University of
Cambridge

Mathematics Tripos

Part IB

Groups, Rings and Modules

Lent, 2017

Lectures by
O. Randal-Williams

Notes by
Qiangru Kuang

Contents

1 Groups

1.1 Definitions

Definition (Group)**.** A *group* is a triple $(G, \cdot, e)$ of a set G, a function $- \cdot - : G \times G \to G$ and $e \in G$ such that

- associativity: for all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
- identity: for all $a \in G$, $a \cdot e = a = e \cdot a$,
- inverse: for all $a \in G$, there exists $\alpha^{-1} \in G$ such that $a \cdot a^{-1} = e = a^{-1} \cdot a$.

Definition (Subgroup)**.** If $(G, \cdot, e)$ is a group, $H \subseteq G$ is a *subgroup* if

- $e \in H$,
- for all $a, b \in H$, $a \cdot b \in H$.

This makes $(H, \cdot, e)$ into a group. Write $H \leq G$.

Lemma 1.1. *If $H \subseteq G$ is non-empty and for all $a, b \in H$, $a \cdot b^{-1} \in H$ then $H \leq G$.*

Example.

1. Additive groups: $(\mathbb{N}, +, 0)$, $(\mathbb{R}, +, 0)$, $(\mathbb{C}, +, 0)$.
2. Groups of symmetries: S_n, D_{2n}, $\mathrm{GL}_n(\mathbb{R})$. They have subgroups $A_n \leq S_n$, $C_n \leq D_{2n}$, $\mathrm{SL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{R})$.
3. An group G is *abelian* is a group such that $a \cdot b = b \cdot a$ for all $a, b \in G$.

If $H \leq G$, $g \in G$, we define the *left H-coset* of G to be

$$gH = \{gh : h \in H\}.$$

As we have seen in IA Groups, the H-cosets form a partition of G and are in bijection with each other via

$$\begin{aligned} H &\leftrightarrow gH \\ h &\mapsto gh \\ g^{-1}h &\mapsfrom h \end{aligned}$$

We write G/H for the set of left cosets.

Theorem 1.2 (Lagrange)**.** *If G is a finite group and $H \leq G$ then*

$$|G| = |H| \cdot |G/H|.$$

We call $|G/H|$ the *index* of H in G.

Definition (Order)**.** Given $g \in G$, the *order* of g is the smallest n such that $g^n = e$. We write $n = o(g) = |g|$. If no such n exists then g has infinite order.

Recall that if $g^m = e$ then $|g| \mid m$.

Lemma 1.3. *If G is finite and $g \in G$ then $|g| \mid |G|$.*

Proof. The set
$$\langle g \rangle = \{e, g, \dots, g^{|g|-1}\}$$
is a subgroup of G. The result follows from Lagrange. □

1.2 Normal subgroups, Quotients and Homomorphisms

Recall that $gH = g'H$ if and only if $g^{-1}g' \in H$. In particular, if $h \in H$ then $ghH = gH$.

Given a subgroup $H \leq G$, we want to define a group structure on its cosets. Argurably the most natural candidate for the group operation would be

$$\begin{aligned} - \cdot - : G/H \times G/H &\to G/H \\ (gH, g'H) &\mapsto gg'H \end{aligned}$$

But is this well-defined? Suppose $g'H = g'hH$, then

$$(gH) \cdot (g'hH) = gg'hH = gg'H$$

so it is well-defined in the second coordinate. Suppose $gH = ghH$, then

$$(ghH) \cdot (g'H) = ghg'H \stackrel{?}{=} gg'H$$

where the last step holds if and only if $(g')^{-1}hg' \in H$ for all $h \in H$, $g' \in G$. Thus we need this true to define a group structure on the cosets. This motivates us to define

Definition (Normal subgroup)**.** A subgroup $H \leq G$ is *normal* if for all $h \in H$, $g \in G$, $g^{-1}hg \in H$. Write $H \trianglelefteq G$.

Definition (Quotient group)**.** If $H \trianglelefteq G$, then G/H equipped with the product

$$\begin{aligned} G/H \times G/H &\to G/H \\ (gH, g'H) &\mapsto gg'H \end{aligned}$$

and identity eH is a group. This is the *quotient group* of G by H.

Now we have defined and seen quite a few groups. We are interested not in the internal structure of groups but how they relate to each other. This motivates to define morphisms between groups:

> **Definition** (Homomorphism)**.** If $(G, \cdot, e_G)$ and $(H, *, e_H)$ are groups, a function $\varphi : G \to H$ is a *homomorphism* if for all $g, h \in G$,
>
> $$\varphi(g \cdot g') = \varphi(g) * \varphi(g').$$

This implies that $\varphi(e_G) = e_H$ and $\varphi(g^{-1}) = \varphi(g)^{-1}$. We define

$$\begin{aligned} \ker\varphi &= \{g \in G : \varphi(g) = e_H\}, \\ \operatorname{Im}\varphi &= \{\varphi(g) : g \in G\}. \end{aligned}$$

> **Lemma 1.4.**
>
> - $\ker\varphi \trianglelefteq G$,
> - $\operatorname{Im}\varphi \leq H$.

Proof. Easy. $\square$

> **Definition** (Isomorphism)**.** A homomorphism φ is an *isomorphism* if it is a bijection. Say G and H are *isomorphic* if there exists some isomorphism $\varphi : G \to H$. Write $G \cong H$.

Exercise. If φ is an isomorphism then the inverse $\varphi^{-1} : H \to G$ is also an isomorphism.

> **Theorem 1.5** (1st Isomorphism Theorem)**.** *Let $\varphi : G \to H$ be a homomorphism. Then* $\ker \trianglelefteq\leq G$, $\operatorname{Im}\varphi \leq G$ *and*
>
> $$G/\ker\varphi \cong \operatorname{Im}\varphi.$$

Proof. We have done the first part. For the second part, define

$$\begin{aligned} \theta : G/\ker\varphi &\to \operatorname{Im}\varphi \\ g\ker\varphi &\mapsto \varphi(g) \end{aligned}$$

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, two heads] & H \\ G/\ker\varphi \arrow[ur, dashed, "\theta"'] & \end{tikzcd}$$

Check this is well-defined: if $g\ker\varphi = g'\ker\varphi$ then $g^{-1}g' \in \ker\varphi$ so $e_H = \varphi(g^{-1}g') = \varphi(g)^{-1}\varphi(g')$, $\varphi(g) = \varphi(g')$ and $\theta(g\ker\varphi) = \theta(g'\ker\varphi)$.

θ is a homomorphism:

$$\theta(g\ker\varphi \cdot g'\ker\varphi) = \theta(gg'\ker\varphi) = \varphi(gg') = \varphi(g)\varphi(g') = \theta(g\ker\varphi)\theta(g\ker\varphi).$$

θ is surjective and finally to show it is injective, suppose $\theta(g\ker\varphi) = e_H$. Then $g \in \ker\varphi$ so $g\ker\varphi = e\ker\varphi$. $\square$

Example. Consider

$$\begin{aligned}\varphi : \mathbb{C} &\to \mathbb{C} \setminus \{0\}\\ z &\mapsto e^z\end{aligned}$$

$e^{z+w} = e^z \cdot e^w$ so $\varphi : (\mathbb{C}, +, 0) \to (\mathbb{C} \setminus \{0\}, \times, 1)$ is a homomorphism. φ is surjective (as log is a left inverse).

$$\ker \varphi = \{z \in \mathbb{C} : e^z = 1\} = \{2\pi i k : k \in \mathbb{Z}\} = 2\pi i \mathbb{Z}$$

so by 1st Isomorphism Theorem

$$\mathbb{C}/2\pi i\mathbb{Z} \cong \mathbb{C} \setminus \{0\}.$$

Theorem 1.6 (2nd Isomorphism Theorem)**.** *Let $H \leq G$ and $K \trianglelefteq G$. Then*

$$\begin{aligned}HK &\leq G\\ H \cap K &\trianglelefteq H\\ HK/K &\cong H/(H \cap K)\end{aligned}$$

Proof. Let $h, h' \in H$, $k, k' \in K$. Then

$$(h'k')(hk)^{-1} = h'k'k^{-1}h^{-1} = (h'h^{-1})(hk'k^{-1}h^{-1}) \in HK.$$

Consider

$$\begin{aligned}\varphi : H &\to G/K\\ h &\mapsto hK\end{aligned}$$

This is the composition $H \overset{\iota}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} G/K$ so a homomorphism. Since

$$\begin{aligned}\ker \varphi &= \{hK : hK = eK\} = H \cap K \trianglelefteq H\\ \operatorname{Im} \varphi &= \{gK : gK = hK \text{ for some } h \in H\} = HK/K\end{aligned}$$

so by 1st Isomorphism Theorem

$$H/(H \cap K) \cong HK/K.$$

□

As a corollary we have

Theorem 1.7 (Subgroup correspondence)**.** *Let $K \trianglelefteq G$. There is a bijection between*

$$\begin{aligned}\{\textit{subgroups of } G/K\} &\leftrightarrow \{\textit{subgroups of } G \textit{ containing } K\}\\ H &\mapsto \{g \in G : gK \in H\}\\ L/K &\leftarrow\!\shortmid K \trianglelefteq L \leq G\end{aligned}$$

Moreover, the same map gives a bijection between

$$\{\textit{normal subgroups of } G/K\} \leftrightarrow \{\textit{normal subgroups of } G \textit{ containing } K\}.$$

Theorem 1.8 (3rd Isomorphism Theorem)**.** *Let $K \leq L \leq G$ be normal subgroups. Then*

$$\frac{G/K}{L/K} \cong G/L.$$

Proof. Consider

$$\begin{aligned} \varphi : G/K &\to G/L \\ gK &\mapsto gL \end{aligned}$$

Check it is well-defined: if $gK = g'K$, $g^{-1}g' \in K \subseteq L$ so $gL = g'L$. φ is clearly surjective and has kernel

$$\ker \varphi = \{gK \in G/K : gL = eL\} = L/K$$

so by 1st Isomorphism Theorem

$$\frac{G/K}{L/K} \cong G/L.$$

□

Definition (Simple group)**.** A group G is *simple* if its only normal subgroups are $\{e\}$ and G.

Lemma 1.9. *An abelian group is simple if and only if it is isomorphic to C_p for some prime p.*

Proof. In an abelian group every subgroup is normal. Let $g \in G$ be non-trivial. Then

$$\langle g \rangle = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\} \trianglelefteq G.$$

If G is simple, this must be the whole group so G is cyclic. If G is infinite, it is isomorphic to $\mathbb{Z}$ which is not simple as $2\mathbb{Z} \trianglelefteq G$. Therefore $G \cong C_n$ for some n. If $n = ab$, $a, b \in \mathbb{N}$, $a, b \neq 1$ then $\langle g^a \rangle \trianglelefteq G$. Absurd. Thus n is a prime.

For the other directions, note that C_p is simple for prime p by Lagrange. □

Theorem 1.10. *Let G be a finite group. Then there is a chain of subgroups*

$$G = H_0 \geq H_1 \geq H_2 \geq \dots \geq H_s = \{e\}$$

such that $H_{n+1} \trianglelefteq H_n$ and H_n/H_{n+1} is simple for all n.

Proof. Let H_1 be a normal subgroup of $H_0 = G$ of maximal order. If H_0/H_1 is not simple, there would be a proper normal subgroup $X \trianglelefteq H_1/H_2$. This corresponds to a normal subgroup of H_0, Y, which strictly contains H_1. Absurd. Thus H_0/H_1 is simple.

Choose H_2 to be the maximal normal subgroup of H_1 and continue. As H_{n+1} is a proper subgroup of H_n, $|H_{n+1}| < |H_n|$ so this process terminates after finitely many steps. □

1.3 Actions & Permutations

Part of the reason we study groups is that they have interesting internal structures. However, more importantly, groups are interesting because many transformations of an object can be described by a group. This is formalised by the concept of group action in this section.

The *symmetric group* S_n is the set of permutations of $\{1, \dots, n\}$. Every permutation is a product of transpositions. A permutation is *even* if it is a product of evenly-many transpositions and *odd* otherwise.

The *sign* of a permutation is a homomorphism

$$\begin{aligned} \operatorname{sgn} : S_n &\to \{\pm 1\} \\ \sigma &\mapsto \begin{cases} 1 & \sigma \text{ is even} \\ -1 & \sigma \text{ is odd} \end{cases} \end{aligned}$$

The kernel of sgn is the *alternating group* $A_n \trianglelefteq S_n$ of index 2 for $n \geq 2$.

For any set X, we let $\mathrm{Sym}(X)$ denote the set of all permutations of X, with composition as the group operation.

Here is a definition that is included in the syllabus but seems to be never used anywhere:

Definition. A group G is a *permutation group of degree n* if

$$G \leq \mathrm{Sym}(X)$$

with $|X| = n$.

Example.

1. S_n is a permutation group of order n, so is A_n.
2. D_{2n} acts on the n vertices of a regular n-gon, so

$$D_{2n} \leq S(\{n \text{ vertices}\}).$$

Definition (Group action)**.** An *action* of a group $(G, \cdot, e)$ on a set X is a function $- * - : G \times X \to X$ such that

1. For all $g, h \in G$, $x \in X$,

$$g * (h * x) = (gh) * x.$$

2. For all $x \in X$,

$$e * x = x.$$

Lemma 1.11. *Giving an action of G on X is the same as giving a homomorphism $\varphi : G \to \mathrm{Sym}(X)$.*

Proof.

- $\Rightarrow$: Let $- * -$ be an action. For all $g \in G$, let

$$\begin{aligned} \varphi : X &\to X \\ x &\mapsto g * x \end{aligned}$$

This satisfies

$$\varphi(gh)(x) = (gh) * x = g * (h * x) = \varphi(g)(\varphi(h)(x)) = (\varphi(g) \circ \varphi(h))(x)$$

so $\varphi(gh) = \varphi(g) \circ \varphi(h)$.

In addition $\varphi(e)(x) = e * x = x = \mathrm{id}_X(x)$ so $\varphi(e) = \mathrm{id}\, X$. Now we note that

$$\mathrm{id}_X = \varphi(e) = \varphi(gg^{-1}) = \varphi(g) \circ \varphi(g^{-1})$$

so $\varphi(g^{-1})$ is inverse to $\varphi(g)$. In particular $\varphi(g)$ is a bijection.

- $\Leftarrow$: Let $\varphi : G \to \mathrm{Sym}(X)$ be a homomorphism. Define

$$\begin{aligned} - * - : G \times X &\to X \\ (g, x) &\mapsto \varphi(g)(x) \end{aligned}$$

Verify that

$$\begin{aligned} g * (h * x) &= \varphi(g)(\varphi(h)(x)) = (\varphi(g) \circ \varphi(h))(x) = \varphi(gh)(x) = (gh) * x \\ e * x &= \varphi(e)(x) = \mathrm{id}_X(x) = x \end{aligned}$$

□

Given a homomorphism $\varphi : G \to \mathrm{Sym}(X)$ induced by an action, define $G^X = \mathrm{Im}\,\varphi, G_X = \ker \varphi$. Then by 1st Isomorphism Theorem $G_X \trianglelefteq G, G/G_X \cong G^X$.

If $G_X = \{e\}$, i.e. φ is injective then we say φ is a *permutation representation of* G. It follows that $G \cong G^X \leq \mathrm{Sym}(X)$.

Example.

1. Let G be the symmetries of a cube. Then G acts on the set X of diagonals. $|X| = 4$ and $\varphi : G \to \mathrm{Sym}(X)$ is surjective so $G^X = \mathrm{Sym}(X) \cong S_4$. $G_X = \{\mathrm{id}, \text{antipodal map}\}$ so by Lagrange

$$|G| = |G_X| \cdot |G^X| = 48.$$

2. For any group G, left multiplication is a homomorphism:

$$\begin{aligned} \varphi : G &\to \mathrm{Sym}\, G \\ g &\mapsto g \cdot - \end{aligned}$$

$G_X = \{g \in G : gh = h \text{ for all } G\} = \{e\}$ so φ is a permutation representation. This is

> **Theorem 1.12** (Cayley)**.** *Every group is isomorphic to a subgroup of a symmetric group.*

3. If G is a group and $H \leq G$, we have

$$\begin{aligned} \varphi : G &\to \mathrm{Sym}(G/H) \\ g &\mapsto g \cdot - \end{aligned}$$

$G_X = \{g \in G : gaH = aH \text{ for all } aH\} = \bigcap_{a\in G} aHa^{-1}$. This is the largest subgroup of H which is normal in G.

Theorem 1.13. *Let G be a finite group and $H \leq G$ with index n. Then there is a $K \trianglelefteq G, K \leq H$ such that G/K is isomorphic to a subgroup of S_n. In particular*

$$\begin{aligned} |G/K| &\mid n! \\ n &\mid |G/K| \end{aligned}$$

Proof. Let $K = G_X$ for the action of G on $X = G/H$. Then

$$G/G_X \cong G^X \leq \mathrm{Sym}(X) \cong S_n.$$

□

Theorem 1.14. *Let G be a non-abelian simple group and $H \leq G$ is a subgroup of index $n > 1$. Then G is isomorphic to a subgroup of A_n for some $n \geq 5$.*

Proof. Let G act on G/H, giving $\varphi : G \to \mathrm{Sym}(G/H)$. Then $\ker\varphi \trianglelefteq G$. As G is simple, $\ker\varphi = \{e\}$ or G. But $\ker\varphi = \bigcap_{g\in G} g^{-1}Hg \leq H$, a proper subgroup of G so $\ker\varphi = \{e\}$. By 1st Isomorphism Theorem

$$G = G/\{e\} \cong \mathrm{Im}\,\varphi = G^X \leq \mathrm{Sym}(G/H) \cong S_n.$$

Applying 2nd Isomorphism Theorem to $A_n \trianglelefteq S_n, G^X \leq S_n$, we get

$$G^X \cap A_n \trianglelefteq G^X,\ G^X/(G^X \cap A_n) \cong G^X A_n/A_n.$$

As $G^X \cong G$ is simple, $G^X \cap A_n$ is either trivial or G^X, i.e. $G^X \leq A_n$. But if $G^X \cap A_n = \{e\}$,

$$G^X \cong G^X A_n/A_n \leq S_n/A_n \cong C_2$$

which contradicts $G^X \cong G$ being non-abelian. Hence $G \cong G^X \leq A_n$.

$$1 \longrightarrow G \xrightarrow{\varphi} \mathrm{Sym}(G/H) \xrightarrow{\mathrm{sgn}} C_2$$

To see that we must have $n \geq 5$, observe that A_2, A_3 and A_4 have no non-abelian simple subgroup. □

Corollary 1.15. *If G is non-abelian simple, $H \leq G$ of index n, then*

$$|G| \mid \frac{n!}{2}.$$

Some futher definitions we have already met in IA Groups:

Definition (Orbit & Stabiliser)**.** If G acts on X, the *orbit* of $x \in X$ is

$$G \cdot x = \{g * x : g \in G\}.$$

and the *stabiliser* of x is

$$G_x = \{g \in G : g * x = x \forall x \in X\}.$$

Theorem 1.16 (Orbit-stabiliser)**.** *If G acts on X, for all $x \in X$ there is a bijection*

$$\begin{aligned} G \cdot x &\leftrightarrow G/G_x \\ g * x &\leftrightarrow gG_x \end{aligned}$$

1.4 Conjugacy class, Centraliser & Normaliser

In the previous section we use a group action of a group on itself, namely left multiplication, to study the structure of a group. In this section we study conjugation, another group action that gives much richer results.

There is an action of G on $X = G$ via $g * x = gxg^{-1}$, giving $\varphi : G \to \mathrm{Sym}(G)$.

Remark.

$$\varphi(g)(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = \varphi(g)(x)\varphi(g)(y)$$

so $\varphi(g)$ is a group homomorphism. In fact this is an automorphism and $\varphi(g) \in \mathrm{Inn}(G)$, which is the group of all automorphisms arising from conjugation.

Denote

$$\mathrm{Aut}(G) = \{\theta : G \to G : \theta \text{ is an isomorphism}\} \leq \mathrm{Sym}(G).$$

We have shown $\varphi : G \to \mathrm{Sym}(G)$ has image in $\mathrm{Aut}(G) \leq \mathrm{Sym}(G)$, i.e. $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.

Definition (Conjugacy class)**.** The *conjugacy clss* of $x \in G$ is

$$G \cdot x = \mathrm{Cl}_G(x) = \{gxg^{-1} : g \in G\}.$$

Definition (Centraliser)**.** The *centraliser* of $x \in G$ is

$$C_G(x) = \{g \in G : gx = xg\}.$$

Definition (Centre)**.** The *centre* of G is

$$Z(G) = \ker \varphi = \{g \in G : gxg^{-1} = x \forall x \in G\}.$$

Definition (Normaliser)**.** The *normaliser* of $H \leq G$ is

$$N_G(H) = \{g \in G : gHg^{-1} = H\}.$$

By Orbit-stabiliser, there is a bijection between

$$\mathrm{Cl}_G(x) \leftrightarrow G/C_G(x)$$

so if G is finite, $|\mathrm{Cl}_G(x)| = |G/C_G(x)|$ divides $|G|$.

Recall from IA Groups that in the permutation group S_n

1. every element can be written as a product of disjoint cycles,
2. permutations are conjugations if and only if they have the same cycle type.

We will use these knowledge to make our first (and the only one in this course) step towards classification of finite simple groups:

Theorem 1.17. *A_n is simple for $n \geq 5$.*

Proof. First claim A_n is generated by 3-cycles. Need to show that double transpositions are generated by 3-cycles. There are two cases:

- $(ab)(bc) = (abc)$,
- $(ab)(cd) = (acb)(acd)$.

Let $H \trianglelefteq A_n$. Suppose H contains a 3-cycle, say (abc). There exists $\sigma \in S_n$ such that

$$(abc) = \sigma^{-1}(123)\sigma.$$

If $\sigma \in A_n$ then $(123) \in H$. If $\sigma \notin A_n$, let $\sigma' = (45)\sigma \in A_n$. Here we use the fact that $n \geq 5$. Then

$$(abc) = \sigma'^{-1}(45)(123)(45)\sigma' = \sigma'^{-1}(123)\sigma'.$$

Hence H contains all 3-cycles and $H = A_n$. It then suffices to show any non-trivial $H \trianglelefteq A_n$ contains a 3-cycle. Split into different cases:

- Case I: H contains $\sigma = (12 \cdots r)\tau$, written in disjoint cycle notation, for some $r \geq 4$. Let $\pi = (123)$ and consider the *commutator*

  $$[\sigma, \pi] = \sigma^{-1}\pi^{-1}\sigma\pi = \tau^{-1}(r \cdots 21)(132)(12 \cdots r)\tau(123) = (23r)$$

  which is a 3-cycle in H.
- Case II: H contains $\sigma = (123)(456)\tau$. Let $\pi = (124)$ and consider

  $$[\sigma, \pi] = \tau^{-1}(132)(465)(142)(123)(456)\tau(124) = (12436)$$

  which is a 5-cycle in H. This reduces to Cases I.
- Case III: H contains $\sigma = (123)\tau$ and τ is a product of 2-cycles. Then $\sigma^2 = (132) \in H$.

- Case IV: H contains $\sigma = (12)(34)\tau$ where τ is a product of 2-cycles. Let $\pi = (123)$ and

$$u = [\sigma, \pi] = (12)(34)(132)(12)(34)(123) = (14)(23).$$

Not let $v = (125)$ where we used the fact $n \geq 5$ again. Then

$$[u, v] = (14)(23)(152)(14)(23)(125) = (12345) \in H$$

which is a 5-cycle.

□

1.5 Finite p-groups

A finite group G is a *p-group* if $|G| = p^n$ for some prime p.

Theorem 1.18. *If G is a finite p-group then $Z(G) \neq \{e\}$.*

Proof. The conjugacy classes partition G and $|\operatorname{Cl}(x)| = |G/C(x)|$ which divides $|G|$. Thus $|\operatorname{Cl}(x)|$ is a power of p. Class equation reads

$$|G| = |Z(G)| + \sum_{\text{other ccl's}} |\operatorname{Cl}(x)|$$

Reduce mod p, we get $|Z(G)| = 0 \mod p$. But $|Z(G)| \geq 1$ so $|Z(G)| \geq p$. □

Corollary 1.19. *A group of order p^n, $n > 1$ is never simple.*

Lemma 1.20. *For any group G, if $G/Z(G)$ is cyclic, G is abelian.*

Proof. Let $G/Z(G) = \langle gZ(G) \rangle$. Then every coset is of the form $g^r Z(G)$, $r \in \mathbb{Z}$. Thus every element of G is of the form $g^r z$ where $z \in Z(G)$. Then

$$g^r z g^{r'} z' = g^r g^{r'} z z' = g^{r+r'} z' z = g^{r'} z' g^r z$$

and hence G is abelian. □

Corollary 1.21. *If $|G| = p^2$, G is abelian.*

Proof. $Z(G) \neq \{e\}$ so $|Z(G)| = p$ or p^2. Suppose $|Z(G)| = p$, $|G/Z(G)| = p$ so $G/Z(G) \cong C_p$ so by the lemma G is abelian. Absurd. Thus $Z(G) = G$ and thus G is abelian. □

Theorem 1.22. *If $|G| = p^a$, G has a subgroup of order p^b for all $0 \leq b \leq a$.*

Proof. Induction on a. If $a = 1$ then done. Suppose $a > 1$. Then $Z(G) \neq \{e\}$. Let $x \in Z(G)$ be non-identity. Then x has order a power of p, say p^i. Then $z = x^{p^{i-1}}$ has order precisely p. Let $C = \langle z \rangle \trianglelefteq G$. Then G/C has order p^{a-1}. By induction hypothesis we can find a subgroup $H \leq G/C$ of order p^{b-1}. Then H must be of the form L/C for some $L \leq G$ and $|L| = p^b$. □

1.6 Finite abelian groups

Theorem 1.23. *If G is a finite abelian group then*

$$G \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_k}$$

with $d_{i+1} \mid d_i$ for all i.

Proof. This will be a corollary of the main result on modules by considering abelian groups as $\mathbb{Z}$-modules. □

Example. If $|G| = 8$ and G is abelian, G is isomorphic to one of C_8, $C_4 \times C_2$ and $C_2 \times C_2 \times C_2$.

Lemma 1.24 (Chinese Remainder Theorem)**.** *If n and m are coprime, then*

$$C_{nm} \cong C_n \times C_m.$$

Proof. Let $g \in C_n$ has order n, $h \in C_m$ has order m. Consider

$$x = (g, h) \in C_n \times C_m.$$

If $e = x^r = (g^r, h^r)$, then $n \mid r, m \mid r$ so $nm \mid r$. Thus $|x| = nm$. The group is cyclic. □

Corollary 1.25. *If G is a finite abelian group then*

$$G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_\ell}$$

with each n_i a power of prime.

Proof. If $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, a factorisation of distinct primes, the above lemma shows

$$C_d \cong C_{p_1^{a_1}} \times C_{p_2^{a_2}} \times \cdots \times C_{p_r^{a_r}}.$$

Apply this to the theorem above. □

1.7 Sylow's Theorem

Theorem 1.26 (Sylow's Theorem)**.** *Let $|G| = p^a \cdot m$ with $(p, m) = 1$ where p is a prime. Then*

1. *the set*
$$\mathrm{Syl}_p(G) = \{P \le G : |P| = p^a\}$$
of Sylow p-subgroups *is not empty,*

2. *all elements of* $\mathrm{Syl}_p(G)$ *are conjugates in G,*

3. *the number*
$$n_p = |\,\mathrm{Syl}_p(G)|$$

satisfies

$$n_p = 1 \mod p,\ n_p \mid |G|.$$

Lemma 1.27. *If $n_p = 1$ then the unqiue Sylow p-subgroup is normal in G.*

Proof. Let $P \le G$ be the Sylow p-subgroup and $g \in G$. As $gPg^{-1} \in \mathrm{Syl}_p(G)$, $gPg^{-1} = P$ so $P \trianglelefteq G$. $\square$

Example. Let G be group of order $96 = 2^5 \cdot 3$. Then

- $n_2 = 1 \mod 2$ and $n_2 \mid 3$ so $n_2 = 1$ or 3.
- $n_3 = 1 \mod 3$ and $n_3 \mid 32$ so $n_3 = 1, 4$ or 16.

G acts on the set $\mathrm{Syl}_p(G)$ by conjugation. The second part of Sylow's Theorem says that this action has precisely one orbit. The stabiliser of $P \in \mathrm{Syl}_p(G)$ is the normaliser $N_G(P) \le G$ of index $n_p = |\mathrm{Syl}_p(G)|$.

Corollary 1.28. *If G is non-abelian simple, then $|G| \mid \frac{(n_p)!}{2}$ and $n_p \ge 5$.*

Proof. $N_G(P)$ has index n_p so Theorem 1.14 to get the result. Alternatively, consider the conjugation action of G on $\mathrm{Syl}_p(G)$. $\square$

Example (Continued)**.** $|G| \nmid \frac{3!}{2}$ so G cannot be simple.

Example. Suppose G is a simple group of order $132 = 2^2 \cdot 3 \cdot 11$. We have $n_{11} = 1 \mod 11$ and $n_{11} \mid 12$. As G is simple we can't have $n_{11} = 1$ so $n_{11} = 12$. Each Sylow 11-subgroup has order 11 so isomorphic to C_{11}, and thus contains 10 elements of order 11. Such subgroups can only intersect in the identity so we have $12 \times 10 = 120$ elements of order 11.

In addition we know $n_3 = 1 \mod 3$ and $n_3 \mid 44$, so $n_3 = 4$ or 22. If $n_3 = 4$, we must have $|G| \mid \frac{4!}{2}$ by the previous corollary. Absurd. Thus $n_3 = 22$. As above, we get $22 \cdot (3-1) = 44$ elements of order 3. This gives $164 > 132$ elements. Absurd.

Thus there is no simple group of order 132.

Proof of Sylow's Theorem. Let $|G| = p^n \cdot m$.

1. Let
$$\Omega = \{X \subseteq G : |X| = p^n\}$$
and G act on Ω via
$$g * \{g_1, g_2, \dots, g_{p^n}\} = \{gg_1, gg_2, \dots, gg_{p^n}\}.$$
Let $\Sigma \subseteq \Omega$ be an orbit of the action. If $\{g_1, \dots, g_{p^n}\} \in \Sigma$, then
$$(gg_1^{-1}) * \{g_1, \dots, g_{p^n}\} \in \Sigma$$
so for all $g \in G$ there is an element of Σ containing g. Thus $|\Sigma| \ge \frac{|G|}{p^n} = m$.
If there is some orbit Σ with $|\Sigma| = m$, its stabiliser G_Σ has order p^n so we have a Sylow p-subgroup.

To show this happens, we must show it is *not* possible for every orbit to have size strictly bigger than m. By Orbit-stabiliser, for any Σ, $|\Sigma| \mid p^n \cdot m$ so if $|\Sigma| > m$ then $p \mid |\Sigma|$. If all orbits have size $> m$, p divides all of them so $p \mid |\Omega|$.

Let us calculate $|\Omega|$. We have

$$|\Omega| = \binom{p^n \cdot m}{p^n} = \prod_{j=0}^{p^n-1} \frac{p^n \cdot m - j}{p^n - j}.$$

The largest power of p dividing $p^n \cdot m - j$ is the same as the largest power of p dividing j, which is the same as the largest power of p dividing $p^n - j$. Thus $|\Omega|$ is *not* divisible by p.

2. Let us show something stronger: if $P \in \mathrm{Syl}_p(G)$ and Q is a p-subgroup then there is a $g \in G$ such that $g^{-1}Qg \le P$.

   Let Q act on G/P by
   $$q * gP = qgP.$$
   By Orbit-stabiliser, the size of an orbit divides $|Q| = p^b$ so it is either 1 or divisible by p.

   On the other hand $|G/P| = \frac{|G|}{|P|} = m$ which is not divisible by p. Thus there must be an orbit of size 1, say $\{gP\}$, i.e. for all $q \in Q$, $qgP = gP$ so $g^{-1}qg \in P$. $g^{-1}Qg \le P$.

3. By 2 G acts on $\mathrm{Syl}_p(G)$ by conjugation with one orbit. By Orbit-stabiliser $n_p = |\mathrm{Syl}_p(G)|$ divides $|G|$, which is the second part of the statement.

   Now we show $n_p = 1 \mod p$. Let $P \in \mathrm{Syl}_p(G)$ and let P act on $\mathrm{Syl}_p(G)$ by conjugation. By Orbit-stabiliser, the size of an orbit divides $|P| = p^n$ so each orbit either has size 1 or dividible by p. But $\{P\}$ is a singleton orbit. To show $n_p = 1 \mod p$ it suffices to show every other orbit has size > 1.

   Suppose that $\{Q\}$ is another singleton orbit. Then for all $p \in P$, $p^{-1}Qp = Q$ so $P \le N_G(Q)$. But we also have $Q \trianglelefteq N_G(Q)$ (since the normaliser is the largest subgroup of G in which Q is normal). Now P and Q are Sylow p-subgroups of $N_G(Q)$ so are conjugates in $N_G(Q)$. Thus there exists $g \in N_G(Q)$ such that $P = g^{-1}Qg = Q$. Thus $P = Q$ which contradicts Q being different from P.

□

Example. Let $G = \mathrm{GL}_n(\mathbb{F}_p)$. It has order

$$|G| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) = \prod_{i=0}^{n-1}(p^n-p^i) = p^{\frac{n(n-1)}{2}}\prod_{i=0}^{n-1}(p^{n-i}-1).$$

Let U be the set of upper triangular matrices with diagonal entries 1, which forms a subgroup of G. $|U| = p^{\frac{n(n-1)}{2}}$ so U is a Sylow p-subgroup.

Consider $\mathrm{GL}_2(\mathbb{F}_p)$. It has order $(p^2-1)(p^2-p) = p(p+1)(p-1)^2$. Let ℓ be an odd prime dividing $p-1$. Then $\ell \nmid p, \ell \nmid p+1$ so ℓ^2 is the largest power of ℓ dividing $|\mathrm{GL}_2(\mathbb{F}_p)|$.

Define the unit group

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{x \in \mathbb{Z}/p\mathbb{Z} : \exists y \in \mathbb{Z}/p\mathbb{Z}, xy = 1\} = \{x \in \mathbb{Z}/p\mathbb{Z} : x \neq 0\}$$

which is isomorphic to C_{p-1}. Thus it has a subgroup $C_\ell \leq C_{p-1}$, i.e. we can find $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $x^\ell = 1$.

Let

$$H = \left\{\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) : a, b \in (\mathbb{Z}/p\mathbb{Z})^\times, a^\ell = b^\ell = 1\right\} \cong C_\ell \times C_\ell \leq \mathrm{GL}_2(\mathbb{F}_p).$$

Then H is a Sylow ℓ-subgroup.

Example. Let

$$\mathrm{SL}_2(\mathbb{F}_p) = \ker(\det : \mathrm{GL}_2(\mathbb{F}_p) \to (\mathbb{Z}/p\mathbb{Z})^\times).$$

det is surjective as $\det\left(\begin{smallmatrix} \lambda & 0 \\ 0 & 1 \end{smallmatrix}\right) = \lambda$ so $\mathrm{SL}_2(\mathbb{F}_p) \trianglelefteq \mathrm{GL}_2(\mathbb{F}_p)$ has index $p-1$. Thus

$$|\mathrm{SL}_2(\mathbb{F}_p)| = (p-1)p(p+1).$$

Further define

$$\mathrm{PSL}_2(\mathbb{F}_p) = \mathrm{SL}_2(\mathbb{F}_p)/\{\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right)\}.$$

If $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{F}_p)$, then $\lambda^2 = 1$. As long as $p > 2$, there are two such λ's, ± 1 so

$$|\mathrm{PSL}_2(\mathbb{F}_p)| = \frac{(p-1)p(p+1)}{2}.$$

Let $(\mathbb{Z}/p\mathbb{Z})_\infty = \mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$. Then $\mathrm{PSL}_2(\mathbb{F}_p)$ acts on $(\mathbb{Z}/p\mathbb{Z})_\infty$ by the Möbius map

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} * z = \frac{az+b}{cz+d}.$$

Take $p = 5$ for example, this actions gives a homomorphism

$$\varphi : \mathrm{PSL}_2(\mathbb{F}_5) \to S_6.$$

$|\mathrm{PSL}_2(\mathbb{F}_5)| = 60$. Claim φ is injective.

Proof. Suppose $\frac{az+b}{cz+d} = z$ for all z. Set $z = 0$, $b = 0$. $z = \infty$, $c = 0$. $z = 1$, $a = d$. Thus

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in \mathrm{PSL}_2(\mathbb{F}_5).$$

□

Further claim $\operatorname{Im}\varphi \leq A_6$.

Proof. Consider

$$1 \longrightarrow \mathrm{PSL}_2(\mathbb{F}_5) \xrightarrow{\varphi} S_6 \xrightarrow{\mathrm{sgn}} C_2.$$

Need to show $\psi = \mathrm{sgn} \circ \varphi$ is trivial. We already know elements of odd order in $\mathrm{PSL}_2(\mathbb{F}_5)$ has be be sent to 1.

Note that $H = \left\{\left[\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & \lambda \\ -\lambda^{-1} & 0 \end{smallmatrix}\right]\right\}$ has order 4, so it is a Sylow 2-subgroup of $\mathrm{PSL}_2(\mathbb{F}_5)$. Any elemnt of order 2 or 4 is conjugate to an element in the group. We will show $\psi(H) = \{e\}$.

H is generated by $\left[\begin{smallmatrix} -2 & 0 \\ 0 & 2 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$. $\left[\begin{smallmatrix} -2 & 0 \\ 0 & 2 \end{smallmatrix}\right]$ acts on $(\mathbb{Z}/5\mathbb{Z})_\infty$ via $z \mapsto -z$. It is thus an even permutation. $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ acts via $z \mapsto -\frac{1}{z}$, which is also an even permutation. □

2 Rings

2.1 Definitions

Definition (Ring)**.** A *ring* is a quintuple $(R, +, \cdot, 0_R, 1_R)$ such that

- $(R, +, 0_R)$ is an abelian group,
- the operation $- \cdot - : R \times R \to R$ is associative and satisfies

$$1_R \cdot r = r = r \cdot 1_R$$

- $r \cdot (r_1 + r_2) = r \cdot r_1 + r \cdot r_2$ and $(r_1 + r_2) \cdot r = r_1 \cdot r + r_2 \cdot r$.

A ring is *commutative* if for all $a, b \in R$, $a \cdot b = b \cdot a$. We will only consider commutative rings in this course.

Definition (Subring)**.** If $(R, +, \cdot, 0_R, 1_R)$ is a ring and $S \subseteq R$, then it is a *subring* if $0_R, 1_R \in S$ and $+, \cdot$ make S into a ring. Write $S \leq R$.

Example.

1. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ with usual $0, 1, +$ and $\cdot$.
2. $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ is the subring of *Gaussian integers*.
3. $\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}b : a, b \in \mathbb{Q}\} \leq \mathbb{R}$.

Definition (Unit)**.** An element $r \in R$ is a *unit* if there exists $s \in R$ such that $s \cdot r = 1_R$.

Note that being a unit depends on the ambient ring: $2 \in \mathbb{Z}$ is not a unit but $2 \in \mathbb{Q}$ is.

If every $r \in R, r \neq 0_R$ is a unit, then R is a *field*.

Notation. If $x \in R$, write $-x \in R$ for the inverse of x in $(R, +, 0_R)$. Write $y - x = y + (-x)$.

Example. $0_R + 0_R = 0_R$ so

$$r \cdot 0_R = r \cdot (0_R + 0_R) = r \cdot 0_R + r \cdot 0_R$$

so $r \cdot 0_R = 0_R$. Thus if $R \neq \{0\}$, $0_R \neq 1_R$ since choosing $r \neq 0_R$, we would get $r = r \cdot 1_R = r \cdot 0_R = 0_R$. Absurd.

However, $(\{0\}, +, \cdot, 0, 0)$ is indeed a ring.

Example. If R and S are rings, then $R \times S$ is a ring via

$$\begin{aligned}
(r_1, s_1) + (r_2, s_2) &= (r_1 + r_2, s_1 + s_2) \\
(r_1, s_1) \cdot (r_2, s_2) &= (r_1 \cdot r_2, s_1 \cdot s_2) \\
1_{R \times S} &= (1_R, 1_S) \\
0_{R \times S} &= (0_R, 0_S)
\end{aligned}$$

Let $e_1 = (1_R, 0), e_2 = (0, 1_S)$, then[1]

$$\begin{aligned} e_1^2 &= e_1 \\ e_2^2 &= e_2 \\ e_1 + e_2 &= 1_{R\times S} \end{aligned}$$

Example (Polynomial)**.** Let R be a ring. A *polynomial* f over R is an expression

$$f = a_0 + a_1 X + \cdots a_n X^n$$

with $a_i \in R$ for all i. Note that X is just a symbol and the sum is formal. We will consider f and

$$a_0 + a_1 X + \cdots a_n X^n + 0_R \cdot X^{n+1}$$

as equal.

The *degree* of f is the largest n such that $a_n \neq 0$. If in addition $a_n = 1_R$, we say f is *monic*.

Write $R[X]$ for the set of all polynomials over R. If

$$g = b_0 + b_1 X + \cdots + b_m X^m,$$

we define

$$\begin{aligned} f + g &= \sum_{i=0}^{\max(f,g)} (a_i + b_i) X^i \\ f \cdot g &= \sum_i \sum_{j=0}^{i} a_j b_{i-j} X^i \end{aligned}$$

which make $R[X]$ a ring.

We consider R as a subring of $R[X]$, given by the polynomials of degree 0. In particular, $1_R \in R$ gives $1_{R[X]}$.

Example. Conisder $\mathbb{Z}/2\mathbb{Z}[X]$, $f = X + X^2 \neq 0$. We have

$$\begin{aligned} f(0) &= 0 + 0 = 0 \\ f(1) &= 1 + 1 = 0 \end{aligned}$$

This shows that a polynomial vanishing everywhere on a finite ring is not necessarily zero (but necessarily so for an infinite ring).

Example. Write $R[[X]]$ for the ring of *formal power series* with elements

$$f = a_0 + a_1 X + a_2 X^2 + \ldots$$

with the same addition and multiplication as above.

Example. The *Laurent polynomials* $R[X, X^{-1}]$ is the set of expressions

$$f = \sum_{i\in\mathbb{Z}} a_i X^i$$

such that only finitely many a_i's are non-zero.

[1] This is known as orthogonal idempotents.

Example. The ring of *Laurent series* are elements of the form

$$f = \sum_{i \in \mathbb{Z}} a_i X^i$$

with only finitely many $i < 0$ such that $a_i \neq 0$.

Example. If R is a ring and X is a set, the set R^X of all functions $f : X \to R$ is a ring via

$$\begin{aligned} (f+g)(x) &= f(x) + g(x) \\ (f \cdot g)(x) &= f(x) \cdot g(x) \\ (1_{R^X})(x) &= 1_R \\ (0_{R^X})(x) &= 0_R \end{aligned}$$

For example, we have the following chain

$$\mathbb{R}[X] = \{f : \mathbb{R} \to \mathbb{R} \text{ polynomial}\} < \{f : \mathbb{R} \to \mathbb{R} \text{ continuous}\} < \mathbb{R}^{\mathbb{R}}.$$

2.2 Homomorphism, Ideals and Isomorphisms

Definition (Homomorphism)**.** A function $\varphi : R \to S$ between rings is a *homomorphism* if

- $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$, i.e. $\varphi : (R, +, 0_R) \to (S, +, 0_S)$ is a group homomorphism,
- $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$,
- $\varphi(1_R) = 1_S$.

If in addition φ is a bijection, it is an *isomorphism.*

The *kernel* of $\varphi : R \to S$ is

$$\ker \varphi = \{r \in R : \varphi(r) = 0_S\}.$$

Lemma 2.1. *$\varphi : R \to S$ is injective if and only if $\ker \varphi = \{0_R\}$.*

Proof. $\varphi : (R, +, 0_R) \to (S, +, 0_S)$ is a group homomorphism and its kernel as group homomorphism is also $\ker \varphi$. $\square$

Definition (Ideal)**.** A subset $I \subseteq R$ is an *ideal* if

- I is a subgroup of $(R, +, 0_R)$,
- strong (multiplicative) closure: for all $x \in I, r \in R$, $x \cdot r \in I$.

Write $I \trianglelefteq R$.

We say $I \trianglelefteq R$ is *proper* if $I \neq R$.

Lemma 2.2. *If $\varphi : R \to S$ is a homomorphism then* $\ker \varphi \trianglelefteq R$.

Proof. The first axiom holds since φ is a group homomorphism. Let $x \in \ker \varphi, r \in R$, then

$$\varphi(r \cdot x) = \varphi(r) \cdot \varphi(x) = \varphi(r) \cdot 0_S = 0_S$$

so $r \cdot x \in \ker \varphi$. □

Example.

1. If $I \trianglelefteq R$ and $1_R \in I$, then for all $r \in R$, $r = r \cdot 1_R \in I$ so $I = R$.

   Equivalently, if I is a proper ideal then $1_R \notin I$. Consequenctly, proper ideals are never subrings.

2. This can be generalaised to units: if u is a unit in R with inverse $v \in R$, then if $u \in I$, so is $1_R = u \cdot v \in R$ so $I = R$.

   Equivalently, if I is a proper ideal then it contains no unit.

Example. If R is a field then $\{0\}$ and R are the only ideals.

Example. In the ring $\mathbb{Z}$, all ideals are of the form

$$n\mathbb{Z} = \{\dots, -2n, -n, 0, n, 2n, \dots\}.$$

Proof. $n\mathbb{Z}$ is certainly an ideal.

Let $I \trianglelefteq \mathbb{Z}$ be an ideal. Let $n \in I$ be the smallest positive element. Then $n\mathbb{Z} \subseteq I$. If this is not an equality, choose $m \in I \setminus n\mathbb{Z}$. By Euclidean algorithm, $m = nq + r$ with $0 \le r < n$. So $r = m - nq \in I$. But n is the smallest positive element in I, so $r = 0$. Thus $m \in n\mathbb{Z}$. □

Definition (Generated ideal)**.** For an element $a \in R$, write

$$(a) = \{a \cdot r : r \in R\} \trianglelefteq R,$$

the ideal *generated by* a.

More generally, for a set of elements $\{a_1, \dots, a_s\}$, write

$$(a_1, \dots, a_s) = \{a_1 r_1 + \dots + a_s r_s : r_1, \dots, r_s \in R\} \trianglelefteq R.$$

Definition (Principal ideal)**.** If $I \trianglelefteq R$ if of the form (a), we say it is a *principal ideal.*

Example.

1. $n\mathbb{Z} = (n) \trianglelefteq \mathbb{Z}$ is ideal. In fact we have shown that all ideals of $\mathbb{Z}$ are principal.
2. $(X) = \{\text{polynomials with constant coefficient } 0\} \trianglelefteq \mathbb{C}[X]$.

Proposition 2.3 (Quotient ring)**.** *Let $I \trianglelefteq R$ be an ideal. The* quotient ring *is the set of cosets $r + I$ (i.e. $(R, +, 0)/I$). Addition and multiplication are given by*

$$\begin{aligned}(r_1 + I) + (r_2 + I) &= r_1 + r_2 + I \\ (r_1 + I) \cdot (r_2 + I) &= r_1 r_2 + I\end{aligned}$$

with $0_{R/I} = 0_R + I, 1_{R/I} = 1_R + I$. This is a ring, and the quotient map

$$\begin{aligned}R &\to R/I \\ r &\mapsto r + I\end{aligned}$$

is a ring homomorphism.

Proof. We already knew $(R/I, +, 0_{R/I})$ is an abelian group and addition as described above is well-defined. Suppose

$$\begin{aligned}r_1 + I &= r_1' + I \\ r_2 + I &= r_2' + I\end{aligned}$$

then $r_1' - r_1 = a_1 \in I, r_2' - r_2 = a_2 \in I$. So

$$r_1' r_2' = (r_1 + a_1)(r_2 + a_2) = r_1 r_2 + \underbrace{r_1 a_2 + r_2 a_1 + a_1 a_2}_{\in I}.$$

Thus $r_1' r_2' + I = r_1 r_2 + I$. This shows multiplication is well-defined. The ring axioms for R/I then follow from those of R. ☐

Example.

1. $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ so $\mathbb{Z}/n\mathbb{Z}$ is a ring. It has elements

   $$0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}$$

   and addition and multiplication are modular arithmetic mod n.

2. $(X) \trianglelefteq \mathbb{C}[X]$ so $\mathbb{C}[X]/(X)$ is a ring. We have

   $$a_0 + \underbrace{a_1 X + a_2 X^2 + \dots + a_n X^n}_{\in (X)} + (X) = a_0 + X.$$

   If $a_0 + (X) = b_0 + (X)$ then $a_0 - b_0 \in (X)$ so $a_0 - b_0$ is divisible by X, $a_0 - b_0 = 0$. Consider

   $$\begin{aligned}\varphi : \mathbb{C} &\to \mathbb{C}[X]/(X) \\ a &\mapsto a + (X)\end{aligned}$$

   which is a bijection. Observe that φ is a bijection and its inverse is given by the map $f + (X) \mapsto f(0)$.

Proposition 2.4 (Euclidean algorithm for polynomials)**.** *Let F be a field and $f, g \in F[X]$. Then we may write*

$$f = g \cdot q + r$$

with $\deg r < \deg g$.

Proof. Let $\deg f = n, \deg g = m$ so

$$\begin{aligned} f &= a_0 + a_1 X + \dots + a_n X^n \\ g &= b_0 + b_1 X + \dots + b_m X^m \end{aligned}$$

with $a_n, b_m \neq 0$.

If $n < m$, let $q = 0, r = f$ so done. Suppose $n \geq m$ and proceed by induction on n. Let

$$f_1 = f - gX^{n-m} a_n b_m^{-1}$$

where b_m^{-1} exists since $b_m \in F$ and $b_m \neq 0$. This has degree $< n$. If $n = m$ then

$$f = g(X^{n-m} a_n b_m^{-1}) + f_1$$

with $\deg f_1 < n = m = \deg g$. If $n > m$, by induction we have $f_1 = gq_1 + r$ with $\deg r < \deg g$ so

$$f = g(X^{n-m} a_n b_m^{-1}) + gq_1 + r = g(X^{n-m} a_n b_m^{-1} + q_1) + r$$

as required. □

Example. Consider $(X^2 + 1) \trianglelefteq \mathbb{R}[X]$ and let $R = \mathbb{R}[X]/(X^2 + 1)$. It has elements of the form $f + (X^2 + 1)$. By Euclidean algorithm for polynomials $f = (X^2 + 1)g + r$ with $\deg r \leq 1$ so $f + (X^2 + 1) = r + (X^2 + 1)$. Any element can be represented by a polynomial of degree ≤ 1, say $a + bX + (X^2 + 1)$. If $a_1 + b_1 X + (X^2 + 1) = a_2 + b_2 X + (X^2 + 1)$ then $(a_1 + b_1 X) - (a_2 + b_2 X)$ is divisible by $X^2 + 1$. But degrees add in multiplication so $a_1 + b_1 X = a_2 + b_2 X$. Consider the bijection

$$\begin{aligned} \varphi : R &\to \mathbb{C} \\ a + bX + (X^2 + 1) &\mapsto a + bi \end{aligned}$$

It obviously send addition to addition. For multiplication,

$$\begin{aligned} &\varphi((a + bX + (X^2 + 1)) \cdot (c + dX + (X^2 + 1))) \\ =&\varphi(ac + (bc + ad)X + bdX^2 + (X^2 + 1)) \\ =&\varphi(ac + (bc + ad)X + bd(X^2 + 1) - bd + (X^2 + 1) \\ =&(ac - bd) + (bc + ad)i \\ =&(a + bi) \cdot (c + di) \\ =&\varphi(a + bX + (X^2 + 1)) \cdot \varphi(c + dX + (X^2 + 1)) \end{aligned}$$

Thus we have shown that $\mathbb{C} \cong \mathbb{R}[X]/(X^2 + 1)$.

Remark. The key idea in the proof is to force $X^2 + 1$ to vanish by quotient the polynomial ring by the generated ideal so that "$X = \pm i$". Similarly $\mathbb{Q}[X]/(X^2 - 2) \cong \mathbb{Q}[\sqrt{2}] \leq \mathbb{R}$.

This is a nice result. However, the proof is too cumbersome to be generalised as we have to check well-definedness for each case. Instead, we have the following theorems stating the general results for abstract rings and ideals. The proofs are similar to those for groups and are omitted.

Theorem 2.5 (1st Isomorphism Theorem)**.** *Let* $\varphi : R \to S$ *be a ring isomorphism. Then* $\ker\varphi \trianglelefteq R, \operatorname{Im}\varphi \leq S$ *and*

$$\begin{aligned} R/\ker\varphi &\to \operatorname{Im}\varphi \\ r + \ker\varphi &\mapsto \varphi(r) \end{aligned}$$

is a ring isomorphism.

Theorem 2.6 (2nd Isomorphism Theorem)**.** *Let* $R \leq S$ *and* $J \trianglelefteq S$*. Then* $R \cap J \trianglelefteq R$ *and*

$$\frac{R+J}{J} \cong \frac{R}{R \cap J}$$

as rings.

Theorem 2.7 (Subring and ideal correspondence)**.** *Let* $I \trianglelefteq R$*. Then there is a bijection between*

$$\begin{aligned} \{\textit{subrings of } R/I\} &\leftrightarrow \{\textit{subrings of } R \textit{ containing } I\} \\ L \leq R/I &\mapsto \{r \in R : r + I \in L\} \\ S/I \leq R/I &\mapsfrom I \trianglelefteq S \leq R \end{aligned}$$

and

$$\begin{aligned} \{\textit{ideals of } R/I\} &\leftrightarrow \{\textit{ideals of } R \textit{ containing } I\} \\ L \trianglelefteq R/I &\mapsto \{r \in R : r + I \in L\} \\ J/I \trianglelefteq R/I &\mapsfrom I \trianglelefteq J \trianglelefteq R \end{aligned}$$

Theorem 2.8 (3rd Isomorphism Theorem)**.** *Let* $I, J \trianglelefteq R, I \subseteq J$*. Then* $J/I \trianglelefteq R/I$ *and*

$$\frac{R/I}{J/I} \cong R/J.$$

Example. Consider the homomorphism

$$\begin{aligned} \varphi : \mathbb{R}[X] &\to \mathbb{C} \\ \sum a_n X^n &\mapsto \sum a_n i^n \end{aligned}$$

i.e. evaluation at i. It is surjective and

$$\ker\varphi = \{f \in \mathbb{R}[X] : f(i) = 0\} = (X^2+1)$$

because real polynomials with i as a root also have $-i$ as aroot, so are divisible by $(X-i)(X+i) = X^2+1$. By 1st Isomorphism Theorem

$$\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}.$$

Example (Characteristic of a ring)**.** For any ring R there is a unique homomorphism

$$\begin{aligned} \iota : \mathbb{Z} &\to R \\ n &\mapsto \begin{cases} \underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ times}} & n > 0 \\ -\underbrace{(1_R + 1_R + \cdots + 1_R)}_{n \text{ times}} & n < 0 \end{cases} \end{aligned}$$

$\ker \iota \trianglelefteq \mathbb{Z}$ so $\ker \iota = n\mathbb{Z}$ for some $n \geq 0$. This number n is called the *characteristic* of R, denoted $\operatorname{ch} R$.

For example, $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ all have characteristic 0. $\mathbb{Z}/n\mathbb{Z}$ have characteristic n.

2.3 Integral domain, Field of fractions, Maximal and Prime ideals

Definition (Integral domain)**.** A non-zero ring R is an *integral domain* if for all $a, b \in R$, $a \cdot b = 0$ implies that $a = 0$ or $b = 0$.

Definition (Zero divisor)**.** x is a *zero divisor* in R if $x \neq 0$ and there exists $y \neq 0$ such that $x \cdot y = 0$.

Example.

1. All fields are integral domains: if $xy = 0$ with $y \neq 0$, then y^{-1} exists and
$$0 = 0 \cdot y^{-1} = (xy) \cdot y^{-1} = x.$$
2. A subring of an integral domain is an integral domain. Thus $\mathbb{Z} \leq \mathbb{Q}, \mathbb{Z}[i] \leq \mathbb{C}$ are integral domains.

Definition (Principal ideal domain)**.** A ring R is a *principal ideal domain* (PID) if it is an integral domain and every ideal is principal, i.e. for all $I \trianglelefteq R$, there exists $a \in R$ such that $I = (a)$.

Example. $\mathbb{Z}$ is a PID.

Lemma 2.9. *A finite integral domain is a field.*

Proof. Let $a \neq 0 \in R$ and consider

$$\begin{aligned} a \cdot - : R &\to R \\ b &\mapsto ab \end{aligned}$$

This is a group homomorphism and its kernel is

$$\ker(a \cdot -) = \{b \in R : ab = 0\} = \{0\}.$$

Thus $a \cdot -$ is injective. As $|R| < \infty$, $a \cdot -$ must also be surjective. Thus there exists $b \in R$ such that $ab = 1$. $b = a^{-1}$. $\square$

Lemma 2.10. *Let R be an integral domain. Then $R[X]$ is an integral domain.*

Proof. Let

$$f = \sum_{i=0}^{n} a_i X^i$$
$$g = \sum_{j=0}^{m} b_j X^j$$

with $a_n, b_m \neq 0$ be non-zero polynomials. Then the largest power of X in fg is X^{m+n} and its coefficient is $a_n b_m \in R$. This is a product of non-zero elements on an integral domain so non-zero. Thus $fg \neq 0$. $\square$

This gives us a way to produce a new integral domain from old ones. Moreover, iterating this, $R[X_1, \dots, X_n] = ((R[X_1])[X_2] \dots [X_n])$ is an integral domain.

Theorem 2.11 (Field of fractions)**.** *Let R be an integral domain. There is a* field of fractions *F of R with the following properties:*

1. *F is a field,*
2. *$R \leq F$,*
3. *every element of F is of the form $a \cdot b^{-1}$ where $a, b \in R \leq F$.*

Proof. Consider $S = \{(a, b) \in R^2 : b \neq 0\}$ with an equivalence relation

$$(a, b) \sim (c, d) \Leftrightarrow ad = bd \in R.$$

This is reflexive and symmetric. To show it is transitive, suppose $(a, b) \sim (c, d), (c, d) \sim (e, f)$. Then

$$(ad)f = (bc)f = b(cf) = b(ed)$$

so $d(af - be) = 0$. As $d \neq 0$ and R is an *integral domain*, $af - be = 0$, i.e. $(a, b) \sim (e, f)$.

Let $F = S/\sim$ and write $[(a, b)] = \frac{a}{b}$. Define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$
$$0_F = \frac{0}{1}$$
$$1_F = \frac{1}{1}$$

These are well-defined. If $\frac{a}{b} \neq 0_F = \frac{0}{1}$ then $a \cdot 1 \neq 0 \cdot b = 0$. Then $\frac{b}{a} \in F$ and $\frac{a}{b} \cdot \frac{b}{a} = \frac{1}{1} = 1_F$ so $\frac{a}{b} \in F$ has an inverse. F is a field.

R is a subring of F via

$$R \hookrightarrow F$$
$$r \mapsto \frac{r}{1}$$

which is injective as R is an integral domain. $\square$

Example.

1. The field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$.
2. The field of fractions of $\mathbb{C}[X]$ is

$$\mathbb{C}(X) = \left\{ \frac{p(X)}{q(X)} : p(X), q(X) \in \mathbb{C}[X], q(X) \neq 0 \right\},$$

the field of *rational functions*.

As we have mentioned before, $\{0\}$ is a bona fide ring although it is a (trivial) counterexample to many results. However, it is not a field as we require $0 \neq 1$. To emphasise this, we declare

Fiat. The ring $\{0\}$ is *not* a field.

Lemma 2.12. *A non-zero ring R is a field if and only if its only ideals are $\{0\}$ and R.*

Proof.

- $\Rightarrow$: Suppose $I \trianglelefteq R$ is a non-zero ideal, then it contains $a \neq 0$. But an ideal containing a unit must be the whole ring.
- $\Leftarrow$: Let $x \neq 0 \in R$. Then $(x) = R$ as it is not the zero ideal. Thus there exists $y \in R$ such that $xy = 1_R$ so x is a unit.

□

Definition (Maximal ideal)**.** An ideal $I \trianglelefteq R$ is *maximal* if there is no proper ideal which properly contains I.

Lemma 2.13. *An ideal $I \trianglelefteq R$ is maximal if and only if R/I is a field.*

Proof. R/I is a field if and only if I/I and R/I are the only ideals in R/I, if and only if $I, R \trianglelefteq R$ are the only ideals containing I. □

Definition (Prime ideal)**.** An ideal $I \trianglelefteq R$ is *prime* if I is proper and if $a, b \in R$ such that $ab \in I$ then $a \in I$ or $b \in I$.

Example. The ideal $n\mathbb{Z}$ is prime if and only if n is 0 or a prime number: if p is prime and $a, b \in p\mathbb{Z}$ then $p \mid ab$ so $p \mid a$ or $p \mid b$, i.e. $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$. Conversely, if $n = uv$ is composite, $u < n$ then $uv \in n\mathbb{Z}$ but $u \notin n\mathbb{Z}$.

Lemma 2.14. *$I \trianglelefteq R$ is prime if and only if R/I is an integral domain.*

Proof.

- $\Rightarrow$: Supose $I \trianglelefteq R$ is prime. Let $a+I, b+I \in R/I$ be such that $(a+I)(b+I) = 0_{R/I}$. Since $ab+I = 0_{R/I}$, $ab \in I$. As I is prime, $a \in I$ or $b \in I$, i.e. $a+I = 0_{R/I}$ or $b+I = 0_{R/I}$. Thus R/I is an integral domain.

- $\Leftarrow$: Suppose R/I is an integral domain. Let $a, b \in R$ such that $ab+I = 0_{R/I}$. $(a+I)(b+I) = 0_{R/I}$. As R/I is an integral domain, $a+I = 0_{R/I}$ or $b+I = 0_{R/I}$, i.e. $a \in I$ or $b \in I$.

$\square$

Corollary 2.15. *Maximal ideals are prime.*

Proof. Fields are integral domains. $\square$

Lemma 2.16. *If R is an integral domain then its characteristic is 0 or a prime number.*

Proof. Consider $\ker(\iota : \mathbb{Z} \to R) = n\mathbb{Z}$. By 1st Isomorphism Theorem

$$\mathbb{Z}/n\mathbb{Z} \cong \operatorname{Im} \iota \leq R.$$

As a subring of an integral domain is an integral domain, $\mathbb{Z}/n\mathbb{Z}$ is an integral domain so $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ is prime. Thus $n = 0$ or a prime number. $\square$

2.4 Factorisation in integral domains

Let R be an integral domain in this section.

We begin with several definitions. Note that for every statement about an element of the ring there is an equivalent one in terms of ideals.

Definition (Unit, divisibility, associates, irreducible, prime)**.**

- An element $a \in R$ is a *unit* if there is $b \in R$ such that $ab = 1_R$. Equivalently, $(a) = R$.

- $a \in R$ *divides* $b \in R$ if there is a $c \in R$ such that $b = ac$. Equivalently, $(b) \subseteq (a)$. Write $a \mid b$.

- $a, b \in R$ are *associates* if $a \mid b$ and $b \mid a$. Equivalently, $(a) = (b)$.

- $r \in R$ is *irreducible* if it is not zero, not a unit and if $r = ab$ then a or b is a unit.

- $r \in R$ is *prime* if it is not zero, not a unit and if $r \mid ab$ then $r \mid a$ or $r \mid b$. Equivalently, $ab \in (r) \Rightarrow a \in (r)$ or $b \in (r)$.

Remark. Being a unit/irreducible/prime depends not only on the element but also on the ambient ring: $2X \in \mathbb{Z}[X]$ is not irreducible but $2X \in \mathbb{Q}[X]$ is.

Lemma 2.17. *$(r) \trianglelefteq R$ is prime if and only if r is zero or prime.*

Proof.

- $\Rightarrow$: Let $(r) \trianglelefteq R$ be a prime ideal and $r \mid ab$. Then $ab \in (r)$ so $a \in (r)$ or $b \in (r)$ as (r) is prime. So $r \mid a$ or $r \mid b$. r is 0 or a prime.
- $\Leftarrow$: If $r = 0$ then $(0) \trianglelefteq R$ is a prime ideal since $R \cong R/(0)$ is an integral domain. Let $r \neq 0$ be a prime and $ab \in (r)$. Then $r \mid ab$ so $r \mid a$ or $r \mid b$. $a \in (r)$ or $b \in (r)$ as required.

□

Lemma 2.18. *If $r \in R$ is prime then it is irreducible.*

Proof. Let $r = ab$. Then $r \mid ab$ so $r \mid a$ or $r \mid b$. Suppose $r \mid a$ wlog. Then $a = rc$. $r = (rc)b$, $r(bc - 1) = 0$. As $r \neq 0$ and R is an integral domain, $bc - 1 = 0$ so b is a unit. □

Example. Let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \leq \mathbb{C}$. This is a subring of a field so an integral domain. Define

$$
\begin{aligned}
N : R &\to \mathbb{Z}_{\geq 0} \\
a + b\sqrt{-5} &\mapsto a^2 + 5b^2
\end{aligned}
$$

so $N(z) = z\bar{z}$. Note $N(r_1 r_2) = N(r_1)N(r_2)$. If r is a unit then there exists $s \in R$ such that $rs = 1$, then $N(r)N(s) = N(1) = 1$, so $N(r) = 1$. So $r = a + b\sqrt{-5}$ such that $a^2 + 5b^2 = 1$. The only possibility is $r = \pm 1$. Claim that $2 \in R$ is irreducible:

Proof. Let $2 = ab$ so $N(a)N(b) = 4$. $N(a) = 1, 2$ or 4. But $N(a) \neq 2$ so $N(a) = 1$ or 4, $N(b) = 4$ or 1 so a or b is a unit. □

Similarly we can show that 3 and $1 \pm \sqrt{-5}$ are irreducible.

Note that

$$
(1 + \sqrt{-5})(1 - \sqrt{-5}) = 1 + 5 = 6 = 2 \cdot 3
$$

so $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$ but $N(1 \pm \sqrt{-5}) = 6$ is *not* divisible by $N(2) = 4$ so $2 \nmid 1 \pm \sqrt{-5}$. Thus $2 \in R$ is not prime.

We also find that $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ has two different factorisations into irreducibles.

Definition (Euclidean domain)**.** An integral domain R is a *Euclidean domain* (ED) if there is a function $\varphi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$, a *Euclidean function* such that

1. $\forall a, b \in R \setminus \{0\}$, $\varphi(ab) \geq \varphi(a)$,
2. $\forall a, b \in R, b \neq 0$, we have $a = bq + r$ with $r = 0$ or $\varphi(r) < \varphi(b)$.

Example.

1. $\mathbb{Z}$ is a Euclidean domain with $\varphi(n) = |n|$.

2. For a field $\mathbb{F}$, $\mathbb{F}[X]$ is a Euclidean domain with $\varphi(f) = \deg f$.

3. $\mathbb{Z}[i]$ is a Euclidean domain with $\varphi(a+ib) = a^2 + b^2 = (a+ib)(a-ib)$.

   Proof. Let $z_1, z_2 \in \mathbb{Z}[i], z_2 \neq 0$. Consider $\frac{z_1}{z_2} \in \mathbb{C}$. By considering the lattice of Gaussian integers on the complex plane, we can find $q \in \mathbb{Z}[i]$ such that $\left|\frac{z_1}{z_2} - q\right| < 1$. Consider $r = z_1 - qz_2 \in \mathbb{Z}[i]$,

   $$\left|\frac{r}{z_2}\right| = \left|\frac{z_1}{z_2} - q\right| < 1$$

   so $|r| < |z_2|$ so $\varphi(r) = |r|^2 < |z_2|^2 = \varphi(z_2)$. □

4. Similarly we can show $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.

Proposition 2.19. *If R is a ED then it is a PID.*

This proof is a generalisation of the proof that $\mathbb{Z}$ is a PID.

Proof. Let $I \trianglelefteq R$ and choose $0 \neq b \in I$ such that $\varphi(b)$ is minimal. If $a \in I$ then Euclidean property gives $a = qb + r$ with $\varphi(r) < \varphi(b)$ or $r = 0$. Then $r = a - qb \in I$ but if $r \neq 0$ then minimality of $\varphi(b)$ is contradicted. Thus $r = 0$ and $a \in (b)$. $I = (b)$. □

Example. $\mathbb{Z}, \mathbb{F}[X]$ and $\mathbb{Z}[i]$ are PIDs.

Example. $\mathbb{Z}[X]$ is *not* a PID. Consider $(2, X) \trianglelefteq \mathbb{Z}[X]$. Suppose $(2, X) = (f)$ for some $f \in \mathbb{Z}[X]$, then $f \mid 2$. Degrees of polynomials on an integral domain add under multiplication so if f divides a constant polynomial it must be constant. Thus $f = \pm 1, \pm 2$. If $f = \pm 2$, $\pm 2 \nmid X$. Absurd. Thus $f = \pm 1$, $(f) = \mathbb{Z}[X]$. But $1 \neq (2, X)$. Absurd.

Example. Let $\mathbb{F}$ be a field and $A \in \mathcal{M}_n(\mathbb{F})$. Consider

$$I = \{f \in \mathbb{F}[X] : f(A) = 0\}.$$

If $f, g \in I$, $(f+g)(A) = f(A) + g(A) = 0$. If $h \in \mathbb{F}[X]$, $(fh)(A) = f(A)h(A) = 0$ so $I \trianglelefteq \mathbb{F}[X]$. As $\mathbb{F}[X]$ is a PID, $I = (m_A)$ for some $m_A \in \mathbb{F}[X]$. This m_A is the *minimal polynomial* of A and it follows that it is unique up to a unit.

Definition (Unique factorisation domain)**.** An integral domain is a *unique factoriation domain* (UFD) if

- every non-zero, non-unit is a product of irreducibles,
- if $p_1 \cdots p_n = q_1 \cdots q_m$ are factorisations into irreducibles, then $n = m$ and p_i is an associate of q_i up to reordering.

We will show that PIDs are UFDs.

Lemma 2.20. *If R is a PID then irreducibles are primes.*

Proof. Let $p \in R$ be irreducible and suppose $s \mid ab$. Need to show that $p \mid a$ or $p \mid b$. Suppose $p \nmid a$. Consider $(p, a) \trianglelefteq R$. As R is a PID, there exists $d \in R$ such that $(d) = (p, a)$, so $p = q_1 d, a = q_2 d$. As p is irreducible, either q_1 or d is a unit. If q_1 is a unit then $a = q_2 d = q_2(q_1^{-1} p)$ so $p \mid a$. Thus d must be a unit and $(p, a) = (d) = R$. Thus $1_R = rp + sa$ for some r and s. $b = brp + abs$ so $p \mid b$. □

Lemma 2.21. *Let R be a PID and $I_1 \subseteq I_2 \subseteq I_2 \subseteq \cdots$ be an increasing sequence of ideal. Then there exists $N \in \mathbb{N}$ such that for all $n \geq N$, $I_n = I_{n+1}$.*

Definition (Noetherian)**.** The above condition is the *ascending chain condition*. A chain satisfying the above condition is *Noetherian*.

Proof. Let $I = \bigcup_{n=1}^{\infty} I_n$ which is again an ideal so $I = (a)$ for some $a \in R$. Then $a \in I$ so there exists $N \in \mathbb{N}$ such that $a \in I_N$. Then

$$(a) \subseteq I_N \subseteq I_{N+1} \cdots \subseteq (a)$$

so equality throughout. □

Theorem 2.22. *PID is UFD.*

Proof. Let R be a PID. The proof consists of two parts: first show the existence of factorisation in R (the proof thereof generalises to all Noetherian rings), and then show its uniqueness.

1. Suppose for contradiction there exists $a \in R$ which cannot be written as a product of irreducibles. then a is not irreducible so $a = a_1 b_1$ with a_1, b_1 not units and one of then cannot be written as a product of irreducibles (otherwise a would be), say it is a_1. Hence $a_1 = a_2 b_2$ where a_2, b_2 are not units and wlog a_2 could not be written as a product of irreducibles. Continue this way. Now

$$(a) \subseteq (a_1) \subseteq (a_2) \subseteq \cdots$$

   is an ascending chain so by ACC we must have $(a_N) = (a_{N+1})$ for some N, i.e. $a_N = a_{N+1} b_{N+1}$ with b_{N+1} a unit.

2. Let $p_1 \cdots p_n = q_1 \cdots q_m$ be factorisations into irreducibles. Thus $p_1 \mid q_1 \cdots q_n$. In a PID irreducibles are primes so $p_1 \mid q_i$ for some i. After reordering $p_1 \mid q_1$ so $q_1 = p_1 \cdot a$. As q_1 is irreducible, a is a unit so p_1 and q_1 are associates. Now $p_1(p_2 \cdots p_n - a q_2 \cdots q_m) = 0$. As R is an integral domain $p_2 \cdots p_n = (a q_2) \cdots q_m$. Continue this way, we get $n \leq m$ and $1 = (\text{unit}) \cdot q_{n+1} \cdots q_m$. Thus $q_{n+1}, \ldots q_m$ are units. Absrud. Thus $n = m$ and p_i's and q_i's are associates up to reordering.

□

Definition (gcd, lcm)**.**

- d is a *greatest common divisor* (gcd) of $a_1, \dots, a_n$, written $\gcd(a_1, \dots, a_n)$, if $d \mid a_i$ for all i and if $d' \mid a_i$ for all i then $d' \mid d$.
- d is a *lowest common multiple* (lcm) of $a_1, \dots, a_n$, written $\operatorname{lcm}(a_1, \dots, a_n)$, if $a_i \mid m$ for all i and if $a_i \mid d'$ for all i then $d \mid d'$.

It is easy to see that if gcd or lcm exists then it is unique up to associates.

Proposition 2.23. *If R is a UFD then gcd's and lcm's exist.*

Proof. Write each a_i as a product

$$a_i = u_i \cdot \prod_j p_j^{n_i j}$$

where u_i is a unit and p_j's are (the same) irreducibles which are not associates of each other. Set

$$d = \prod_j p_j^{m_j}$$

where $m_j = \min_i n_{ij}$. Certainly $d \mid a_i$ for all i. If $d' \mid a_i$ for all i then write

$$d' = u \cdot \prod_j p_j^{t_j}$$

for some t_j. As $d' \mid a$ we must have $t_j \leq n_{ij}$ for all i so $t_j \leq \min_i n_{ij} = m_j$ for all j. Thus $d' \mid d$.

The argument for lcm is similar. $\square$

2.5 Factoriation in polynomial rings

For a field $\mathbb{F}$ we know $\mathbb{F}[X]$ is a ED, so also a PID and UFD so

1. any $I \trianglelefteq \mathbb{F}[X]$ is principal, i.e. $I = (f)$ for some f;
2. $f \in \mathbb{F}[X]$ is irreducible if and only if f is prime;
3. let $f \in \mathbb{F}[X]$ be irreducible and $(f) \subseteq J \trianglelefteq \mathbb{F}[X]$ be a larger ideal. Then $J = (g)$ for some $g \in \mathbb{F}[X]$ so $(f) \subseteq (g)$, i.e. $g \mid f$. But f is irreducible so either g is a unit, then $(g) = \mathbb{F}[X]$, or g is an associate of f, so $(g) = (f)$. Thus (f) is maximal;
4. $$(f) \text{ prime} \implies f \text{ prime} \implies f \text{ irreducible} \implies (f) \text{ maximal}$$

   so prime ideals of $\mathbb{F}[X]$ are precisely the maximal ideals;
5. $f \in \mathbb{F}[X]$ is irreducible if and only if (f) is maximal, if and only if $\mathbb{F}[X]/(f)$ is a field.

Definition (Content)**.** Let R be a UFD and

$$f = a_0 + a_1 X + \dots a_n X^n \in R[X]$$

with $a_n \neq 0$. The *content* is

$$c(f) = \gcd(a_0, \dots, a_n).$$

Definition (Primitive)**.** f above is *primitive* if $c(f)$ is a unit, i.e. a_i's are coprime.

Theorem 2.24 (Gauss' Lemma)**.** *Let R be a UFD and F be its field of fractions. Let $f \in R[X]$ be primitive. Then f is irreducible in $R[X]$ if and only if f is irreducible in $F[X]$.*

Example. Let $f = 1 + X + X^3 \in \mathbb{Z}[X]$. $c(f) = 1$ so f is primitive. Suppose $f = gh$, a product of irreducibles in $\mathbb{Z}[X]$. As f is primitive, neither g nor h can be a constant polynomial so they have degree 1 and 2 respectively. Wlog suppose $g = b_0 + b_1 X, h = c_0 + c_1 X + c_2 X^2 \in \mathbb{Z}[X]$. Expanding out and equating the coefficients, $b_0 c_0 = 1, b_1 c_2 = 1$ so $b_0 b_1 = \pm 1$. Thus g has one of ± 1 as a root and so does f. But it doesn't so such factorisation does not exist. Thus $\mathbb{Q}[X]/(1 + X + X^3)$ is a field.

Lemma 2.25. *Let R be a UFD. If $f, g \in F[X]$ are primitives then so is fg.*

Proof. Let

$$\begin{aligned} f &= a_0 + a_1 X + \dots + a_n X^n \\ g &= b_0 + b_1 X + \dots + b_m X^m \end{aligned}$$

with $a_n, b_m \neq 0$. If fg is not primitive, then $c(fg)$ is not a unit so there is an irreducible $p \mid c(fg)$. As $c(f)$ and $c(g)$ are units, we have

$$\begin{aligned} p \mid a_0, p \mid a_1, \dots, p \mid a_{k-1}, p \nmid a_k \\ p \mid b_0, p \mid b_1, \dots, p \mid b_{\ell-1}, p \nmid b_\ell \end{aligned}$$

The coefficients of $X^{k+\ell}$ in fg is

$$\sum_{i+j=k+\ell} a_i b_j = \dots + a_{k+1} b_{\ell-1} + a_k b_\ell + a_{k-1} b_{\ell+1} + \dots$$

where LHS is divisible by p so $p \mid a_k b_\ell$ but p is prime so $p \mid a_k$ or $p \mid b_\ell$. Absurd. Thus $c(fg)$ is a unit and fg is a primitive. $\square$

Corollary 2.26. *Let R be a UFD. Then $c(fg)$ is an associate of $c(f)c(g)$.*

Proof. Let $f = c(f) \cdot f_1, g = c(f) \cdot g_1$ with f_1, g_1 primitive. Then

$$fg = c(f)c(g) \cdot (f_1 g_1)$$

where $f_1 g_1$ is primitive by the lemma above. Thus $c(f)c(g)$ is a gcd of the coefficients of fg. $\square$

Proof of Gauss' Lemma. Let $f \in R[X]$ be primitive. If $f = gh$ is reducible in $R[X]$ then g, h cannot be constants as otherwise f would not be primitive. Thus $g, h \in F[X]$ are not units so $f \in F[X]$ is reducible.

Suppose instead f is reducible in $F[X]$, say $f = gh$. We can "clear the denominators": find $a, b \in R$ such that $ag, bh \in R[X]$, then

$$abf = (ag) \cdot (bh) \in R[X].$$

Take contents, $ag = c(ag) \cdot g_1, bh = c(bh) \cdot h_1$ with g_1, h_1 primitive. Then

$$ab \cdot f = c(ag)c(bf) \underbrace{g_1 h_1}_{\text{primitive}}$$

so ab is an associate of $c(ag)c(bh)$ so $c(ag)c(bh) = uab$ where u is a unit. Thus $abf = uabg_1h_1$ and cancel to get $f = (ug_1)h_1$ is reducible in $R[X]$. □

Proposition 2.27. *Let R be a UFD and $g \in R[X]$ primitive. Let $I = (g) \trianglelefteq F[X]$ where F is the field of fraction of R and $J = (g) \trianglelefteq R[X]$. Then*

$$J = I \cap R[X].$$

Equivalently, if $f \in R[X]$ is divisible by a primitive $g \in F[X]$ then it is divisible by g in $R[X]$.

Proof. The $\subseteq$ inclusion is clear. To show the other direction, let $f = gh \in F[X]$. Clear denominators by find $b \in R$ such that $bh \in R[X]$ so $bf = (bh) \cdot g \in R[X]$. Thus $bf = c(bh)h_1g$ with h_1 primitive. Now it follows that $b \mid c(bh)$, as $bc(f) = c(bh)$, so we get $f = c(f) \cdot h_1g \in R[X]$. g divides f in $R[X]$. □

Theorem 2.28. *If R is a UFD then so is $R[X]$.*

Proof. To show existence, let $f \in R[X]$ and write $f = c(f) \cdot f_1$ with f_1 primitive. As R is a UFD we can write $c(f) = p_1 \cdots p_n \in R$ with p_i irreducible in R, so also irreducible in $R[X]$. If f_1 is not irreducible, write $f_1 = f_2 \cdot f_3$with f_2, f_3 not units and are primitive. Thus f_2, f_3 are not constants so have degree smaller than that of f_1. If f_2 or f_3 is irreducible, factor again. The degree continues to strictly decrease and this stops eventually. So

$$f = p_1 \cdots p_n q_1 \cdots q_m,$$

a product of irreducibles.

Now for the uniqueness part, note $p_1 \cdots p_n = c(f) \in R$, a UFD so the p_i's are unique up to reordering and associates. Thus it suffices to show if $q_1 \cdots q_m = r_1 \cdots r_\ell$ as products of primitive polynomials then $m = \ell$ and the q_i's and r_i's are the same up to reordering and associates. Since $F[X]$ *is a PID and thus UFD*, $q_1 \cdots q_m = r_1 \cdots r_\ell \in R[X] \subseteq F[X]$ implise that $m = \ell$ and q_i's equal to r_i's in $F[X]$. If q_1 is an associate of r_1 in $F[X]$ then $q_1 = ur_1$ for some unit $u \in F[X]$. Then $u \in F$ is a unit, write $u = \frac{a}{b}$. Get $bq_1 = ar_1 \in R[X]$. Taking contents, it follows that b is an associate of a in R. Cancel to get $q_1 = ar_1 \in R[X]$. Repeat for q_i's and r_i's. □

Example.

1. $\mathbb{Z}[X]$ is a UFD.
2. If R is a UFD then so is $R[X_1, \dots, X_n]$.

Proposition 2.29 (Eisenstein's criterion)**.** *Let R be a UFD and $f = a_0 + a_1X + \dots + a_nX^n \in R[X]$ with $a_n \neq 0$ be primitive. Suppose $p \in R$ is an irreducible such that*

- $p \nmid a_n$,
- $p \mid a_i$ *for* $i = 0, 1, \dots, n-1$,
- $p^2 \nmid a_0$

then f is irreducible in $R[X]$, so also in $F[X]$.

Proof. Let $f = gh$ with

$$\begin{aligned} g &= r_0 + r_1X + \dots + r_kX^k \\ h &= s_0 + s_1X + \dots + r_\ell X^\ell \end{aligned}$$

with $r_k, s_\ell \neq 0$. Then $k + \ell = n$ and $a_n = r_ks_\ell$. As $p \nmid a_n$, $p \nmid r_k$ and $p \nmid s_\ell$. Since $p \mid a_0$ and $p^2 \nmid a_0$, suppose wlog that $p \mid r_0, p \nmid s_0$. Suppose $p \mid r_0, p \mid r_1, p \mid r_{j-1}, p \nmid r_j$. Then

$$a_j = s_0r_j + s_1r_{j-1} + s_2r_{j-2} + \dots + s_jr_0$$

so $p \nmid a_j$ and by 2 $j = n$. Thus $\deg g = n$ and h is a constant. As f (and hence g and h) is a primitive h is a unit. □

Example. For $p \in \mathbb{Z}$ prime, $f = X^m - p \in \mathbb{Z}[X]$ is irreducible in $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$ so f does not have a root in $\mathbb{Q}$. In particular, this shows that $\sqrt[m]{p} \notin \mathbb{Q}$). This will be important in IID Galois Theory.

Example. For $p \in \mathbb{Z}$ prime, let

$$f = X^{p-1} + X^{p-2} + \dots + X + 1 \in \mathbb{Z}[X].$$

Note that $(X-1)f = X^p - 1$. Consider the ring isomorphism

$$\begin{aligned} \varphi : \mathbb{Z}[X] &\to \mathbb{Z}[X] \\ X &\mapsto X + 1 \end{aligned}$$

Then

$$\varphi(f) = \underbrace{X^{p-1}}_{p\nmid} + \underbrace{\binom{p}{1}}_{p\mid} X^{p-1} + \dots + \underbrace{\binom{p}{p-2}}_{p\mid} X + \underbrace{\binom{p}{p-1}}_{=p}$$

so Eisenstein's criterion says that $\varphi(f)$ is irreducible, so is f.

Remark. The hypothesis of Eisenstein's criterion depends on the ambient ring while the conclusiohn does not. As a heuristics, we can apply ring isomorphisms to reduce the problem sometimes.

2.6 Gaussian integers

Recall
$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \leq \mathbb{C}.$$
It has a norm $N(a + ib) = a^2 + b^2$, making it a ED, and thus a PID and UFD. In particular primes and irreducibles agree. The units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$ as they are the only elements of norm 1. In addition, we have the following observations:

1. $2 = (1 + i)(1 - i)$ is *not* a prime.
2. $N(3) = 9$. If $3 = xy$ then $9 = N(x)N(y)$. Either x or y is a unit or $N(x) = N(y) = 3$. But the norm is never 3 so 3 *is* a prime.
3. $5 = (2 + i)(2 - i)$ is *not* a prime.
4. 7 *is* a prime.

Proposition 2.30. *A prime $p \in \mathbb{Z}$ is a prime in $\mathbb{Z}[i]$ if and only if $p \neq a^2 + b^2$ for $a, b \in \mathbb{Z}$.*

Proof.

- $\Rightarrow$: If $p = a^2 + b^2 = (a + ib)(a - ib)$, it is reducible and thus not a prime.
- $\Leftarrow$: Note $N(p) = p^2$. If p factors as uv with u, v not units then $N(u) = N(v) = p$. Write $u = a + ib$, we have $p = N(u) = a^2 + b^2$.

$\square$

Now we prove a lemma regarding the multiplicative group of a finite field:

Lemma 2.31. *Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be a field with p elements and p prime. Then $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ is a group under multiplication and is isomorphic to C_{p-1}.*

Proof. Certainly $\mathbb{F}_p^\times$ is an abelian group of order $p - 1$. By the classification theorem of finite abelain groups, $\mathbb{F}_p^\times$ is either cyclic or contains $C_m \times C_m$ as a subgroup for some $m \geq 2$.

Suppose $C_m \times C_m \leq \mathbb{F}_p^\times$. Consider $f = X^m - 1 \in \mathbb{F}_p[X]$. Each element of $C_m \times C_m \leq \mathbb{F}_p^\times \subseteq \mathbb{F}_p$ gives a root of f so it has at least m^2 distinct roots. But as $\mathbb{F}_p[X]$ is a ED and thus UFD, it can be factorised into at most m unique irreducibles. Thus it has at most m distinct roots in $\mathbb{F}_p$. Thus there is no subgroup $C_m \times C_m$ in $\mathbb{F}_p^\times$ and $\mathbb{F}_p^\times$ is cyclic. $\square$

Proposition 2.32. *The primes in $\mathbb{Z}[i]$ are, up to associates,*

1. *prime $p \in \mathbb{Z}$ with $p = 3 \mod 4$,*
2. *$z \in \mathbb{Z}[i]$ such that $N(z) = p$ where p is a prime and $p = 2$, or $p = 1$* mod 4.

Proof. First show what we claimed are indeed primes, i.e. irreducibles:

1. if $p = 3 \mod 4$, $p \neq a^2 + b^2$ so $p \in \mathbb{Z}[i]$ is a prime.
2. suppose $z = uv$ then $N(u)N(v) = p$ so $N(u)$ or $N(v) = 1$. u or v is a unit so z is irreducible.

Now let $z \in \mathbb{Z}[i]$ be a prime. Then $\overline{z}$ is irreducible too so $N(z) = z\overline{z}$ is a factorisation of $N(z)$ into irreducibles in $\mathbb{Z}[i]$. Let $p \in \mathbb{Z}$ be a prime dividing $N(z)$.

- Case 1: $p = 3 \mod 4$. Then p is irreducible in $\mathbb{Z}[i]$. As $p \mid N(z)$, $p \mid z$ or $p \mid \overline{z}$. Wlog $p \mid z$. As p and z are both irreducibles, they are associates.
- Case 2: $p = 2$, or $p = 1 \mod 4$. If $p = 1 \mod 4$, consider $\mathbb{F}_p^\times \cong C_{p-1} = C_{4k}$. It has a unique element of order 2, namely $[-1]$. As $4 \mid p-1$, there is also an element $[a] \in \mathbb{F}_p^\times$ order 4. Then $[a^2]$ has order 2 and thus $a^2 = -1 \mod p$. Thus there exists $b \in \mathbb{Z}$ such that $a^2 + 1 = pb$, $p \mid (a+i)(a-i)$.

  If $p = 2$ then $p \mid (1+i)(1-i)$.

  But $p \nmid a+i, p \nmid a-i$ so $p \in \mathbb{Z}[i]$ is not prime and thus not irreducible. Hence $p = z_1 z_2$ with z_1, z_2 not units. $p^2 = N(p) = N(z_1)N(z_2)$, $N(z_1) = N(z_2) = p$ so $p = z_1\overline{z_1} = z_2\overline{z_2}$. But also $p = z_1 z_2$ so $z_2 = \overline{z}_1$.

  We choose p such that $p \mid N(z)$ so $z_1\overline{z_1} \mid z\overline{z}$ and z is prime so $z \mid z_1$ or $z \mid \overline{z_1}$. z_1 or $\overline{z_1}$ is an associate of z. $N(z) = N(z_1)$ or $N(\overline{z_1}) = p$.

□

> **Corollary 2.33.** *An integer $n \in \mathbb{Z} > 0$ can be written as $a^2 + b^2$, $a, b \in \mathbb{Z}$ if and only if when we write $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ with p_i's distinct, if $p_i = 3 \mod 4$ then n_i's are even.*

Proof. Let $n = a^2 + b^2 = (a+ib)(a-ib) = N(a+ib)$. Let $z = a + ib$. Then $z = \alpha_1 \cdots \alpha_s$ as a product of irreducibles (i.e. primes) in $\mathbb{Z}[i]$. Then $n = N(\alpha_1) \cdots N(\alpha_s)$. Each α_i is either a prime p congruent to 3 mod 4 so $N(\alpha_i) = p^2$, or has $N(\alpha_i) = q$, a prime not congruent to 3 mod 4. Thus n can be written as a product of primes as claimed.

Conversely, suppose $n = p_1^{n_1} \cdots p_k^{n_k}$ with n_i even if $p = 3 \mod 4$. For each i if $p_i = 3 \mod 4$ then $N(p_i) = p_i^2$, $p_i^{n_i} = N(p_i^{n_i/2})$. As n is a product of norms of Gaussian integers, it is the norm of a Gaussian integer so is a sum of squares. □

Example. In how many ways can 65 be written as a sum of two squares?

$65 = 5 \times 13$, $5 = 1^2 + 2^2 = (2+i)\overline{(2+i)}$, $13 = 2^2 + 3^2 = (2+3i)\overline{(2+3i)}$ so

$$\begin{aligned} 65 &= (2+i)(2+3i)\overline{(2+i)(2+3i)} \\ &= N((2+i)(2+3i)) = N(1+8i) = 1^2 + 8^2 \\ &= N((2+i)(2-3i)) = N(7-4i) = 7^2 + 4^2 \end{aligned}$$

Exercise (Challenge)**.** Find conditions such that $n = a^2 + 2b^2$ and $a^2 + 3b^2$ in $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\sqrt{-3}]$.

2.7 Algebraic integers

Definition (Algebraic integer)**.** A complex number $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic polynomial with integer coefficients.

If α is an algebraic integer, let $\mathbb{Z}[\alpha] \leq \mathbb{C}$ be the smallest subring containing α, i.e. it is the image of the ring homomorphism

$$\begin{aligned} \varphi : \mathbb{Z}[X] &\to \mathbb{C} \\ X &\mapsto \alpha \end{aligned}$$

Thus by 1st Isomorphism Theorem $\mathbb{Z}[\alpha] \cong \mathbb{Z}[X]/I$ where $I = \ker \varphi$.

Proposition 2.34 (Minimal polynomial)**.** *If α is an algebraic integer then $I = \ker \varphi$ is principal and is generated by an irreducible $f_\alpha \in \mathbb{Z}[X]$, the* minimal polynomial *of α.*

Proof. As α is an algebraic integer, it is a root of some $f \in \mathbb{Z}[X]$ so $f \in I$. Let $f_\alpha \in I$ be a polynomial of minimal degree, which we may assume is positive. We want to show that

1. $I = (f_\alpha)$,
2. f_α is irreducible.

1. Let $h \in I$. Now $\mathbb{Q}[X]$ is a ED so we can write $h = qf_\alpha + r \in \mathbb{Q}[X]$ with $r = 0$ or $\deg r < \deg f_\alpha$. Clearing denominators, there is an $a \in \mathbb{Z}$ such that $aq, ar \in \mathbb{Z}[X]$, so $ah = (aq)f_\alpha + ar \in \mathbb{Z}[X]$. α is a root of h and of f_α so is also a root of ar. As f_α has minimal degree among polynomials with α as a root, we must have $ar = 0$. Thus $ah = (aq)f_\alpha$. Now $c(ah) = a \cdot c(h)$, $c((aq)f_\alpha) = c(aq)$ so $a \mid c(aq)$ so $aq = a\overline{q}$ with $\overline{q} \in \mathbb{Z}[X]$. Cancelling shows that $\overline{q} = q$. Thus $h = \overline{q}f_\alpha$ so $h \in (f_\alpha)$.
2. $\mathbb{Z}[X]/(f_\alpha) \cong \mathbb{Z}[\alpha] \leq \mathbb{C}$. As $\mathbb{C}$ is an integral domain, so is $\mathbb{Z}[\alpha]$. Thus (f_α) is prime. Thus $f_\alpha \in \mathbb{Z}[X]$ is a prime and hence irreducible.

□

Example.

1. $\alpha = i$, $f_\alpha = X^2 + 1$.
2. $\alpha = \sqrt{2}$, $f_\alpha = X^2 - 2$.
3. $\alpha = \frac{1+\sqrt{-3}}{2}$, $f_\alpha = X^2 - X + 1$.
4. Less trivially, for $d \in \mathbb{Z}$, $X^5 - X + d$ has a unique real root α. This α cannot be constructed using $(\mathbb{Z}, +, \times, \sqrt{\ })$. c.f. IID Galois Theory.

Lemma 2.35. *If α is an algebraic integer and $\alpha \in \mathbb{Q}$ then $\alpha \in \mathbb{Z}$.*

Proof. $f_\alpha \in \mathbb{Z}[X]$ is irreducible and primitive. By Gauss' Lemma $f_\alpha \in \mathbb{Q}[X]$ is also irreducible. But if $\alpha \in \mathbb{Q}$, $X - \alpha \mid f_\alpha$ in $\mathbb{Q}[X]$ so $f_\alpha = X - a$. But $f_\alpha \in \mathbb{Z}[X]$ so $\alpha \in \mathbb{Z}$. □

2.8 Hilbert Basis Theorem

Recall that a ring R satisfies the ascending chain condition (ACC) if whenever

$$I_1 \subseteq I_2 \subseteq \cdots$$

ais an increasing sequence of ideals then there exists $N \in \mathbb{N}$ such that for all $n \geq N$, $I_n = I_{n+1}$.

A ring satisfying ACC is called *Noetherian*.

We have shown that a PID is Noetherian.

Lemma 2.36. *A ring R is Noetherian if and only if every ideal of R if finitely generated.*

Proof.

- $\Leftarrow$: Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideal and $I = \bigcup_n I_n$. Then $I = (a_1, \dots, a_n)$ for some $a_i \in R$. For all i there exists $n_i \in \mathbb{N}$ such that $a_i \in I_{n_i}$ so
$$(a_1, \dots, a_n) \subseteq I_{\max_i n_i} \subseteq I.$$
Take $N = \max_i n_i$ and the result follows.
- Suppose R is Noetherian and $I \trianglelefteq R$. Choose $a_1 \in I$. If $I = (a_1)$ then done, so suppose not. Then choose $a_2 \in I \setminus (a_1)$. If $I = (a_1, a_2)$ then done, so suppose not. If we are never finished by this process then we get
$$(a_1) \subseteq (a_1, a_2) \subseteq \cdots$$
which is impossible as R is Noetherian. Thus $I = (a_1, \dots, a_n)$ for some n.

$\square$

Theorem 2.37 (Hilbert Basis Theorem)**.** *If R is Noetherian then so is $R[X]$.*

Proof. Let $J \trianglelefteq R[X]$. Let $f_1 \in J$ be of minimal minimal degree. If $J = (f_1)$ then done, else choose $f_2 \in J \setminus (f_1)$ of minimal degree. Suppose we have

$$(f_1) \subseteq (f_1, f_2) \subseteq \cdots$$

as an ascending chain of non-stabilising ideas. Let $a_i \in R$ be the coefficient of the largest power of X in f_i and consider

$$(a_1) \subseteq (a_1, a_2) \subseteq \cdots \trianglelefteq R.$$

As R is Noetherian this chain stabilises, i.e. there exists $m \in \mathbb{N}$ such that all a_i's lie in $(a_1, \dots, a_m)$. In particular, $a_{m+1} = \sum_{i=1}^m a_i b_i$ for some $b_i \in R$. Let

$$g = \sum_{i=1}^m b_i f_i X^{\deg f_{m+1} - \deg f_i}$$

which has leading term

$$\sum_{i=1}^m b_i a_i X^{\deg f_{m+1}} = a_{m+1} X^{\deg f_{m+1}}.$$

Thus $\deg(f_{m+1} - g) < \deg f_{m+1}$. But $g \in (f_1, \dots, f_m)$ but $f_{m+1} \notin (f_1, \dots, f_m)$ so $f_{m+1} - g \notin (f_1, \dots, f_m)$. This contradicts the minimality of the degree of f_{m+1}. $\square$

Example. $\mathbb{Z}[X_1, \dots, X_n]$, $\mathbb{F}[X_1, \dots, X_n]$ are Noetherian.

Lemma 2.38. *A quotient of a Noetherian ring is Noetherian.*

Corollary 2.39. *Any ring which may be generated by finitely many elements is Noetherian.*

Example (Non-example)**.** $\mathbb{Z}[X_1, X_2, \dots]$ is *not* Noetherian since

$$(X_1) \subseteq (X_1, X_2) \subseteq \cdots$$

is an non-stabilising ascending chain.

Remark. Suppose $\mathcal{F} \subseteq \mathbb{F}[X_1, \dots, X_n]$ is a set of polynomials. $\alpha = (a_1, \dots, a_n) \in \mathbb{F}^n$ is a solution of $\mathcal{F}$ if and only if $\mathcal{F}$ is contained in the kernel of

$$\begin{aligned} \varphi_a : \mathbb{F}[X_1, \dots, X_n] &\to \mathbb{F} \\ X_i &\mapsto a_i \end{aligned}$$

As $\mathbb{F}[X_1, \dots, X_n]$ is Noetherian, $(\mathcal{F}) = (f_1, \dots, f_m)$ for finitely many f_i's. α is a simultaneous solution to $\mathcal{F}$ if and only if $\ker \varphi_\alpha \supseteq (\mathcal{F}) = (f_1, \dots, f_m)$, if and only if α is a simultaneous solution to $f_1, \dots, f_n$. That is to say, we only have to consider a finite family of polynomials of which α is a root. This is important in algebraic geometry.

3 Modules

3.1 Definitions

Definition (Module)**.** Let R be a commutative ring. A quadruple $(M, +, 0_M, \cdot)$ is an *R-module* if $(M, +, 0_M)$ is an abelian group and the operation $- \cdot - : R \times M \to M$ satisfies

- $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$,
- $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$,
- $r_2 \cdot (r_1 \cdot m) = (r_2 r_2) \cdot m$,
- $1_R \cdot m = m$.

Example.

1. If $R = \mathbb{F}$ is a field then an R-module is precisely an $\mathbb{F}$-vector space.
2. For any ring R, $R^n = \underbrace{R \times \cdots \times R}_{n \text{ times}}$ is an $\mathbb{R}$-module via
$$r \cdot (r_1, \dots, r_n) = (rr_1, \dots, rr_n).$$
In particular for $n = 1$, R is an R-module.
3. If $I \trianglelefteq R$ then I is an R-module via
$$r \cdot a = ra \in I.$$
Also R/I is an $\mathbb{R}$-module via
$$r \cdot (r_1 + I) = rr_1 + I \in R/I.$$
4. For $R = \mathbb{Z}$, an $\mathbb{R}$-module is precisely an abelian group. This is because the axiom for $\cdot$ says that
$$\begin{aligned} - \cdot - : \mathbb{Z} \times M &\to M \\ (n, m) &\mapsto \begin{cases} \underbrace{m + \cdots + m}_{n \text{ times}} & n \geq 0 \\ -(\underbrace{m + \cdots + m}_{n \text{ times}}) & n < 0 \end{cases} \end{aligned}$$
so $\cdot$ is determined by the abelian structure on M.
5. Let $\mathbb{F}$ be a field and V be a vector space over $\mathbb{F}$. Let $\alpha : V \to V$ be a linear map. Then we can make V into an $\mathbb{F}[X]$-module via
$$\begin{aligned} \mathbb{F}[X] \times V &\to V \\ (f, v) &\mapsto f(\alpha)(v) \end{aligned}$$
Different α's make V into different $\mathbb{F}[x]$-modules.
6. Restriction of scalars: if $\varphi : R \to S$ is a ring homomorphism and M is an S-module, then M becomes an R-modules via
$$r \cdot_R m = \varphi(r) \cdot_s m.$$

Definition (Submodule)**.** If M is an $\mathbb{R}$-module, $N \subseteq M$ is a *submodule* if N is a subgroup of $(M, +, 0_M)$ and for any $n \in N, r \in R$, $r \cdot n \in N$. Write $N \leq M$.

Example. A subset of R is a submodule if and only if it is an ideal.

Definition (Quotient module)**.** If $N \leq M$ is a submodule, the *quotient module* M/N is the set of N-cosets in $(M, +, 0_M)$, i.e. the quotient abelian group with

$$r \cdot (m + N) = r \cdot m + N.$$

Definition (Homomorphism)**.** A function $f : M \to N$ is an $\mathbb{R}$-*module homomorphism* if it is a homomorphism of abelian groups and $f(r \cdot m) = r \cdot f(m)$.

Example. If $R = \mathbb{F}$ is a field and V and W are $\mathbb{F}$-modules (i.e. $\mathbb{F}$-vector spaces), then a map is an $\mathbb{F}$-module homomorphism if and only if it is an $\mathbb{F}$-linear map.

Theorem 3.1 (1st Isomorphism Theorem)**.** *If $f : M \to N$ is an R-module homomorphism then*

$$\ker f = \{m \in M : f(m) = 0\} \leq M$$
$$\operatorname{Im} f = \{n \in N : n = f(m)\} \leq N$$

and

$$M/\ker f \cong \operatorname{Im} f.$$

Theorem 3.2 (2nd Isomorphism Theorem)**.** *Let $A, B \leq M$ be submodules. Then*

$$A + B = \{m \in M : m = a + b, a \in A, b \in B\} \leq M$$
$$A \cap B \leq M$$

and

$$(A + B)/A \cong B/(A \cap B).$$

Theorem 3.3 (3rd Isomorphism Theorem)**.** *Let $N \leq L \leq M$ be a chain of submodules. Then*

$$\frac{M/N}{L/N} \cong M/L.$$

Definition (Annihilator)**.** If M is an R-module and $m \in M$, the *annihilator* of m is

$$\operatorname{Ann}(m) = \{r \in R : r \cdot m = 0_M\} \trianglelefteq R.$$

The *annihilator* of M is

$$\operatorname{Ann}(M) = \bigcap_{m \in M} \operatorname{Ann}(m) \trianglelefteq R.$$

Definition (Generated submodule)**.** If M is an R-module and $m \in M$, the *submodule generated by* m is

$$Rm = \{r \cdot m \in M : r \in R\}.$$

Note. Intuitively, the annihilator of an element is the stabiliser of a ring action and that of a module is the kernel. We also have

$$Rm \cong R / \operatorname{Ann}(m).$$

Definition (Finitely generated)**.** M is *finitely generated* if there are $m_1, \dots, m_n \in M$ such that

$$M = Rm_1 + \dots Rm_n = \{r_1 m_1 + \dots + r_n m_n : r_i \in R\}.$$

Lemma 3.4. *An R-module M is finitely generated if and only if there is a surjection $\varphi : R^n \twoheadrightarrow M$ for some n.*

Proof.

- $\Rightarrow$: Suppose $M = Rm_1 + \dots + Rm_n$. Define

$$\begin{aligned} \varphi : R^n &\to M \\ (r_1, \dots, r_n) &\mapsto r_1 m_1 + \dots + r_n m_m \end{aligned}$$

  This is an R-module homomorphism and is surjective.

- $\Leftarrow$: Let $m_i = \varphi((0, \dots, 0, 1, 0, \dots, 0))$ with 1 in the ith position. Then

$$\begin{aligned} \varphi((r_1, \dots, r_n)) &= \varphi((r_1, 0, \dots, 0) + \dots + (0, \dots, 0, r_n)) \\ &= \varphi((r_1, 0, \dots, 0)) + \dots + \varphi((0, \dots, 0, r_n)) \\ &= r_1 \varphi((1, 0, \dots, 0)) + \dots + r_n \varphi((0, \dots, 0, 1)) \\ &= r_1 m_1 + \dots + r_n m_n \end{aligned}$$

  As φ is surjective, $M = Rm_1 + \dots + Rm_n$.

□

Corollary 3.5. *Let M be an R-module and $N \leq M$. If M is finitely generated the so is M/N.*

Proof.

$$R^n \xrightarrow{f} M \xrightarrow{\pi} M/N.$$

□

Note. A submodule of a finitely generated R-module need *not* be finitely generated. For example,

$$(X_1, X_2, \dots) \trianglelefteq \mathbb{Z}[X_1, X_2, \dots] = R$$

is an R-module but not finitely generated, as otherwise it would be a finitely generated ideal.

Example. For $\alpha \in \mathbb{C}$, α is an algebraic integer if and only if $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module.

3.2 Direct Sums and Free Modules

Definition (Direct sum)**.** If $M_1, \dots, M_k$ are R-modules, the *direct sum* $M_1 \oplus \cdots \oplus M_k$ is the set $M_1 \times \cdots \times M_k$ with addition

$$(m_1, \dots, m_k) + (m_1', \dots, m_k') = (m_1 + m_1', \dots, m_k + m_k')$$

and R-module structure

$$r \cdot (m_1, \dots, m_k) = (rm_1, \dots, rm_k).$$

Example.

$$R^n = \underbrace{R \oplus \cdots \oplus R}_{n \text{ times}}.$$

Definition (Independence)**.** Let $m_1, \dots m_k \in M$. They are *independent* if

$$\sum_i r_i \cdot m_i = 0$$

implies that $r_i = 0$ for all $1 \le i \le k$.

Definition (Free generation)**.** A subset $S \subseteq M$ *generates M freely* if

1. S generates M.
2. Any function $\psi : S \to N$ to an R-module N extends to an R-module homomorphism $\theta : M \to N$.

$$\begin{tikzcd} S \arrow[r, hook] \arrow[dr, "\psi"'] & R^S \arrow[d, dashed, "\theta"] \\ & N \end{tikzcd}$$

Note. We can show this extension is unique: given $\theta_1, \theta_2 : M \to N$ two extensions of ψ, $\theta_1 - \theta_2 : M \to N$ is an R-module homomorphism so $\ker(\theta_1 - \theta_2) \le M$. But θ_1, θ_2 both extend ψ so $S \subseteq \ker(\theta_1 - \theta_2)$. As S generates M, $M \le \ker(\theta_1 - \theta_2)$ so $\theta_1 = \theta_2$.

An R-module which is freely generated by $S \subseteq M$ is said to be *free* and S is called a *basis*.

Proposition 3.6. *For a finite subset $S = \{m_1, \dots, m_k\} \subseteq M$, TFAE:*

1. *M is freely generated by S.*
2. *M is generated by S and S is independent.*
3. *Every $m \in M$ can be written as $r_1 m_1 + \dots + r_k m_k$ for some unique $r_i \in R$.*

Proof.

- $1 \Rightarrow 2$: Let S generate M freely. If S is not independent, then there is a non-trivial relation
$$\sum_{i=1}^{k} r_i m_i = 0$$
with $r_j \neq 0$. Let
$$\begin{aligned} \psi : S &\to R \\ m_i &\mapsto \begin{cases} 0_R & i \neq j \\ 1_R & i = j \end{cases} \end{aligned}$$
This extends to an R-module homomorphism $\theta : M \to R$. Then
$$0 = \theta(0) = \theta\left(\sum r_i m_i\right) = \sum r_i \theta(m_i) = r_j.$$
Absurd. Thus S is independent.
- The other steps follow similarly from those in IB Linear Algebra.

□

Example. Unlike vector spaces, a minimal generating set need not be independent. For example $\{2, 3\} \subseteq \mathbb{Z}$ generates $\mathbb{Z}$ but is not linear independent as $(-3) \cdot 2 + (2) \cdot 3 = 0$.

However, like vector spaces, in case a module is freely generated, it is isomorphic to direct sums of copies of the ring:

Lemma 3.7. *If $S = \{m_1, \dots, m_k\} \subseteq M$ freely generates M then*
$$M \cong R^k$$
as an R-module.

Proof. This is entirely analogous to vector spaces. Let
$$\begin{aligned} f : R^k &\to M \\ (r_1, \dots, r_k) &\mapsto \sum_i r_i m_i \end{aligned}$$
It is surjective as S generates M and injective as m_i's are independent. □

If an R-module is generated by $m_1, \dots, m_k$, we have seen before that there is a surjection $f : R^k \twoheadrightarrow M$. We define

Definition (Relation module)**.** The *relation module* for the generators is

$$\ker f \leq R^k.$$

As $M \cong R^k / \ker f$, knowing M is equivalent to knowing the relation module.

Definition (Finitely presented)**.** M is *finitely presented* if there is a finite generating set $m_1, \dots, m_k$ for which the associated relation module is finitely generated.

Let $\{n_1, \dots, n_r\} \subseteq \ker f \leq R^k$ be a set of generators. Then

$$n_i = (r_{i1}, r_{i2}, \dots, r_{ik})$$

and M is generated by $m_1, \dots, m_k$ subject to relations

$$\sum_{j=1}^{k} r_{ij} m_j = 0$$

for $1 \leq i \leq r$.

Proposition 3.8 (Invariance of Dimension)**.** *If $R^n \cong R^m$ then $n = m$.*

Note. This does not hold in general for modules over non-commutative rings.

Proof. As a general strategy, let $I \trianglelefteq R$. Then

$$IM = \left\{ \sum a_i m_i : a_i \in I, m_i \in M \right\} \leq M$$

is a submodule as

$$r \cdot \sum a_i m_i = \sum (r a_i) m_i \in IM.$$

Thus we have a quotient R-module M/IM. We can make this into an R/I-module via

$$(r + I) \cdot (m + IM) = rm + IM.$$

Let $I \trianglelefteq R$ be a maximal proper ideal (this requires Zorn's Lemma). Then R/I is a field and therefore $R^n \cong R^m$ implies

$$R^n / IR^n \cong R^m / IR^m$$
$$(R/I)^n \cong (R/I)^m$$

This is a vector space isomorphism so $n = m$. ☐

We have classified all finite abelian groups (well, at least we claimed so), i.e. $\mathbb{Z}$-modules. What if we want to classify all R-modules? That is going to be the final goal we will build towards.

Recall that M is finitely generated by $m_1, \dots, m_k$ if and only if there is a surjection $f : R^k \twoheadrightarrow M$. M is finitely presentely if and only $\ker f$ is finitely generated, say $n_1, \dots, n_\ell$. Let

$$n_i = (r_{i1}, r_{i2}, \dots, r_{ik})$$

then such an R-module M is determined by the matrix

$$\begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1\ell} \\ r_{r1} & & & \\ \vdots & & \ddots & \\ r_{k1} & & & r_{k\ell} \end{pmatrix} \in \mathcal{M}_{k,\ell}(R).$$

3.3 Matrices over Euclidean Domains

For this section assume R to be a Euclidean domain and let $\varphi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ be the Euclidean function. For $a, b \in R$, we have shown that $\gcd(a, b)$ exists and is unique up to associates. In addition, the Euclidean algorithm shows that $\gcd(a, b) = ax + by$ for some $x, y \in R$.

What follows would be very similar to what we have learned in IB Linear Algebra — in fact identical except a single modification:

Definition (Elementary row operation)**.** *Elementary row operation* on an $m \times n$ matrix with entries in R are

1. Add $\lambda \in R$ times the ith row to the jth row where $i \neq j$. This can be realised by left multiplication by $I + C$ where C is λ in (j, i)th position and 0 elsewhere.
2. Swapping the ith and jth row where $i \neq j$. Realised by left multiplication by
$$\begin{pmatrix} 1 & 0 & \cdots & & & 0 \\ \vdots & \ddots & & & & \vdots \\ & & 0 & & 1 & 0 \\ 0 & \cdots & 0 & \ddots & 0 & 0 \\ & & 1 & 0 & 0 & \\ \vdots & & & \ddots & & \\ 0 & & \cdots & & \cdots & 0 \end{pmatrix}$$
3. Multiply the ith row by a *unit* $c \in R$. Realised by left multiplication by
$$\begin{pmatrix} 1 & 0 & \cdots & & 0 \\ & \ddots & & & \\ \vdots & & c & & \vdots \\ & & & \ddots & \\ 0 & \cdots & & 0 & 1 \end{pmatrix}$$

Definition (Elementary column operation)**.** Defined analogously by replacing "row" with "column".

Similarly to IB Linear Algebra, we define an equivalence relation

Definition (Equivalence)**.** $A, B \in \mathcal{M}_{m,n}(R)$ are *equivalent* if there is a sequence of elementary row and column operations taking A to B.

If A and B are equivalent then there are invertible square matrices P and Q such that
$$B = QAP^{-1}.$$

Theorem 3.9 (Smith Normal Form)**.** *An $n \times m$ matrix over a Euclidean* *domain R is equivalent to*

$$\begin{pmatrix} d_1 & & & & & & \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$$

where the d_i's are non-zero and

$$d_1 \mid d_2 \mid \cdots \mid d_r.$$

Proof. This proof is going to be algorithmic. If the matrix $A = 0$ we are done. Otherwise there is a $A_{ij} \neq 0$. By swapping 1st and ith row, and 1st and jth column we may suppose $A_{11} \neq 0$. We want to reduce $\varphi(A_{11})$ as much as possible. Split into three cases:

- Case 1: if there is a A_{1j} not divisible by A_{11} then have

$$A_{1j} = qA_{11} + r$$

  with $\varphi(r) < \varphi(A_{11})$. Add $-q$ times the 1st column to the jth. This makes the $(1, j)$th entry r. Swap 1st and jth column to get $A_{11} = r$. Thus we have *strictly* decreased the φ value of the $(1, 1)$ entry.

- Case 2: if A_{11} does not divide some A_{i1}, do the analogous to entries in the first column to strictly reduce $\varphi(A_{11})$.

  As $\varphi(A_{11})$ can only strictly decrease finitely many times, after some applications of Case 1 and 2 we can assumes A_{11} divides all the entries in the 1st row and 1st column. If $A_{1j} = qA_{11}$ then we can add $-q$ times the 1st column to the jth row to make the (i, j)th entry 0. Thus we obtain

$$A = \begin{pmatrix} d & 0 \\ 0 & C \end{pmatrix}$$

- Case 3: if there is an entry c_{ij} of C not divisible by d, write

$$c_{ij} = qd + r$$

  where $\varphi(r) < \varphi(d)$. Conduct the following series of elementary operations

$$\begin{pmatrix} d & 0 & \cdots & 0 & \cdots & 0 \\ 0 & & & & & \\ \vdots & & & & & \\ 0 & & & c_{ij} & & \\ \vdots & & & & & \\ 0 & & & & & \end{pmatrix} \xrightarrow{\text{EC 1}} \begin{pmatrix} d & 0 & \cdots & d & \cdots & 0 \\ 0 & & & & & \\ \vdots & & & & & \\ 0 & & & c_{ij} & & \\ \vdots & & & & & \\ 0 & & & & & \end{pmatrix}$$

$$\xrightarrow{\text{ER 1}} \begin{pmatrix} d & 0 & \cdots & d & \cdots & 0 \\ 0 & & & & & \\ \vdots & & & & & \\ -qd & & & r & & \\ \vdots & & & & & \\ 0 & & & & & \end{pmatrix} \xrightarrow{\text{ER 2,EC 2}} \begin{pmatrix} r & * & \cdots & * \\ * & & & \\ \vdots & & * & \\ * & & & \end{pmatrix}$$

Repeat Case 1 and 2, we finally get

$$\begin{pmatrix} d' & \\ & C' \end{pmatrix}$$

where $\varphi(d') < \varphi(d)$.

Eventually we can suppose that d' divides every entry of C'. By induction C' is equivalent to

$$\begin{pmatrix} d_2 & & & & & & \\ & d_3 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$$

with

$$d_2 \mid d_3 \mid \cdots \mid d_r$$

and we must have $d' \mid d_i$ for $i > 1$. □

Remark. The d_i's in Smith Normal Form are unique up to associates.

Certainly Smith Normal Form is a nice form and the algorithm guarantees its existence and uniqueness (up to associates). However, the computation is too cumbersome to be useful. However, if we could prove it is invariant under matrix conjugation, we may apply some clever tricks to extract the d_i's in Smith Normal Form without explicitly computing them.

> **Definition** (Minor)**.** A $k \times k$ *minor* of a matrix A is the determinant of a matrix formed by forgetting all but k rows and k columns of A.

> **Definition** (Fitting ideal)**.** The kth *Fitting ideal* of A $\operatorname{Fit}_k(A) \trianglelefteq R$ is the ideal generated by all $k \times k$ minors of A.

Given a matrix A in Smith Normal Form as above with $d_1 \mid \cdots \mid d_r$, the only $k \times k$ submatrices which do not have a whole row or column 0 are those which keep both i_1th row and i_1th column, both i_2th row and i_2th column, etc. Therefore

$$\begin{aligned} \operatorname{Fit}_k(A) &= \left(\det \begin{pmatrix} d_{i_1} & & & \\ & d_{i_2} & & \\ & & \ddots & \\ & & & d_{i_k} \end{pmatrix} \right) \\ &= (d_{i_1} \cdots d_{i_k} : \text{ sequences } i_1, \dots, i_k) \\ &= (d_1 d_2 \cdots d_k) \end{aligned}$$

as $d_m \mid d_{i_m}$ for all m.

Therefore from the above computation $\operatorname{Fit}_k(A)$ and $\operatorname{Fit}_{k-1}(A)$ determine d_k up to associates.

> **Lemma 3.10.** *If A and B are equivalent matrices then* $\mathrm{Fit}_k(A) = \mathrm{Fit}_k(B)$ *for all k.*

Proof. It amounts to show that elementary operations does not change $\mathrm{Fit}_k(A) \trianglelefteq R$. We do the first type of row operation. Fix a $k \times k$ submatrix C in A. Recall that this row operation adds λ times the ith row to the jth row. Depending on i and j, split into three cases:

- Case 1: if the jth row is not in C then C is unchanged, so is its determinant.
- Case 2: if the ith and jth rows are both in C, the operation changes C by a row operation so its determinant is unchanged.
- Cases 3: if the jth row is in C but the ith is not, suppose wlog the ith row of A corresponding to columns of C has entries $(f_1, f_2, \dots, f_k)$. After the row operation, C is changed to C' whose jth row is

  $$(c_{j,1} + \lambda f_1, c_{j,2} + \lambda f_2, \dots, c_{j,k} + \lambda f_k).$$

  By expansion along the jth row,

  $$\det C' = \det C \pm \lambda \det D$$

  where D is the matrix obtained by replacing the jth row of C with $(f_1, \dots, f_k)$, which is a $k \times k$ submatrix of A up to reordering (which is accounted for by the $\pm$ sign), by multilinearity of det. So $\det C' \in \mathrm{Fit}_k(A)$ as it is a linear combination of minors. Therefore $\mathrm{Fit}_k(A') \subseteq \mathrm{Fit}_k(A)$ where A' is obtained from A by this operation. As row operations are invertible, we must have equality.

The other two types of row operations are similar but easier. Column operations follow analogously. ☐

Example. Let

$$A = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} \in \mathcal{M}_{2,2}(\mathbb{Z}).$$

Algorithmically, we can carry out the following sequence of operations to obtain Smith Normal Form:

$$\begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} \overset{\text{ER 2}}{\to} \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix} \overset{\text{ER 1}}{\to} \begin{pmatrix} 1 & 2 \\ 0 & -5 \end{pmatrix} \overset{\text{ER 1}}{\to} \begin{pmatrix} 1 & 0 \\ 0 & -5 \end{pmatrix} \overset{\text{ER 3}}{\to} \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}$$

Alternatively, using what we have just proved,

$$\begin{aligned} \mathrm{Fit}_1(A) &= (2, -1, 2, 1) = (1) \\ \mathrm{Fit}_2(A) &= (\det A) = (5) \end{aligned}$$

so $d_1 = 1, d_1 d_2 = 5$ so $d_2 = 5$.

Recall that we have remarked that a submodule of a finitely genereated module may not be finitely generated. However the following lemma tells us that submodules of finitely generated free modules over some particular rings are so:

Lemma 3.11. *Let R be a PID. Any submodule of R^n is generated by at most n elements.*

Proof. Let $N \leq R^n$ and consider the ideal

$$I = \{r \in R : \exists r_2, \dots, r_n \text{ such that } (r, r_2, \dots, r_n) \in N\},$$

which is the image of $N \xrightarrow{\iota} R^n \xrightarrow{\pi_1} R$, a submodule of R.

As R is a PID, $I = (a) \trianglelefteq R$ for some $a \in R$. Thus there is some

$$n_1 = (a, a_2, a_2, \dots, a_n) \in N.$$

Suppose $(r_1, r_2, \dots, r_n) \in N$. Then there exists some $x \in R$ such that $r_1 = ax$. Then

$$(r_1, \dots, r_n) - x \cdot n_1 = (0, r_2 - xa_2, \dots, r_n - xa_n) \in N \cap (0 \oplus R^{n-1}).$$

By induction $N \cap (0 \oplus R^{n-1}) \cong N' \leq R^{n-1}$ is generated by $n_2, \dots, n_n$ so $n_1, \dots, n_n$ generate N. ☐

Theorem 3.12. *Let R be a Euclidean domain and $N \leq R^n$. Then there is a basis $v_1, \dots, v_n$ of R^n such that N is generated by $d_1 v_1, \dots, d_r v_r$ for some $0 \leq r \leq n$ and some $d_1 \mid \dots \mid d_r$.*

Proof. By the previous lemma there are $x_1, \dots, x_m \in N$ which generate N and $0 \leq m \leq n$. Each x_i is an element of R^n so we can form an $n \times m$ matrix whose first m columns are x_i, i.e.

$$A = \begin{pmatrix} \uparrow & \uparrow & & \uparrow \\ x_1 & x_2 & \cdots & x_m \\ \downarrow & \downarrow & & \downarrow \end{pmatrix} \in \mathcal{M}_{n,m}(R)$$

We can put A into Smith Normal Form with diagonal entries $d_1 \mid \cdots \mid d_r$ by elementary operations. Each row operation is given by a change of basis of R^n and each column operation is given by rechoosing the generating set $x_1, \dots, x_m$. Thus after a change of basis of R^n to $v_1, \dots, v_n$, N is generated by $d_1 v_1, \dots, d_r v_r$. ☐

Corollary 3.13. *A submodule $N \leq R^n$ is isomorphic to R^m for some $m \leq n$.*

Proof. By the theorem above, we can find a basis $v_1, \dots, v_n$ for R^n such that N is generated by $d_1 v_1, \dots, d_m v_m$. These are linearly independent as a dependence between them would give a dependence between $v_1, \dots, v_n$. ☐

Now we are ready for the big theorem in this course:

Theorem 3.14 (Classification Theorem for Finitely Generated Modules over Euclidean Domain)**.** *Let R be a Euclidean domain and M a finitely generated R-modules. Then*

$$M \cong \frac{R}{(d_1)} \oplus \frac{R}{(d_2)} \oplus \cdots \oplus \frac{R}{(d_r)} \oplus R \oplus \cdots \oplus R$$

for some $d_i \neq 0$ with $d_1 \mid d_2 \mid \cdots \mid d_r$.

Proof. Let M be generated by $m_1, \dots, m_n \in M$, giving a surjection $\varphi : R^n \twoheadrightarrow M$ so $M \cong R^n / \ker \varphi$. By the previous theorem there is a basis $v_1, \dots, v_n$ of R^n such that $\ker \varphi$ is generated by $d_1 v_1, \dots, d_r v_r$ with $d_1 \mid \cdots \mid d_r$. Thus by changing the basis of R^n to v_i's, $\ker \varphi$ is generated by columns of

$$\begin{pmatrix} d_1 & & & & & & \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$$

so

$$M \cong \frac{R^n}{\ker \varphi} \cong \left(\bigoplus_{i=1}^r \frac{R}{(d_i)} \right) \oplus R \oplus \cdots \oplus R$$

as required. □

Example. Let $R = \mathbb{Z}$, a Euclidean domain, and A be the abelian group (i.e. $\mathbb{Z}$-module) generated by a, b, c, subject to

$$\begin{cases} 2a + 3b + c = 0 \\ a + 2b = 0 \\ 5a + 6b + 7c = 0 \end{cases}$$

Thus $A = \mathbb{Z}^3 / N$ where $N \leq \mathbb{Z}^3$ is generated by $(2,3,1)^T, (1,2,0)^T, (5,6,7)^T$. The matrix A whose columns are these vectors

$$A = \begin{pmatrix} 2 & 1 & 5 \\ 3 & 2 & 6 \\ 1 & 0 & 7 \end{pmatrix}$$

has Smith Normal Form with diagonal entries $1, 1, 3$:

Proof.

$$\begin{aligned} \mathrm{Fit}_1(A) &= (1) \\ \mathrm{Fit}_2(A) &\supseteq \left(\det \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} \right) = (1) \\ \mathrm{Fit}_3(A) &= (\det A) = 3 \end{aligned}$$

so $d_1 = 1, d_1 d_2 = 1, d_1 d_2 d_3 = 3$. □

After change of basis, N is generated by $(1,0,0)^T, (0,1,0)^T, (0,0,3)^T$ so

$$A \cong \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}.$$

We can derive, as a corollary actually, what we stated earlier without proof

Theorem 3.15 (Structure Theorem for Finitely Generated Abelian Groups)**.** *Any finitely generated abelian group is isomorphic to*

$$C_{d_1} \times C_{d_2} \times \cdots \times C_{d_r} \times C_\infty \times \cdots \times C_\infty$$

with $d_1 \mid \cdots \mid d_r$*.*

Proof. "Trivial" should suffice here but let us spell it out: apply Classification Theorem for Finitely Generated Modules over Euclidean Domain to $\mathbb{Z}$, and note that

$$\mathbb{Z}/(d) = C_d,\ \mathbb{Z} = C_\infty.$$

□

The above classification theorem decompose into modules whose relation modules' principal ideals form a descending chain by divisibility. It turns out it is also possible to decompose by the coprime factors of the relation modules. Before that let us prove something we have known for a (very) long time, but at a higher level:

Lemma 3.16 (Chinese Remainder Theorem)**.** *Let R be a Euclidean domain and $a, b \in R$ with* $\gcd(a, b) = 1$*. Then*

$$R/(ab) \cong R(a) \oplus R/(b).$$

Proof. Consider the R-module homomorphism

$$\begin{aligned} \varphi : R/(a) \oplus R/(b) &\to R/(ab) \\ (r_1 + (a), r_2 + (b)) &\mapsto br_1 + ar_2 + (ab) \end{aligned}$$

As $\gcd(a, b) = 1$, $(a, b) = (1)$ so $1 = xa + yb$ for some $x, y \in R$. Therefore for $r \in R$, $r = rxa + ryb$ so

$$r + (ab) = rxa + ryb + (ab) = \varphi((ry + (a), rx + (b)))$$

and so φ is surjective.

If $\varphi((r_1 + (a), r_2 + (b))) = 0$ then $br_1 + ar_2 \in (ab)$. Thus $a \mid br_1 + ar_2, a \mid br_1$. As $\gcd(a, b) = 1$, $a \mid r_1$ so $r_1 + (a) = 0 + (a)$. Similarly $r_2 + (b) = 0 + (b)$ so φ is injective. □

We thus have

Theorem 3.17 (Primary Decomposition Theorem)**.** *Let R be a Euclidean domain and M be a finitely generated R-module. Then*

$$M \cong \bigoplus_{i=1}^{n} N_i$$

with each N_i either equal to R or $R/(p^m)$ for some prime $p \in R$ and $n \geq 1$.

Proof. Note that if $d = p_1^{m_1} \cdots p_k^{m_k}$ with $p_i \in R$ distinct primes, by the previous lemma

$$\frac{R}{(d)} \cong \frac{R}{(p_1^{n_1})} \oplus \cdots \oplus \frac{R}{(p_k^{m_k})}.$$

Plug this into Classification Theorem for Finitely Generated Modules over Euclidean Domain to get the required result. □

3.4 $\mathbb{F}[X]$-modules and Normal Form

For any field $\mathbb{F}$, $\mathbb{F}[X]$ is a Euclidean domain and so results of the last section apply. If V is an $\mathbb{F}$-vector space and $\alpha : V \to V$ is an endomorphism, then we have

$$\begin{aligned} \mathbb{F}[X] \times V &\to V \\ (f, v) &\mapsto f(\alpha)(v) \end{aligned}$$

which makes V into an $\mathbb{F}[X]$-module, call it V_α. It turns out that $\mathbb{F}[X]$-module is the correct tool to study endomorphisms and many results in IB Linear Algebra, as well as many further results in algebra, can be obtained by looking into the $\mathbb{F}[X]$-module structure.

Lemma 3.18. *If V is finite-dimensional then V_α is finitely generated as an $\mathbb{F}[X]$-module.*

Proof. V is a finitely generated $\mathbb{F}$-module and $\mathbb{F} \leq \mathbb{F}[X]$ so V is also a finitely generated $\mathbb{F}[X]$-module. □

Example.

1. Suppose $V_\alpha \cong \mathbb{F}[X]/(X^r)$ as an $\mathbb{F}[X]$-module. This has $\mathbb{F}$-basis $\{X^i\}_{i=0}^{r-1}$ and the action of α corresponds to multiplication by X. Thus in this basis α has matrix representation

$$\begin{pmatrix} 0 & & & & \\ 1 & 0 & & & \\ & 1 & 0 & & \\ & & & \ddots & \\ & & & 1 & 0 \end{pmatrix}$$

2. Suppose $V_\alpha \cong \mathbb{F}[X]/((X-\lambda)^r)$. Consider $\beta = \alpha - \lambda \cdot \mathrm{id}$. Then $V_\beta \cong \mathbb{F}[Y]/(Y^r)$ as an $\mathbb{F}[Y]$-module. By the previous example V has a basis so that β is given by the matrix above and α is given by

$$\begin{pmatrix} \lambda & & & & \\ 1 & \lambda & & & \\ & 1 & \lambda & & \\ & & & \ddots & \\ & & & 1 & \lambda \end{pmatrix}$$

3. Suppose $V_\alpha \cong \mathbb{F}[X]/(f)$ where

$$f = X^r + a_{r-1}X^{r-1} + \cdots + a_1 X + a_0.$$

Then $\{X^i\}_{i=0}^{r-1}$ is an $\mathbb{F}$-basis and in this basis α is given by

$$\begin{pmatrix} 0 & & & & & -a_0 \\ 1 & 0 & & & & -a_1 \\ & 1 & 0 & & & -a_2 \\ & & 1 & 0 & & -a_3 \\ & & & & \ddots & \vdots \\ & & & & 1 & -a_{r-1} \end{pmatrix}$$

This matrix is called the *companion matrix* for f, written $C(f)$.

Theorem 3.19 (Rational Canonical Form)**.** *Let V be a finite-dimensional $\mathbb{F}$-vector space and $\alpha : V \to V$ be linear. Regard V as an $\mathbb{F}[X]$-module V_α, we have*

$$V_\alpha \cong \frac{\mathbb{F}[X]}{(d_1)} \oplus \cdots \oplus \frac{\mathbb{F}[X]}{(d_r)}$$

with $d_1 \mid d_2 \mid \cdots \mid d_r$. There is a basis of V with respect to which α is given by

$$\begin{pmatrix} C(d_1) & & & \\ & C(d_2) & & \\ & & \ddots & \\ & & & C(d_r) \end{pmatrix}$$

Proof. Apply Classification Theorem for Finitely Generated Modules over Euclidean Domain to $\mathbb{F}[X]$, a Euclidean domain. Note that no copies of $\mathbb{F}[X]$ appear as it has infinite dimension over V. □

Some observations:

1. If α is represented by a matrix A in some basis, then A is conjugate to the above matrix.
2. The minimal polynomial of α is $d_r \in \mathbb{F}[X]$.
3. The characteristic polynomial of α is $d_1 d_2 \cdots d_r$.

Recall that we have two classification theorems for modules over Euclidean domain. The above theorem corresponds to invariant decomposition. One might naturally ask what result follows from primary decomposition. Before that let's convince ourselves that primes in $\mathbb{C}[X]$ are as simple as they can be:

Lemma 3.20. *The primes in $\mathbb{C}[X]$ are $X - \lambda$ for $\lambda \in \mathbb{C}$ up to associates.*

Proof. If $f \in \mathbb{C}[X]$ is irreducible then Fundamental Theorem of Algebra says that f has a root λ, or f is a constant. If it is constant then it is 0 or a unit, absurd. Thus $(X - \lambda) \mid f$, write $f = (X - \lambda)g$. But f is irreducible so g is a unit. Thus f is an associate of $X - \lambda$. □

Remark. The lemma is equivalent to the statement that $\mathbb{C}$ is algebraically closed, which says that every polynomial with coefficients in $\mathbb{C}$ factorises into linear factors over $\mathbb{C}$. In fact, every field can be extended to an algebraically closed one. This will be discussed in detail in IID Galois Theory.

Theorem 3.21 (Jordan Normal Form)**.** *Let V be a finite-dimensional $\mathbb{C}$-vector space and $\alpha : V \to V$ linear. Consider V_α as an $\mathbb{C}[X]$-module, then*

$$V_\alpha \cong \frac{\mathbb{C}[X]}{((X-\lambda_1)^{a_1})} \oplus \frac{\mathbb{C}[X]}{((X-\lambda_2)^{a_2})} \oplus \cdots \oplus \frac{\mathbb{C}[X]}{((X-\lambda_r)^{a_r})}$$

where the λ_i's are not necessarily distinct. There is a basis of V with respect to which α is given by

$$\begin{pmatrix} J_{a_1}(\lambda_1) & & & \\ & J_{a_2}(\lambda_2) & & \\ & & \ddots & \\ & & & J_{a_r}(\lambda_r) \end{pmatrix}$$

where

$$J_m(\lambda) = \begin{pmatrix} \lambda & & & & \\ 1 & \lambda & & & \\ & 1 & \lambda & & \\ & & & \ddots & \\ & & & 1 & \lambda \end{pmatrix}$$

has size m.

Proof. Immediate from Primary Decomposition Theorem and knowing all the primes in $\mathbb{C}[X]$. ☐

Remark.

1. The $J_m(\lambda)$ are called *Jordan λ-blocks.*
2. The minimal polynomial of α is
$$m_\alpha(t) = \prod_\lambda (X-\lambda)^{a_\lambda}$$
where a_λ is the largest λ-block.
3. The characteristic polynomial of α is
$$\chi_\alpha(t) = \prod_\lambda (X-\lambda)^{b_\lambda}$$
where b_λ is the sum of the sizes of the λ-blocks.
4. Consider $\ker(X \cdot - : V_\alpha \to V_\alpha)$. What is its dimension?
On $\mathbb{C}[X]/(X-\lambda)^a$, if $\lambda \neq 0$ then the map $X \cdot -$ is an isomorphism since
$$\ker(X \cdot -) = \{f + ((X-\lambda)^a) : Xf \in ((X-\lambda)^a)\}$$
so if $Xf = (X-\lambda)^a \cdot g$, as X and $X-\lambda$ are coprime, $X \mid g$, $(X-\lambda)^a \mid f$ so $\ker(X \cdot -) = 0$.
If $\lambda = 0$, $X \cdot - : \mathbb{C}[X]/(X^a) \to \mathbb{C}[X]/(X^a)$ has matrix
$$\begin{pmatrix} 0 & & & & \\ 1 & 0 & & & \\ & 1 & 0 & & \\ & & & \ddots & \\ & & & 1 & 0 \end{pmatrix}$$

so 1-dimensional kernel. Thus

$$\dim\ker(X\cdot - : V_\alpha \to V_\alpha) = \#\text{Jordan 0-blocks}.$$

5. Similarly, $X^2\cdot - : \mathbb{C}[X]/((X-\lambda)^a) \to \mathbb{C}[X]/((X-\lambda)^a)$ is an isomorphism for $\lambda \neq 0$ and for $\lambda = 0$ is given by the matrix

$$\begin{pmatrix} 0 & & & & \\ 0 & 0 & & & \\ 1 & 0 & 0 & & \\ & 1 & 0 & & \\ & & & \ddots & \\ & & & & 0 \end{pmatrix}$$

which has 2-dimensional kernel if $a > 1$ and 1-dimensional kernel if $a = 1$. Therefore

$$\begin{aligned}\dim\ker(X^2\cdot - : V_\alpha \to V_\alpha) = \#&\text{Jordan 0-blocks}\\ &+ \#\text{Jordan 0-blocks of size} > 1.\end{aligned}$$

so

$$\#\text{Jordan 0-blocks of size } 1 = 2\dim\ker(X\cdot -) - \dim\ker(X^2\cdot -).$$

Using the same method we can find Jordan 0-blocks of other sizes.

3.5 Conjugacy*

Lemma 3.22. *If $\alpha : V \to V$ and $\beta : W \to W$ are endomorphism of $\mathbb{F}$-vector spaces, then $V_\alpha \cong W_\beta$ as $\mathbb{F}[X]$-modules if and only if there is an isomorphism $\gamma : V \to W$ such that*

$$\gamma^{-1}\beta\gamma = \alpha,$$

i.e. α and β are conjugates.

Proof. Let $\hat{\gamma} : V_\alpha \to W_\beta$ be an $\mathbb{F}[X]$-module isomorphism. In particular $\hat{\gamma}$ gives an $\mathbb{F}$-vector space isomorphism $\gamma : V \to W$. Then

$$\begin{aligned}\beta\circ\gamma : W_\beta &\to W_\beta\\ v &\mapsto X\cdot\gamma(v)\end{aligned}$$

Now

$$\begin{aligned}X\cdot\gamma(v) &= X\cdot\hat{\gamma}(v) \text{ } \hat{\gamma} \text{ as an } \mathbb{F}[X]\text{-module map}\\ &= \hat{\gamma}(X\cdot v) \text{ in } \mathbb{F}[X]\text{-module } V_\alpha\\ &= \hat{\gamma}(\alpha(v))\\ &= \gamma(\alpha(v))\end{aligned}$$

so $\beta\circ\gamma = \gamma\circ\alpha$, $\gamma^{-1}\circ\beta\circ\gamma = \alpha$. Therefore if $W = V$ then $V_\alpha \cong V_\beta$ if and only if α and β are conjugates.

$$\begin{tikzcd} V \arrow[r, "\alpha"] \arrow[d, dashed, "\gamma"'] & V \arrow[d, dashed, "\gamma"] \\ W \arrow[r, "\beta"] & W \end{tikzcd} \qquad \begin{tikzcd} V_\alpha \arrow[r, dashed, "\alpha = X\cdot -"] \arrow[d, "\hat{\gamma}"'] & V_\alpha \arrow[d, "\hat{\gamma}"] \\ W_\beta \arrow[r, dashed, "\beta = X\cdot -"] & W_\beta \end{tikzcd}$$

□

Applying Classification Theorem for Finitely Generated Modules over Euclidean Domain, we get

Corollary 3.23. *There is a bijection*

$$\{\textit{conjugacy class of } \mathcal{M}_n(\mathbb{F})\} \leftrightarrow \left\{ \begin{array}{c} \textit{sequence of monic polynomials } d_1, \dots, d_r \\ \textit{where } d_1 \mid \cdots \mid d_r \textit{ and } \deg(d_1 \cdots d_r) = n \end{array} \right\}$$

Example. Consider $\mathrm{GL}_2(\mathbb{F})$. The conjugacy classes are described by $d_1 \mid \cdots \mid d_r$ where $\deg(d_1 \cdots d_r) = 2$. Therefore we have one of the followings:

1. $\deg d_1 = 2$,
2. $\deg d_1 = \deg d_2 = 1$. As $d_1 \mid d_2$, $d_1 = d_2$.

These give us respecively

1. $\mathbb{F}[X]/(X^2 + a_1 X + a_0)$,
2. $\mathbb{F}[X]/(X - \lambda) \oplus \mathbb{F}[X]/(X - \lambda)$.

Therefore any $A \in \mathrm{GL}_2(\mathbb{F})$ is conjugate to one of

$$\begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix}, \quad \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$$

They are not conjugates.

The first case be futher split into two cases. If $X^2 + a_1 X + a_0$ is reducible they it factorises as either $(X - \lambda)^2$ or $(X - \lambda)(X - \mu)$ where $\lambda \neq \mu$. Thus we get one of

$$\begin{pmatrix} \lambda & 0 \\ 1 & \lambda \end{pmatrix}, \quad \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$$

Example. Let $\mathbb{F} = \mathbb{Z}/3\mathbb{Z}$. For what a_1, a_0 is $X^2 + a_1 X + a_0 \in \mathbb{F}[X]$ irreducible? There are $3 \times 3 = 9$ polynomials in total, of which $\binom{3}{1} + \binom{3}{2} = 6$ are reducible. Guess (any verify!) that the irreducibles are $X^2 + 1, X^2 + 2X + 2, X^2 + 2X + 2$. Therefore the conjugacy classes in $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ are

$\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 & -2 \\ 1 & -1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 & -2 \\ 1 & -2 \end{smallmatrix}\right)$
$\left(\begin{smallmatrix} \lambda & 0 \\ 1 & \lambda \end{smallmatrix}\right)$	$\lambda \neq 0$	
$\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$	$\lambda, \mu \neq 0$	

so there are in total 8 conjugacy classes. They have order

$\left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 & 1 \\ 1 & 2 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 2 & 0 \\ 1 & 2 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$
4	8	8	3	6	2

Just for fun, let's use what we deduced above and knowledge about Sylow p-subgroups way back in the beginning of the course to determine the group structure of $\mathrm{GL}_2(\mathbb{Z}/3/Z)$.

Recall that

$$|GL_2(\mathbb{Z}/3\mathbb{Z})| = (3^2 - 1)(3^2 - 3) = 2^4 \cdot 3$$

so the Sylow 2-subgroup has order $2^4 = 16$. There are no elements of order 16 so it cannot be cyclic. Let

$$A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$$

so

$$A^{-1}BA = \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix} = B^3.$$

Therefore $\langle B \rangle \trianglelefteq \langle A, B \rangle \leq \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. The 2nd Isomorphism Theorem says that

$$\langle A, B \rangle / \langle B \rangle \cong \langle A \rangle / (\langle A \rangle \cap \langle B \rangle).$$

Now $\langle A \rangle \cap \langle B \rangle = \langle \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix} \right) \rangle$, a group of order 2. Therefore

$$|\langle A, B \rangle| = \frac{|\langle A \rangle| \cdot |\langle B \rangle|}{|\langle A \rangle \cap \langle B \rangle|} = \frac{8 \cdot 4}{2} = 16$$

which is a Sylow 2-subgroup of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. It has presentation

$$\langle A, B | A^4 = B^8 = 1, A^{-1}BA = B^3 \rangle,$$

the semidihedral group of order 16.

Since we still have time left, we can do one more fun example.

Example. Let $R = \mathbb{Z}[X]/(X^2+5) \cong \mathbb{Z}[\sqrt{-5}] \leq \mathbb{C}$. Then

$$(1+X)(1-X) = 1 - X^2 = 1 + 5 = 6 = 2 \cdot 3.$$

As $1 \pm X, 2$ and 3 are irreducibles R is *not* a UFD. Let

$$I_1 = (3, 1+X), I_2 = (3, 1-x)$$

be submodules of R. Consider

$$\begin{aligned} \varphi : I_1 \oplus I_2 &\to R \\ (a, b) &\to a + b \end{aligned}$$

Then $\operatorname{Im} \varphi = (3, 1+X, 1-X)$. Since $3 - (1+X) - (1-X) = 1$, $\operatorname{Im} \varphi = R$. Also

$$\ker \varphi = \{(a, b) \in I_1 \oplus I_2 : a + b = 0\} \cong I_1 \cap I_2$$

where the last isomorphism can be deduced from the map $(x, -x) \leftarrow\!\shortmid x$. Note that $(3) \subseteq I_1 \cap I_2$. Let

$$s \cdot 3 + t \cdot (1+X) \in (3, 1-X) \subseteq R = \mathbb{Z}[X]/(X^2-5).$$

Reduce mod 3, we get

$$t \cdot (1+X) = (1-X)p \mod (3, X^2+5) = (3, X^2-1) = (2, (X+1)(X-1))$$

so $1 - X \mid t$, $(1+X)(1-X) \mid t(1+X)$ so

$$t(1+X) = q(X^2-1) = q(X^2+5-6) = 3(-2q).$$

Then $s \cdot 3 + t \cdot (1+X)$ is divisible by 3 so $I_1 \cap I_2 \subseteq (3)$. Equality follows.

From example sheet 4 we know that if $N \leq M$ and $M/N \cong \mathbb{R}^n$ then $M \cong N \oplus R^n$. Here

$$I_1 \oplus I_2 / \ker \varphi \cong \operatorname{Im} \varphi = R$$

so

$$I_1 \oplus I_2 \cong R \oplus \ker \varphi = R \oplus (3).$$

Consider

$$\begin{aligned} \psi : R &\to (3) \\ x &\mapsto 3x \end{aligned}$$

a surjective R-module map. $\ker \varphi = 0$ as R is an integral domain so φ is an isomorphism. Thus

$$I_1 \oplus I_2 \cong R \oplus R = R^2.$$

In particular this shows that sums of non-free modules can be free.

Next we claim that I_1 is not principal. If $I_1 = (a + bX)$ then $I_2 = (a + bX)$. This is because $I_1 = (3, 1+X)$ and $I_2 = (3, 1-X)$ and R has automorphism $X \mapsto -X$ which interchanging I_1 and I_2.[1] But then

$$(3) = I_1 \cap I_2 = ((a + bX)(a - bX)) = (a^2 - b^2 X^2) = (a^2 + 5b^2)$$

so $a^2 + 5b^2 \mid 3$, absurd.

In summary, we have shown that

1. I_1 needs 2 elements to generate (as it is not principal), but it is not the free module R^2.
2. I_1 is a direct summand of R^2.

[1] This technique will play a central role in IID Galois Theory.

Index