s = -(rs)$*
3. *$(-r)(-s) = rs$*

Proof. 1. From the properties of 0,

$$\begin{aligned} 0 + 0 &= 0 \\ r(0+0) &= r0 \quad \text{now let } r0 + s = 0 \text{ which can be done, by the axioms} \\ (r0 + r0) + s &= r0 + s \\ r0 + (r0 + s) &= 0 \\ r0 &= 0 \end{aligned}$$

To show $0r = 0$ simply start with $(0+0)r = 0r$ and follow a similar process.

2. From above $r0 = 0$ so now use distributivity as follows

$$\begin{aligned} r0 &= 0 \\ r(s + (-s)) &= (rs) + (-(rs)) \\ rs + r(-s) &= \\ r(-s) &= -(rs) \quad \text{using Lemma 11} \end{aligned}$$

The other part can be shown starting with $0r = 0$.

3. Using part 2 $r(-s) = (-r)s$. Now replace r with $-r$ and observe that

$$-(-r) = r$$

□

Looking in the obvious places, it is easy to find a number of examples of rings.

- The integers modulo n. Note the well-definition of addition and multiplication are shown in the usual way. $\mathbb{Z}_n$ inherits most requirements to be a ring from $\mathbb{Z}$. Notice that $[0]$ acts as 0 and $[1]$ acts as 1.
- The Gaussian integers,
$$J = \{a + ib \mid a, b \in \mathbb{Z}\}$$
form a ring when addition and multiplication are defined in the obvious way.
- A boolean ring consists not of numbers but of sets, and are commonly used in computer science. Let Ω be a set and define

$$\begin{aligned} +\colon \mathcal{P} \times \mathcal{P} \to \mathcal{P} \quad &\text{by} \quad (A, B) \mapsto (A \cup B) \setminus (A \cap B) \\ \cdot\colon \mathcal{P} \times \mathcal{P} \to \mathcal{P} \quad &\text{by} \quad (A, B) \mapsto A \cap B \end{aligned}$$

Definition 15 *Let R be a ring.*

- *If $ab = ba$ $\forall a, b \in R$ then R is called a commutative ring.*
- *$R^* = R \setminus \{0\}$.*
- *If $a, b \in R^*$ and $ab = 0$ then a and b are called zero divisors.*

Definition 16 *An integral domain is a commutative ring with a 1 ($1 \neq 0$) which has no zero divisors*

Theorem 17 *Let R be a ring. Then the cancellation laws hold in R if and only of R is an integral domain.*

Proof. ($\Rightarrow$) Suppose the cancellation laws hold in R and let $a \in R^*$ and $b \in R$ with $ab = 0 = a0$. Then by cancellation $b = 0$ hence there can be no zero divisors, so R is an integral domain.

($\Leftarrow$) Suppose that R is an integral domain and let $a \in R^*$ and $b, c \in R$.
Assume $ab = ac$ then $ab - ac = 0$ so $a(b - c) = 0$.
Since R is an integral domain and $a \neq 0$ it must be the case that $b - c = 0$ and so $b = c$. Hence the cancellation laws hold. □

While in general $\mathbb{Z}_n$ is a ring, it is certainly not an integral domain. For example in $\mathbb{Z}_6$, $[2][3] = [0]$. It can be shown that $\mathbb{Z}_n$ is an integral domain only when n is prime.

Definition 18 *Let R be a ring with a 1.*

- *If $\forall a \in R^*$ $\exists b \in R^*$ such that $ab = 1$ then a is invertible.*

- *If every element of R^* is invertible then R is called a division ring.*
- *If R is a commutative division ring, then R is called a field.*

It is quite reasonable to suppose that a division ring has no zero divisors, as if it did the relationship $ab = 1$ would not hold universally.

Lemma 19 *Every field is an integral domain.*

Proof. Let F be a field and suppose $x \in F$ and $y \in F^*$ such that $xy = 0$. Then
$y^{-1} \in F^*$ and $(xy)y^{-1} = x(yy^{-1}) = x$
But also, $(xy)y^{-1} = 0y^{-1} = 0$
hence $x = 0$, meaning that F has no zero divisors. □

Lemma 20 *Every finite integral domain is a field.*

Proof. It is necessary to show that every element of an integral domain has an inverse. Define a map $\phi_r \colon R \to R$ by $t \mapsto tr$ where R is a finite integral domain.
Suppose $\phi_r(t) = \phi_r(u)$ then $tr = ur$ so $t = u$ by cancellation. Hence ϕ is one-to-one (injective). However, since R is finite[*] ϕ is also onto (surjective). Hence ϕ is a bijection.
Since $1 \in R$, $\exists s \in R$ such that $\phi_r(s) = 1$ i.e. such that $rs = 1$. But since R is commutative, $rs = sr = 1$ so s is the inverse of r.
Since ϕ_r can be defined for all $r \in R$, an inverse must exist for all $r \in R$ and hence R is a field. □

Note that $\mathbb{Z}$ is an integral domain that is not a field. The criterion of finiteness fails.

Theorem 21 (Wedderburn) *Every finite division ring is a field.*

Definition 22 *A subring S of a ring R is a subset of R which is itself a ring.*

Lemma 23 *A subset S of a ring R is a subring of R if and only if*

1. $S \neq \emptyset$
2. $\forall a, b \in S$, $ab \in S$ *and* $a - b \in S$

Proof. If S is a ring, then trivially these properties hold. For the reverse implication most of the required properties are inherited from R. The only two which are not are the existence of a zero and the existence of additive inverses. As well as these there is the matter of closure.

Trivially, the two conditions show S to be closed. Let $b = a$ then $a - b = 0$ so there is a zero in S. Now let $a = 0$ so clearly additive inverses are in S. Hence the proof is complete. □

Lemma 24 *Let $\phi \colon R \to S$ be a homomorphism then*

1. $\phi(0_R) = 0_S$
2. $\phi(-a) = -\phi(a)\ \forall a \in R$
3. *Where* $\ker\phi = \{r \in R \mid \phi(r) = 0_S\}$, $\ker\phi$ *is a subring of S which satisfies the property* $rk \in \ker\phi$ *and* $kr \in \ker\phi$ *for all $r \in R$ and $k \in \ker\phi$.*

Proof.
1. $\phi(a) = \phi(a + 0_R) = \phi(a) + \phi(0_R)$ hence the result.
2. $0_S = \phi(0_R) = \phi(a - a) = \phi(a) + \phi(-a)$ hence the result.

[*] Recall that if a function between finite sets is one-to-one then it is onto.

3. Let $k_1, k_2 \in \ker\phi$ then
   - $\phi(k_1 - k_2) = \phi(k_1) - \phi(k_2) = 0_S - 0_S = 0_S$ so $k_1 - k_2 \in \ker\phi$.
   - $\phi(k_1 k_2) = \phi(k_1)\phi(k_2) = 0_S 0_S = 0_S$ so $k_1 k_2 \in \ker\phi$.

   Hence by the test for a subring, $\ker\phi$ is a subring of R. To prove the remaining part,

$$\phi(rk) = \phi(r)\phi(k) = \phi(r)0_S = 0_S$$

Hence $rk \in \ker\phi$. Similarly, $kr \in \ker\phi$. □

Theorem 25 *Suppose that $\phi\colon R \to S$ is a homomorphism. ϕ is a monomorphism if and only if $\ker\phi = \{0_R\}$.*

Proof. $(\Rightarrow)$ Suppose ϕ is a monomorphism and suppose $k \in \ker\phi$.
For $r \in R$ this gives $\phi(r + k) = \phi(r) + \phi(k) = \phi(r) + 0_S = \phi(r)$.
Since ϕ is a monomorphism it must therefore be the case that $r + k = r$ and hence $k = 0_R$. hence $\ker\phi = \{0_R\}$.

$(\Leftarrow)$ Suppose $\ker\phi = \{0_R\}$ and let $r_1, r_2 \in R$ with $\phi(r_1) = \phi(r_2)$.
Hence $0_S = \phi(r_1) - \phi(r_2) = \phi(r_1 - r_2)$.
So $r_1 - r_2 \in \ker\phi$ meaning that $r_1 - r_2 = 0_R$. Therefore $r_1 = r_2$ and hence ϕ is a monomorphism. □

(21.2.2) Fields Of Fractions

The rationals are constructed from the integers using an equivalence relation. In a similar way, every integral domain (such as $\mathbb{Z}$) can generate a field of fractions. Furthermore, such a field contains a subring isomorphic to the integral domain—$\mathbb{Z}$ is embedded in Q.

Lemma 26 *Let F be a field and D be a subring of F. If $1 \in D$ then D is an integral domain.*

Observe that although all fields are integral domains, it does not follow that subrings of fields are.

Proof. Since F is a field and $D \subset F$, D is commutative. By hypothesis D contains a 1. What remains to be shown is the absence of zero divisors in D.

Assume $x, y \in D$ and $xy = 0$. Note that it is not necessarily the case that x^{-1} or y^{-1} are in D, but they do exist in F.
If $y \neq 0$ then $xyy^{-1} = 0y^{-1} = 0$ so $x = 0$.
If $x \neq 0$ then $x^{-1}xy = x^{-1}y = 0$ so $y = 0$.
Hence D is an integral domain. □

Theorem 27 *Let D be an integral domain. There exists a field which contains a subring that is isomorphic to D. This field is called the field of fractions of D.*

Proof. Let $S = \{(a, b) \mid a \in D,\ b \in D^*\}$ and define the relation ρ on S by

$$(a, b)\,\rho\,(c, d) \Leftrightarrow ad = bc$$

This is now shown to be an equivalence relation.

reflexive: Since D is an integral domain $ab = ba$ hence $(a, b)\,\rho\,(a, b)$.

symmetric: Suppose $(a, b)\,\rho\,(c, d)$ then $ad = bc$ so $bc = ad$ and hence $(c, d)\,\rho\,(a, b)$.

transitive: Suppose $(a,b)\,\rho\,(c,d)$ and $(c,d)\,\rho\,(e,f)$ then $ad = bc$ and $cf = de$.
Hence $adcf = bced$ so $adcf - bced = 0$ so $(af - be)cd = 0$.
If $af - be = 0$ then $af = be$ so $(a,b)\,\rho\,(e,f)$.
If $cd = 0$ then c=0 since $d \in D^*$. Hence since $ad = bc$ it must be the case that $a = 0$ and similarly from $cf = de$, $e = 0$. Hence $af = be = 0$ and the relation still holds.

Now let F be the set of equivalence classes of ρ. Define multiplication and addition on F as follows.

$$[a,b] + [c,d] = [ad + bc, bd] \qquad\qquad [a,b][c,d] = [ac, bd]$$

It is now necessary to show that these are well defined.

Say $[a,b] = [a',b']$ then $(a,b)\,\rho\,(a',b')$ so $ab' = a'b$. Similarly, say $[c,d] = [c',d']$ giving $cd' = c'd$.
Now, $[a',b'] + [c',d'] = [a'd' + b'c', b'd']$ and it must be shown that this is equivalent to $[ad + bc, bd]$.

$$\begin{aligned}(a'd' + b'c')bd &= (a'd')bd + (b'c')bd \\ &= (a'b)d'd + (c'd)b'b \\ &= (ab')d'd + (cd')b'b \\ &= (ad + bc)b'd'\end{aligned}$$

Hence the equivalence is shown, so addition is well defined.

For multiplication, $[a',b'][c',d'] = [a'c', b'd']$ Now,

$$(a'c')(bd) = (a'b)(c'd) = (ab')(cd') = (ac)(b'd')$$

Hence $(ac,bd)\,\rho\,(a'c',b'd')$ and so multiplication is well defined.

The axioms for a ring are now verified

1. $[a,b] + [c,d] = [ad + bc, bd] = [cb + da, db] = [c,d] + [a,b]$ this uses the fact that addition and multiplication are commutative in the integral domain D.
2. For associativity,

$$\begin{aligned}[a,b] + ([c,d] + [e,f]) &= [a,b] + [cf + de, df] \\ &= [adf + bcf + bde, bdf] = [(ad + bc)f + (bd)e, (bd)f] \\ &= [ad + bc, bd] + [e,f] \\ &= ([a,b] + [b,c]) + [e,f]\end{aligned}$$

3. Consider $[0,d]$ then for all $[a,b] \in F$, $[a,b] + [0,d] = [ad + 0b, bd] = [ad, bd]$
Now, $a(bd) = b(ad)$ so $(ad,bd)\,\rho\,(a,b)$. Therefore $[ad,bd] = [a,b]$ which means that F has additive zero, $[0] = [0,d]$.
4. $[a,b] + [-a,b] = [ab + (-a)b, b^2] = [0, b^2] = [0]$, so F contains additive inverses.
5. $[a,b]([c,d][e,f]) = [a,b][ce,df] = [ace,bdf] = [ac,bd][e,f] = ([a,b][c,d])[e,f]$ hence multiplication is associative.
6. Cancellation is inherited from D.

Hence F is a ring. It is now shown that F is a field.

- $[a,b][1,1] = [1a,1b] = [a,b] = [a1,b1] = [a,b][1,1]$ so F has a multiplicative identity.
- Suppose $[a,b] \neq [0]$, then $[b,a] \in F$ since $a \neq 0$.
  Now, $[a,b][b,a] = [ab,ab]$. But $(ab)1 = 1(ab)$ and so $[ab,ab] = [1,1]$. Hence all non-zero elements of F have multiplicative inverses in F.
- $[a,b][c,d] = [ad,bc] = [da,cb] = [c,d][a,b]$ so commutativity is inherited from D.

hence F is a field.

The final part of the proof is to show that there exists a subring of F isomorphic to D. Let

$$D_1 = \{[d,1] \in F \mid d \in D\}$$

And define the function μ

$$\mu\colon D \to D_1 \quad \text{by} \quad \mu\colon d \mapsto [d,1]$$

then

$$\begin{aligned}\mu(d_1 + d_2) &= [d_1 + d_2, 1] = [d_1,1] + [d_2,1] = \mu(d_1) + \mu(d_2)\\ \mu(d_1 d_2) &= [d_1 d_2, 1] = [d_1,1][d_2,1] = \mu(d_1)\mu(d_2)\end{aligned}$$

Hence μ is a homomorphism. Certainly μ is onto, but furthermore

$$\mu(d) = 0 \;\Rightarrow\; [d,1] = [0] \;\Rightarrow\; d = 0$$

Hence $\ker\mu = \{0\}$ and so μ is injective. Hence μ is an isomorphism, giving $D \cong D_1 \subset F$ as required. □

Theorem 28 *Let D be an integral domain and let K be a field of fractions containing D. Then there exists a subfield F of K which is isomorphic to the field of fractions of D.*

Proof. Let F_1 be the field of fractions of D and define

$$\phi\colon F_1 \to K \quad \text{by} \quad \phi\colon [d,c] \mapsto dc^{-1}$$

Observe that since $c \neq 0$ and $c \in D \subset K$, c^{-1} exists in K (though not necessarily in D). Now,

$$\begin{aligned}\phi([a,b]+[c,d]) &= \phi([ad+bc,bd]) & \phi([a,b][c,d]) &= \phi([ac,bd])\\ &= (ad+bd)(bd)^{-1} & &= (ac)(bd)^{-1}\\ &= ab^{-1} + cd^{-1} & &= (ab^{-1})(cd^{-1})\\ &= \phi([a,b]) + \phi([c,d]) & &= \phi([a,b])\phi([c,d])\end{aligned}$$

Hence ϕ is a homomorphism. Now,

$$\ker\phi = \{[a,b] \in F_1 \mid ab^{-1} = 0\} = \{[0]\}$$

so ϕ is injective. Putting

$$F = \{\phi([a,b]) \mid [a,b] \in F_1\}$$

makes ϕ onto, so ϕ is an isomorphism and $F \cong F_1$ as required. □

(21.3) Ideals & Quotients

(21.3.1) Ideals

Definition 29 *Let K be a subset of a ring R. K is an ideal (of R) if*

1. *K is a subring of R.*
2. *$rk \in K$ and $kr \in k$ $\forall r \in R$ and $\forall k \in K$.*

If K is an ideal of R, this is written $K \trianglelefteq R$.

An ideal of a ring is rather like a normal subgroup. Clearly if R is a ring then R and $\{0\}$ are ideals of R. In a similar way to normal subgroups, the kernel of a homomorphism is an ideal.

Definition 30 *If I is an ideal of a ring R and $I = aR$ for some $r \in R$ then I is called a principal ideal. Furthermore, if all ideals of R are principal then R is called a principal ideal domain.*

Lemma 31 *If R is a commutative ring, then for any $a \in R$, $aR = \{ar \mid r \in R\}$ is an ideal of R.*

Proof. Let ar_1 and ar_2 be elements of aR. $ar_1 - ar_2 = a(r_2 - r_2) \in aR$.
Now, for any $s \in R$, $s(ar) = a(rs) \in aR$ and hence aR is an ideal of R. This holds for all $s \in aR$ (because $aR \subseteq R$) and so aR must be a subring. Furthermore this holds for all $s \in R$ and hence aR is an ideal. □

Observe that if $I \trianglelefteq R$ and $1 \in I$ then $I = R$. This follows straight from the definition since $1 \in I \Rightarrow 1r \in I$ for all $r \in R$.

Theorem 32 *Let D be a division ring, then the only ideals of D are D and $\{0\}$.*

Proof. Suppose $I \trianglelefteq D$ and $I \neq \{0\}$. Let $a \in I$ then since D is a division ring, $a^{-1} \in D$. But by the definition of an ideal, $aa^{-1} \in I$ hence $1 \in I$ and so $I = D$. □

Theorem 33 *Let R be a commutative ring with a 1. If the only ideals of R are R and $\{0\}$ then R is a field.*

Proof. Suppose $a \in R^*$ and let $K = aR$ so by Lemma 31 K is an ideal of R.
By hypothesis $K = R$ or $K = \{0\}$.
If $K = R$ then since R has a 1, $1 \in K = aR$ and so there exists $b \in aR$ such that $ab = 1$ i.e. a is invertible and hence R is a field.
If however $K = \{0\}$ then since $1 \in R$ it must be the case that $a1 = 0$. But this contradicts $a \neq 0$ and so $K \neq \{0\}$. □

Lemma 34 *If I and J are deals then so are $I \cap J$ and*

$$I + J = \{i + j \mid i \in I \; j \in J\}$$
$$IJ = \left\{ \sum_{s=0}^{n} i_s j_s \mid i \in I \; j \in J \; n \in \mathbb{N} \right\}$$

Furthermore $IJ \subseteq I \cap J$.

(21.3.2) Quotients

Let R be a ring and $I \trianglelefteq R$. For $r \in R$ define

$$r + I = \{r + i \mid I \in I\}$$

Define now the relation $\mathcal{Q}$ such that

$$\mathcal{Q}(r,s) = \{(r,s) \in R \times R \mid r - s \in I\}$$

First of all this is shown to be an equivalence relation.

(↻) Since $0 \in I$ (because I is a ring), $r - r = 0 \in I$ for all $r \in R$. Hence $(r,r) \in \mathcal{Q}$.

(↔) Suppose $r\,\mathcal{Q}\,s$ then $r - s \in I$. But I is a ring and therefore $-(r-s) = s - r \in I$ and hence $s\,\mathcal{Q}\,r$

(⇉) Suppose $r\,\mathcal{Q}\,s$ and $s\,\mathcal{Q}\,t$ then $r - s \in I$ and $s - t \in I$. Since I is a ring the sum of these must be in I i.e. $r - t \in I$ and hence $r\,\mathcal{Q}\,t$.

Hence $\mathcal{Q}$ is an equivalence relation.

Consider the equivalence classes of $\mathcal{Q}$. Observe that $r - s \in I$ means that $r \in s + I$, so these are the equivalence classes.

Definition 35 *Let R be a ring and $I \trianglelefteq R$. The quotient ring of R by I is the field which has elements that are the equivalence classes of $\mathcal{Q}$, namely*

$$\frac{R}{I} = R \mod I = \{r + I \mid r \in R\}$$

In $R \mod I$ define addition and multiplication in the following ways.

$$\begin{aligned} +\colon \frac{R}{I} \times \frac{R}{I} \longrightarrow \frac{R}{I} \quad &\text{defined by} \quad +\colon (r+I) + (s+I) \mapsto (r+s) + I \\ \cdot\colon \frac{R}{I} \times \frac{R}{I} \longrightarrow \frac{R}{I} \quad &\text{defined by} \quad \cdot\colon (r+I)(s+I) \mapsto rs + I \end{aligned}$$

It is now necessary to show these to be well defined. Suppose $r + I = r' + I$ and $s + I = s' + I$.

Now, $r' = r' + 0$ and $0 \in I$. Therefore $r' \in r' + I = r + I$ and so $\exists i \in I$ such that $r' = r + i$.
Similarly, $s' = s' + 0$ and $0 \in I$. Therefore $s' \in s' + I = s + I$ and so $\exists j \in I$ such that $s' = s + j$. Hence

$$(r' + I) + (s' + I) = ((r+i) + I) + ((s+j) + I) = ((r+s) + (i+j)) + I = (r+s) + I$$

since $i + j \in I$ because I is a ring. Hence $(r + s + I) \cap (r' + s' + I) \neq \emptyset$ and since these are equivalence classes this means they must be equal. Hence addition is well defined.

Now, $r's' = (r+i)(s+j) = rs + rj + si + ij$. But since I is an ideal, $rj \in I$, $si \in I$ and $ij \in I$. Therefore

$$r's' + I = (r' + I)(s' + I) = rs + rj + si + ij + I = rs + I$$

Hence multiplication is well defined.

It now remains to prove the 6 axioms for a ring plus the properties for a field. This is omitted.

Lemma 36 *Let R be a ring and $I \trianglelefteq R$, then*

1. *$0 + I$ is the zero of $R \mod I$.*
2. *$-(a + I) = (-a) + I$*
3. *If R has a 1 and $I \neq R$ then $1 + I$ is a 1 of $R \mod I$.*

Theorem 37 *Let R be a ring and $I \trianglelefteq R$. Then*

$$\phi\colon R \longrightarrow \frac{R}{I} \quad \textit{defined by} \quad \phi\colon r \mapsto r + I$$

is an epimorphism with $\ker\phi = I$.

Proof. First of all, to show that ϕ is a homomorphism,

$$\phi(r+s) = (r+s) + I = (r+I) + (s+I) = \phi(r) + \phi(s)$$
$$\phi(rs) = rs + I = (r+I)(s+I) = \phi(r)\phi(s)$$

So ϕ is a homomorphism. Now,

$$\begin{aligned}\ker\phi &= \{x \in R \mid \phi(x) = 0 + I\}\\ &= \{x \in R \mid x + I = 0 + I\}\\ &= \{x \in R \mid x \in I\} = I\end{aligned}$$

Trivially ϕ is an epimorphism since if $r + I \in R \mod I$ then there must certainly exist $r \in R$ such that $\phi(r) = r + I$. □

Theorem 38 (First Isomorphism) *Let* $\phi\colon R \to S$ *be a homomorphism, then* $\frac{R}{\ker\phi} \cong \operatorname{Im}\phi$.

From this it is evident that if ϕ is an epimorphism, $\frac{R}{\ker\phi} \cong S$.

Theorem 39 (Third Isomorphism) *Suppose that* $\phi\colon R \to S$ *is an epimorphism, then there exists a 1 to 1 correspondence between the subrings of* R *that contain* $\ker\phi$ *and the subrings of* S.

This correspondence also holds when "subring" is replaced with "ideal".

Definition 40 *An ideal* $M \neq R$ *is a maximal ideal of* R *if for all ideals* K *such that* $M \subset K$, $K = M$ *or* $K = R$.

Lemma 41 *If* p *is prime then* $p\mathbb{Z}$ *is a maximal ideal of* $\mathbb{Z}$.

Proof. Firstly $\mathbb{Z}$ is shown to be a principal ideal domain, then the main result is shown.

Suppose $K \trianglelefteq \mathbb{Z}$ and choose $k \in K$ such that $|k|$ is minimal. Since K is an ideal, $k\mathbb{Z} \subset K$.
Let $t \in K$ then $t = nk + r$ where $r < k$ (or $r = 0$). But $t \in K$ and $nk \in K$ (since $k \in K$ and K is an ideal) therefore $r = t - nk$ must be in K. This contradicts the minimality of $|k|$ unless $r = 0$. Hence when $K \trianglelefteq \mathbb{Z}$ all elements of K are of the form nk, i.e. $K = k\mathbb{Z}$.

Let p be prime and let $K \trianglelefteq \mathbb{Z}$ with $p\mathbb{Z} \subset K$. From above $K = a\mathbb{Z}$ for some $a \in \mathbb{Z}$.
Now, $p \in a\mathbb{Z}$ means that $p = an$ but since p is prime, a but be either ± 1 or $\pm p$ and therefore $K = \mathbb{Z}$ or $K = p\mathbb{Z}$. Therefore $p\mathbb{Z}$ is a maximal ideal. □

Theorem 42 *Let* R *be a commutative ring with a* 1 *and* I *be a maximal ideal of* R. *Then* $\frac{R}{I}$ *is a field.*

Proof. There are only 2 ideals in R which contain I, namely R and I. By Theorem 37 an epimorphism between R and $\frac{R}{I}$ exists and has kernel I. Hence by the third isomorphism theorem $\frac{R}{I}$ has only two subrings (which must be $\{0\}$ and $\frac{R}{I}$) both of which are ideals and so by Theorem 33 is a field. □

(21.4) Polynomials

Definition 43 *A polynomial of degree* n *in the indeterminate* x *with coefficients in a ring* R *is an expression of the form*

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

where $a_n \neq 0$.

Note x is not a variable, just an 'indeterminate'. Indeed to write $3x = 4$ is most incorrect, as these two polynomials are blatantly not equal. However, with the aid of a homomorphism it is possible to 'evaluate' a polynomial—what would usually be to simply substitute in.

Lemma 44 (Evaluation Homomorphism) *Let E be a field and F be a subfield of E. If $\alpha \in E$ then*

$$\phi_\alpha \colon F[x] \to E \quad by \quad \phi_\alpha \colon p(x) \mapsto p(\alpha)$$

is a homomorphism.

Definition 45 *The degree of a polynomial p is denoted* $\deg p$ *and* $\deg 0$ *is defined to be $-\infty$. The degree of any other constant is 0.*

Definition 46 *Let R be a commutative ring with a* 1*. Then*

$$R[x] = \{p(x) \mid \deg p \geqslant 0\} \cup \{0\}$$

Addition and multiplication are defined in the obvious way.

Theorem 47 *Whenever R is a commutative ring with a* 1*, so is $R[x]$.*

Proof. Simply verify the axioms. □

Lemma 48 *Let R be an integral domain and let $p, q \in R[x]$, then* $\deg(p(x)q(x)) = \deg p(x) + \deg q(x)$*.*

Proof. Suppose $\deg p = n$ and $\deg q = m$ then

$$\begin{aligned} p(x) &= a_n x^n + \cdots + a_0 \\ q(x) &= b_m x^m + \cdots + b_0 \end{aligned}$$

The highest coefficient obtainable in pq is that of x^{m+n} which is given by $a_n b_m$. Since $a_n \neq 0$ and $b_m \neq 0$ and R is an integral domain, $a_n b_m \neq 0$ and hence $\deg pq = \deg q + \deg q$. □

It is immediately clear from this that if R is an integral domain, so is $R[x]$.

Corollary 49 *Let F be a field then the units of $F[x]$ (the invertible elements) are precisely the non-zero constant polynomials.*

Proof. Suppose $f \in F[x]$ is invertible, then $\exists g \in F[x]$ such that $fg = 1$. Hence

$$\deg 1 = 0 = \deg fg = degf + \deg g$$

Since the degree of a polynomial is in $\mathbb{Z}_0^+$ it must be the case that $\deg f = \deg g = 0$. For the converse, it is trivial that constant non-zero polynomials are invertible as F is a field. □

Theorem 50 (The Division Algorithm) *Let F be a field and let p and q be polynomials in $F[x]$ with $q(x) \neq 0$. Then there exists $r(x)$ and $t(x)$ in $F[x]$ such that $p(x) = q(x)t(x) + r(x)$ and* $\deg r < \deg q$*.*

Proof. If $\deg p < \deg q$ then set $p = qt + p$ with $t(x) = 0$.

Suppose $\deg p \geqslant \deg q$ and since the first case is proved induction can be used. Let

$$p(x) = a_n x^n + \cdots + a_0 \quad \text{and} \quad q(x) = b_m x^m + \cdots + b_0$$

Define

$$\begin{aligned} p_1(x) &= p(x) - \frac{a_n}{b_m} q(x) x^{n-m} \qquad (51) \\ &= a_n x^n + \cdots + a_0 - \frac{a_n}{b_m} b_m x^m x^{n-m} - \frac{a_n}{b_m} b_{m-1} x^{m-1} x^{n-m} - \cdots - \frac{a_n}{b_m} b_0 x^{n-m} \\ &= \left(a_{n-1} - \frac{a_n}{b_m} b_{m-1} \right) x^{n-1} + \ldots \end{aligned}$$

So $\deg p_1 < \deg p$. But similarly (by induction) $p_1 = t_1 q + r_1$, so now substituting into (51)

$$\begin{aligned} t_1(x) q(x) + r_{1(x)} &= p(x) - \frac{a_n}{b_m} q(x) x^{n-m} \\ p(x) &= q(x) \left(t_1(x) + \frac{a_n}{b_m} x^{n-m} \right) + r_1(x) \end{aligned}$$

So let $r = r_1$ and $t(x) = t_1(x) + \frac{a_n}{b_m} x^{n-m}$ and the result is shown. □

Algebraic long division works as usual, but care must be taken regarding the field over which one is working. For example in $\mathbb{Z}_5$, $1 \div 2 = 3$.

Definition 52 *Let R be an integral domain. Then the principal ideals of R are all the ideals of the form aR where $a \in R$. If all the ideals of R are principal ideals, then R is called a principal ideal domain.*

Lemma 53 *If F is a field then $F[x]$ is a principal ideal domain.*

Proof. Let $J \trianglelefteq F[x]$. If $J = \{0\}$ then $J = 0F[x]$ so is principal. Assume $J \neq \{0\}$ and let $s \in J \setminus \{0\}$ be chosen such that $\deg s$ is minimal.
Let $q \in J$ then by the division algorithm $q = ts + r$. Therefore $r = q - ts$ and so r must be in J. But $\deg r < \deg s$ so if this is not to be a contradiction, it must be the case that $r = 0$. So $q = ts = st \in sF[x]$ but $sF[x] \subseteq J$ (because $sr \in J \ \forall r \in F[x]$ by the property of ideals) hence since q was any element of J, $J = sF[x]$. □

Observe that principal ideals are, in this case, generated by the element of smallest degree.

(21.4.1) Irreducibles

Definition 54 *A non-zero polynomial $p \in F[x]$ where F is a field is called an irreducible if and only if $p(x) = a(x)b(x)$ implies $\deg a = 0$ or $\deg b = 0$.*

For example it is clear that $x^2 + 1$ is irreducible in $\mathbb{R}[x]$ as its linear factors are complex. However, it is reducible in $\mathbb{C}[x]$ and also in $\mathbb{Z}_2[x]$ where $x^2 + 1 = (x+1)^2$.

Lemma 55 *Let F be a field and $p \in F[x]$ with $\deg p \geqslant 1$. If p is irreducible then $pF[x]$ is a maximal ideal. This ideal will be denoted $\langle p \rangle$.*

Proof. This proof takes a slightly unusual form using $A \Rightarrow B \equiv \neg(A \wedge \neg B)$.

Let $J = pF[x]$ and suppose J is not maximal, then there exists an ideal M such that $M \neq F[x]$ and $J \subset M$.
Since $F[x]$ is a principal ideal domain (by Lemma 53) it must be the case that $M = sF[x]$ for some $s \in F[x]$.
Certainly $p \in J$ and since $J \subseteq M$, $p \in M$.
Since $p \in M$, $p = sr$ for some $r \in F[x]$.
Since p is irreducible, this can only not be a contradiction is when $\deg r = 0$ or $\deg s = 0$.

If $\deg s = 0$ then $M = sF[x] = F[x]$ which contradicts $M \neq F[x]$ so the theorem holds.
If $\deg r = 0$ say $r(x) = r \in F$ which has an inverse. Hence $s = pr^{-1}$ and is therefore in J. But then $M = sF[x] \subseteq J$ which contradicts $J \subset M$. □

Theorem 56 *If F is a field and $p \in F[x]$ is irreducible, then $\frac{F[x]}{\langle p \rangle}$ is a field.*

Proof. By Lemma 55 since p is irreducible, $\langle p \rangle$ is a maximal ideal of $F[x]$. By Theorem 42 the result is obtained. □

This provides yet another way to make new fields. However, not all such fields are new. Considering the function

$$\phi \colon \mathbb{C} \to \frac{\mathbb{R}[x]}{\langle x^2+1 \rangle} \quad \text{defined by} \quad \phi \colon a + ib \mapsto bx + a + \langle x^2+1 \rangle$$

Showing this to be an isomorphism shows $\frac{\mathbb{R}[x]}{\langle x^2+1 \rangle} \cong \mathbb{C}$ and so isn't a 'new' field at all.

A ring $\frac{\mathbb{Z}[x]}{\langle p(x) \rangle}$ is "the polynomials modulo $p(x)$". Its elements are simply the remainders under division by $p(x)$. For example

$$\frac{\mathbb{Z}_3[x]}{\langle x^2+x+1 \rangle} = \{0+J, 1+J, 2+J, x+J, 2x+J, x+1+J, x+2+J, 2x+1+J, 2x+2+J\}$$

where $J = \langle x^2+x+1 \rangle$. There are $9 = 3^2$ elements in this ring. However, it is not a field since $x^2+x+1 = (x+2)^2$. As an example of multiplication in this ring consider

$$(2x+1+J)(x+1+J) = 2x^2+3x+1+J = 2x^2+1+J = 2(x^2+x+1) - 2x - 1 + J = -2x-1+J = x+2+J$$

$x+2$ is the remainder when $2x^2+1$ is divided by x^2+x+1 with coefficients in $\mathbb{Z}_3$.

Lemma 57 *If F is a finite field then $|F| = p^k$ for some prime p and $k \in \mathbb{N}$.*

Theorem 58 *Suppose $r(x) \in \mathbb{Z}_p[x]$ where p is prime. If $r(x)$ is irreducible then $\frac{\mathbb{Z}_p[x]}{\langle r(x) \rangle}$ is a field with $p^{\deg r}$ elements.*

Theorem 59 *Suppose that p is prime, then there exists irreducible polynomials of every (non-zero) degree in $\mathbb{Z}_p[x]$.*

(21.4.2) Irreducible Polynomials In $\mathbb{Q}[x]$

Lemma 60 *Suppose $a, b \in \mathbb{Z}$ and are coprime. If $a \mid b^k n$ where $n, k \in \mathbb{Z}$ ($k \geqslant 0$) then $a \mid n$.*

Theorem 61 (The Rational Roots Test) *Suppose that $f(x) \in \mathbb{Z}[x]$ is a polynomial of degree n, say*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

If $\alpha = \frac{r}{s}$ is a root of f and r and s are coprime then $r \mid a_0$ and $s \mid a_n$.

Proof. Since $f(\alpha) = 0$,

$$\begin{aligned} a_0 + a_1 \frac{r}{s} + \cdots + a_n \left(\frac{r}{s}\right)^n &= 0 \\ a_0 s^n + a_1 r s^{n-1} + \cdots + a_n r^n &= 0 \qquad (62) \\ a_1 r s^{n-1} + \cdots + a_n r^n &= -a_0 s^n \end{aligned}$$

Since r divides the left hand side and r and s are coprime Lemma 60 means that r must divide a_0. Also from equation (62),

$$a_0 s^n + a_1 r s^{n-1} + \cdots + a_{n-1} s r^{n-2} = a_n r^n$$

Clearly s divides the left hand side, so since r and s are coprime Lemma 60 means that s must divide a_n. □

For example, if $x^7 + 3x + 1$ has any rational roots then they must be ± 1. Also, consider $\alpha = \sqrt[5]{80}$, then let $p(x) = x^5 - 80$ which has α as a root. Now, the only possible rational roots are ± 1, ± 2, ± 4, ± 5, ± 8, ± 10 ± 16, ± 20, and ± 40. As none of these are roots α must be irrational.

Lemma 63 (Gauss' Lemma) *If $f(x) \in \mathbb{Z}[x]$ then $f(x)$ can be factored as a product of two polynomials in $\mathbb{Q}[x]$ of degree less than $\deg f$ if and only if such a factorisation exists in $\mathbb{Z}[x]$.*

Theorem 64 (Eisenstein's Criterion) *Let $p \in \mathbb{Z}$ be prime and suppose $f(x) = a_0 + \cdots + a_n x^n$ is in $\mathbb{Z}[x]$. If*

1. *$a_n \not\equiv 0 \mod p$.*
2. *$a_i \equiv 0 \mod p$ for all $0 \leqslant i \leqslant n-1$.*
3. *$a_0 \not\equiv 0 \mod p^2$.*

then f is irreducible in $\mathbb{Q}[x]$.

Corollary 65 *If p is prime then $\Phi_p(x) = \dfrac{x^p - 1}{x - 1}$ is irreducible in $\mathbb{Q}[x]$.*

Proof. Consider $\Phi_p(x+1)$ then

$$\begin{aligned}\Phi_p(x+1) &= \frac{(x+1)^p - 1}{x} \\ &= x^{p-1} + \binom{p}{p-1} x^{p-2} + \cdots + \binom{p}{1}\end{aligned}$$

All the binomial coefficients are divisible by p and $\binom{p}{1} = 1$ which is not divisible by p^2. Hence by Eisenstein's criterion the result is shown. □

Algebraic Numbers

Definition 66 *Let E and F be fields. If $F \subset E$ then E is an extension field of F.*

Definition 67 *Let E be an extension field of F. If $\alpha \in E$ then α is algebraic over F if there exists $f(x) \in F[x]$ such that $\phi_\alpha(f(x)) = 0$. Otherwise α is transcendental.*

Theorem 68 *Let E be an extension field of F and ϕ_α be the evaluation homomorphism. ϕ_α is a monomorphism if and only if α is transcendental.*

Proof. If α is transcendental then it is not the solution of any polynomial other than $f(x) = 0$ so $\ker \phi_\alpha = \{0\}$ meaning that ϕ_α is a monomorphism.

Conversely, if ϕ_α is a monomorphism then $\ker \phi_\alpha = \{0\}$ so α is not the solution to any polynomial (other than $f(x) = 0$) and hence α is transcendental. □

Now, $\operatorname{Im} \phi_\alpha$ is a subring of E and so when α is transcendental E has a subring that is isomorphic to $F[x]$. Moreover, since $F[x]$ is an integral domain Theorem 28 shows that E has a subfield isomorphic to the field of fractions of $F[x]$.

Definition 69 *A polynomial of degree n in $F[x]$ is called monic if $a_n = 0$.*

Observe that if F is a field then for any polynomial $p(x) \in F[x]$ a monic polynomial is $m(x) = a_n^{-1}p(x)$. The two ideals $p(x)F[x]$ and $m(x)F[x]$ are in fact the same since

$$p(x)F[x] \ni q(x) = p(x)r(x) = \left(a_n^{-1}p(x)\right)(a_n r(x)) = q(x) \in m(x)F[x] \tag{70}$$

note that $a_n r(x) \in F[x]$ because $a_n \in F[x]$ and $r(x) \in F[x]$.

Theorem 71 *Let E be an extension field of F and let α be algebraic over F. There exists a unique monic polynomial of least degree, $m(x)$ say, such that $m(\alpha) = 0$. Furthermore $m(x)$ is irreducible and divides any polynomial satisfying $p(\alpha) = 0$.*

Proof. Let $K = \ker \phi_\alpha$ then K is an ideal in $F[x]$. By Lemma 53 $F[x]$ is a principal ideal domain, and so a polynomial of least degree can be chosen such that $K = m(x)F[x]$, and by equation (70) this polynomial can be monic.

Now, if $m(x)$ was reducible then $m(x) = h(x)f(x)$, but $m(\alpha) = 0$ would then give $h(\alpha) = 0$ or $f(\alpha) = 0$, contradicting the minimality of $m(x)$. □

In this case $m(x)$ is referred to as $m_\alpha(x)$, the minimal polynomial of α over F. Also,

$$F(\alpha) = \{\phi_\alpha(f) \mid f \in F[x]\} = \{f(\alpha) \mid f \in F[x]\}$$

is the image of ϕ_α in E.

Theorem 72 *Whenever α is algebraic over F, $\dfrac{F[x]}{\langle m_\alpha(x)\rangle} \cong F(\alpha)$.*

Proof. By Theorem 71 $\ker \phi_\alpha$ is a maximal ideal of $F[x]$ and is equal to $\langle m_\alpha(x)\rangle$. By Theorem 42 the factor ring is a fild which is isomorphic to $F(\alpha)$ by Theorem 38. □

Theorem 73 *Suppose that E is an extension field of F and $\alpha \in E$ is algebraic. If $\deg m_\alpha = m$ that $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is a basis for $F(\alpha)$ over F.*

Proof. The elements of $\frac{F[x]}{m_\alpha(x)F[x]}$ are all of the form $r(x) + m_\alpha(x)F[x]$ where $\deg r < \deg m_\alpha$, and every such polynomial is present. Hence

$$\left\{1 + m_\alpha(x)F[x], x + m_\alpha(x)F[x], \ldots, x^{m-1} + m_\alpha(x)F[x]\right\}$$

where $\deg m_\alpha = m$, is a basis for $\frac{F[x]}{m_\alpha(x)F[x]}$. Define now

$$\psi_\alpha \colon \frac{F[x]}{m_\alpha(x)F[x]} \to F(\alpha) \quad \text{by} \quad \psi_\alpha \colon r(x) + m_\alpha(x)F[x] \mapsto r(\alpha)$$

This is an isomorphism, which shows $\left\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\right\}$ to be a basis for $F(\alpha)$. □

Definition 74 *The degree of the extension $F(\alpha)$ of F is defined as the dimension of $F(\alpha)$ as a vector space over F.*

It is immediately clear this is the same as the degree of $m_\alpha(x)$.

(21.5) Euclidean Domains

Definition 75 *An integral domain R is a Euclidean Domain if there exists a function $v \colon R \setminus \{0\} \to \mathbb{N}$ such that*

1. *If $r, s \in R$ and r divides s then $\nu(r) \leqslant \nu(s)$.*
2. *If $s, t \in R$ then there exists $q, r \in R$ such that $t = sq + r$ with $r = 0$ or $\nu(r) < \nu(s)$.*

ν is called a Euclidean valuation on R.

Examples of Euclidean domains include $\mathbb{Z}$ with $\nu(x) = |x|$ or $F[x]$ with $\nu(x) = \deg x$.

Theorem 76 *Every Euclidean domain is a principal ideal domain.*

Proof. Let R be a Euclidean domain and $J \trianglelefteq R$. If $J = \{0\}$ then $J = 0R$, so assume $J \neq \{0\}$ so that $\exists s \in J \setminus \{0\}$ such that $\nu(s)$ is minimal. Since s is in an ideal, $sR \subseteq J$.

Let $t \in J$ then from Definition 75 $t = sq + r$ where $r = 0$ or $\nu(r) < \nu(s)$. Now, both t and s are in J and since J is an ideal, $t - sq = r \in J$. In order not to contradict the minimality of $\nu(s)$ it must be the case that $r = 0$. Therefore $t = sq \in sR$ so that $J \subseteq sR$. □

Lemma 77 *The units*[†] *of a Euclidean domain R are precisely the elements $a \in R \setminus \{0\}$ with $\nu(q) = \nu(1)$.*

Proof. Suppose a is invertible, then $aa^{-1} = 1$ so a divides 1 hence $\nu(a) \leqslant \nu(1)$. Also, $1a = a$ so 1 divides a and hence $\nu(1) \leqslant \nu(a)$.

Conversely, suppose that $\nu(a) = \nu(1)$. Now, $1 = aq + r$ but $\nu(r) < \nu(a) = \nu(1)$ is impossible, therefore $r = 0$ so that q is the inverse of a. □

Theorem 78 *The Gaussian integers, $J = J(i) = \{a + ib \mid a, b \in \mathbb{Z}\}$ is a Euclidean domain.*

Proof. Firstly, J is a subring of $\mathbb{C}$ and since $\mathbb{C}$ is a field, J is an integral domain. Define now

$$\nu \colon J \to \mathbb{N} \quad \text{by} \quad \nu \colon a + ib \mapsto a^2 + b^2$$

$\nu(xy) = \nu(x)\nu(y)$ since

$$\begin{aligned}
\nu(xy) &= \nu(ac - bd + i(ad + bc)) \\
&= a^2c^2 + b^2d^2 - 2abcd + a^2d^2 + b^2c^2 + 2abcd \\
&= a^2(c^2 + d^2) + b^2(d^2 + c^2) \\
&= (a^2 + b^2)(c^2 + d^2) \\
&= \nu(x)\nu(y)
\end{aligned}$$

Since $\nu(x)$ and $\nu(y)$ must be at least 1, $\nu(x) \leqslant \nu(x)\nu(y) = \nu(xy)$, so property 1 of Definition 75 is shown. Let $s, t \in J$ then seek $q, r \in J$ such that $t = sq + r$. Put $q' = \frac{t}{s}$ which is in $\mathbb{C}$ but not necessarily J, however, $\exists q$ such that $|q' - q| \leqslant \frac{\sqrt{2}}{2} < 1$. Then r is then chosen so that $r = t - sq$. Now,

$$\nu(r) = |r|^2 = |t - qs|^2 = |s|^2 \left| \frac{t}{s} - q \right|^2 = |s|^2 |q' - q|^2 < |s|^2 = \nu(s)$$

Hence property 2 of Definition 75 is shown and the proof is complete. □

From Lemma 77 the invertible elements of J have $\nu(x) = \nu(1) = 1$. These are $(\pm 1, 0)$ and $(0, \pm 1)$.

Lemma 79 *Let R be an integral domain. If $J = sR + tR$ is an ideal of R and $t = sq + r$ then $J = sR + rR$.*

[†] The invertible elements of a ring may also be called 'units'.

Proof. $r = t - sq$ therefore $r \in J$ so $rR \subseteq J$ and so certainly $sR + rR \subseteq J$.
On the other hand $t = sq + r$ so $sR + rR \supseteq tR \supseteq tR + sR = J$. □

This result allows the division algorithm (Theorem 50) to be used to simplify expressions for ideals.

Example 80 *Simplify*

1. $J = (x^3 + x^2 + 7)\mathbb{Q}[x] + (x^2 + 1)\mathbb{Q}[x]$.
2. $K = (3 + 12i)J + (3 + 5i)J$ *where* J *is the Gaussian integers.*

Proof. Solution

1.

$$\begin{aligned} x^3 + x^2 + 7 &= (x^2 + 1)(x + 1) + (-x + 6) && \text{so } J = (x^2 + 1)\mathbb{Q}[x] + (-x + 6)\mathbb{Q}[x] \\ (x^2 + 1) &= (-x + 6)(x + 6) - 35 && \text{so } J = (-x + 6)\mathbb{Q}[x] + 35\mathbb{Q}[x] \\ x - 6 &= 35\left(\frac{x - 6}{35}\right) + 0 && \text{so } J = 35\mathbb{Q}[x] = \mathbb{Q}[x] \end{aligned}$$

2. For the purposes of dividing complex numbers it is advised to use a scientific calculator.

$$\begin{aligned} 3 + 12i &= (3 + 5i)(2 + i) + (2 - i) && \text{so } K = (3 + 5i)J + (2 - i)J \\ 3 + 5i &= (2 - i)(3 + 6i) - i && \text{so } K = (2 - i)J - iJ \\ 2 - i &= i(1 + 2i) && \text{so } K = iJ = J \end{aligned}$$

□