Part IB — GRM

Based on lectures by Dr R Zhou and notes by thirdsgames.co.uk

Lent 2022

Contents

Part I
Groups

§0 Review of IA Groups

This section contains material covered by IA Groups.

§0.1 Definitions

A *group* is a pair $(G, \cdot)$ where G is a set and $\cdot : G \times G \to G$ is a binary operation on G, satisfying

- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
- there exists $e \in G$ such that for all $g \in G$, we have $g \cdot e = e \cdot g = g$; and
- for all $g \in G$, there exists an inverse $h \in G$ such that $g \cdot h = h \cdot g = e$.

Remark 1.
1. Sometimes, such as in IA Groups, a closure axiom is also specified. However, this is implicit in the type definition of $\cdot$. In practice, this must normally be checked explicitly.
2. Additive and multiplicative notation will be used interchangeably. For additive notation, the inverse of g is denoted $-g$, and for multiplicative notation, the inverse is instead denoted g^{-1}. The identity element is sometimes denoted 0 in additive notation and 1 in multiplicative notation.

A subset $H \subseteq G$ is a *subgroup* of G, written $H \leq G$, if $h \cdot h' \in H$ for all $h, h' \in H$, and $(H, \cdot)$ is a group. The closure axiom must be checked, since we are restricting the definition of $\cdot$ to a smaller set.

Remark 2. A non-empty subset $H \subseteq G$ is a subgroup of G if and only if

$$a, b \in H \implies a \cdot b^{-1} \in H$$

An *abelian* group is a group such that $a \cdot b = b \cdot a$ for all a, b in the group. The *direct product* of two groups G, H, written $G \times H$, is the group over the Cartesian product $G \times H$ with operation $\cdot$ defined such that $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2)$.

§0.2 Cosets

Let $H \leq G$. Then, the *left cosets* of H in G are the sets gH for all $g \in G$. The set of left cosets partitions G. Each coset has the same cardinality as H. Lagrange's theorem states that if G is a finite group and $H \leq G$, we have $|G| = |H| \cdot [G\colon H]$, where $[G\colon H]$ is the number of left cosets of H in G. $[G\colon H]$ is known as the *index* of H in G. We can construct Lagrange's theorem analogously using right cosets. Hence, the index of a subgroup is independent of the choice of whether to use left or right cosets; the number of left cosets is equal to the number of right cosets.

§0.3 Order

Let $g \in G$. If there exists $n \geq 1$ such that $g^n = 1$, then the least such n is the *order* of g. If no such n exists, we say that g has infinite order. If g has order d, then:

1. $g^n = 1 \implies d \mid n$;
2. $\langle g \rangle = \left\{1, g, \ldots, g^{d-1}\right\} \leq G$, and by Lagrange's theorem (if G is finite) $d \mid |G|$.

§0.4 Normality and quotients

A subgroup $H \leq G$ is *normal*, written $H \trianglelefteq G$, if $g^{-1}Hg = H$ for all $g \in G$. In other words, H is preserved under conjugation over G. If $H \trianglelefteq G$, then the set G/H of left cosets of H in G forms the *quotient group*. The group action is defined by $g_1H \cdot g_2H = (g_1 \cdot g_2)H$. This can be shown to be well-defined.

§0.5 Homomorphisms

Let G, H be groups. A function $\varphi\colon G \to H$ is a *group homomorphism* if $\varphi(g_1 \cdot_G g_2) = \varphi(g_1) \cdot_H \varphi(g_2)$ for all $g_1, g_2 \in G$. The *kernel* of φ is defined to be $\ker \varphi = \{g \in G\colon \varphi(g) = 1\}$, and the *image* of φ is $\operatorname{Im} \varphi = \{\varphi(g)\colon g \in G\}$. The kernel is a normal subgroup of G, and the image is a subgroup of H.

§0.6 Isomorphisms

An *isomorphism* is a homomorphism that is bijective. This yields an inverse function, which is of course also an isomorphism. If $\varphi\colon G \to H$ is an isomorphism, we say that G and H are isomorphic, written $G \cong H$. Isomorphism is an equivalence relation. The isomorphism theorems are

1. if $\varphi\colon G \to H$, then $G/\ker \varphi \cong \operatorname{Im} \varphi$;

2. if $H \leq G$ and $N \trianglelefteq G$, then $H \cap N \trianglelefteq H$ and $H/H \cap N \cong HN/N$;
3. if $N \leq M \leq G$ such that $N \trianglelefteq G$ and $M \trianglelefteq G$, then $M/N \trianglelefteq G/N$, and $G/N/M/N = G/M$.

§1 Simple groups

§1.1 Introduction

If $K \trianglelefteq G$, then studying the groups K and G/K give information about G itself. This approach is available only if G has nontrivial normal subgroups. It therefore makes sense to study groups with no normal subgroups, since they cannot be decomposed into simpler structures in this way.

Definition 1.1 (Simple Group)
A group G is **simple** if $\{1\}$ and G are its only normal subgroups.

By convention, we do not consider the trivial group to be a simple group. This is analogous to the fact that we do not consider one to be a prime.

Lemma 1.1
Let G be an abelian group. G is simple iff $G \cong C_p$ for some prime p.

Proof. Certainly C_p is simple by Lagrange's theorem. Conversely, since G is abelian, all subgroups are normal. Let $1 \neq g \in G$. Then $\langle g \rangle \trianglelefteq G$. Hence $\langle g \rangle = G$ by simplicity. If G is infinite, then $G \cong \mathbb{Z}$, which is not a simple group; $2\mathbb{Z} \triangleleft \mathbb{Z}$. Hence G is finite, so $G \cong C_{o(g)}$. If $o(g) = mn$ for $m, n \neq 1, p$, then $\langle g^m \rangle \leq G$, contradicting simplicity. □

Lemma 1.2
If G is a finite group, then G has a **composition series**

$$1 \cong G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

where each quotient G_{i+1}/G_i is simple.

Remark 3. It is not the case that necessarily G_i be normal in G_{i+k} for $k \geq 2$.

Proof. We will consider an inductive step on $|G|$. If $|G| = 1$, then trivially $G = 1$. Conversely, if $|G| > 1$, let G_{n-1} be a normal subgroup of largest possible order not equal to $|G|$. Then, G/G_{n-1} exists, and is simple by the correspondence theorem. □

§2 Group actions

§2.1 Definitions

Definition 2.1 (Symmetric Group)

Let X be a set. Then $\mathrm{Sym}(X)$ is the group of permutations of X; that is, the group of all bijections of X to itself under composition. The identity can be written id or id_X.

Definition 2.2 (Permuation Group)

A group G is a permutation group of degree n if $G \leq \mathrm{Sym}(X)$ where $|X| = n$.

Example 2.1

The symmetric group S_n is exactly equal to $\mathrm{Sym}(\{1, \ldots, n\})$, so is a permutation group of order n. A_n is also a permutation group of order n, as it is a subgroup of S_n. D_{2n} is a permutation group of order n.

Definition 2.3 (Group Actions)

A **group action** of a group G on a set X is a function $\alpha \colon G \times X \to X$ satisfying

$$\alpha(e, x) = x; \quad \alpha(g_1 \cdot g_2, x) = \alpha(g_1, \alpha(g_2, x))$$

for all $g_1, g_2 \in G, x \in X$. The group action may be written $*$, defined by $g * x \equiv \alpha(g, x)$.

Proposition 2.1

An action of a group G on a set X is uniquely characterised by a group homomorphism $\varphi \colon G \to \mathrm{Sym}(X)$.

Proof. For all $g \in G$, we can define $\varphi_g \colon X \to X$ by $x \mapsto g * x$. Then, for all $x \in X$,

$$\varphi_{g_1 g_2}(x) = (g_1 g_2) * x = g_1 * (g_2 * x) = \varphi_{g_1}(\varphi_{g_2}(x))$$

Thus $\varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_2}$. In particular, $\varphi_g \circ \varphi_{g^{-1}} = \varphi_e$. We now define

$$\varphi \colon G \to \mathrm{Sym}(X); \quad \varphi(g) = \varphi_g \implies \varphi(g)(x) = g * x$$

This is a homomorphism.

Conversely, any group homomorphism $\varphi\colon G \to \mathrm{Sym}(X)$ induces a group action $*$ by $g * x = \varphi(g)$. This yields $e * x = \varphi(e)(x) = \mathrm{id}\, x = x$ and $(g_1 g_2) * x = \varphi(g_1 g_2)x = \varphi(g_1)\varphi(g_2)x = g_1 * (g_2 * x)$ as required. □

Definition 2.4 (Permutation Representation)

The homomorphism $\varphi\colon G \to \mathrm{Sym}(X)$ defined in the above proof is called a **permutation representation** of G.

Definition 2.5 (Orbit, Stabiliser)

Let G act on X. Then,

1. the **orbit** of $x \in X$ is $\mathrm{Orb}_G(x) = \{g * x \colon g \in G\} \subseteq X$;
2. the **stabiliser** of $x \in X$ is $G_x = \{g \in G \colon g * x = x\} \leq G$.

Definition 2.6 (Transitive Group Action)

If there is only orbit, i.e. $\mathrm{Orb}_G(x) = X \quad \forall\, x$ then the group action is **transitive**.

Definition 2.7 (Kernel)

The **kernel** of a permutation representation is $\bigcap_{x \in X} G_x$.

Remark 4. The kernel of the permutation representation φ is also referred to as the kernel of the group action itself.

Definition 2.8 (Faithful Group Action)

If the kernel is trivial the action is said to be **faithful**.

Theorem 2.1 (Orbit-stabiliser theorem)

The orbit $\mathrm{Orb}_G(x)$ bijects with the set G/G_x of left cosets of G_x in G (which may not be a quotient group). In particular, if G is finite, we have

$$|G| = |\mathrm{Orb}(x)| \cdot |G_x|$$

Example 2.2

If G is the group of symmetries of a cube and we let X be the set of vertices in

the cube, G acts on X. Here, for all $x \in X$, $|\mathrm{Orb}(x)| = 8$ and $|G_x| = 6$ (including reflections), hence $|G| = 48$.

Remark 5. The orbits partition X.

Note that $G_{g*x} = gG_xg^{-1}$. Hence, if x, y lie in the same orbit, their stabilisers are conjugate.

§2.2 Examples

Example 2.3

G acts on itself by left multiplication. This is known as the **left regular action**. The kernel is trivial, hence the action is faithful. The action is transitive, since for all $g_1, g_2 \in G$, the element $g_2g_1^{-1}$ maps g_1 to g_2.

Theorem 2.2 (Cayley's theorem)

Any finite group G is a permutation group of order $|G|$; it is isomorphic to a subgroup of $S_{|G|}$.

Example 2.4

Let $H \leq G$. Then G acts on G/H by left multiplication, where G/H is the set of left cosets of H in G. This is known as the **left coset action**. This action is transitive using the construction above for the left regular action. We have $\ker\varphi = \bigcap_{x\in G} xHx^{-1}$, which is the largest normal subgroup of G contained within H.

Theorem 2.3

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

Proof. Let G act on $X = G/H$ by left multiplication. Let $\varphi\colon G \to \mathrm{Sym}(X)$ be the permutation representation associated to this group action.

Since G is simple, $\ker\varphi = 1$ or $\ker\varphi = G$. If $\ker\varphi = G$, then $\mathrm{Im}\,\varphi = \mathrm{id}$, which is a contradiction since G acts transitively on X and $|X| > 1$. Thus $\ker\varphi = 1$, and $G \cong \mathrm{Im}\,\varphi \leq S_n$.

Since $G \leq S_n$ and $A_n \triangleleft S_n$, the second isomorphism theorem shows that $G \cap A_n \triangleleft G$,

and

$$G/G \cap A_n \cong GA_n/A_n \leq S_n/A_n \cong C_2$$

Since G is simple, $G \cap A_n = 1$ or G. If $G \cap A_n = 1$, then G is isomorphic to a subgroup of C_2, but this is false, since G is non-abelian. Hence $G \cap A_n = G$ so $G \leq A_n$. Finally, if $n \leq 4$ we can check manually that A_n is not simple; A_n has no non-abelian simple subgroups. □

§2.3 Conjugation actions

Example 2.5

Let G act on G by conjugation, so $g * x = gxg^{-1}$. This is known as the **conjugation action**.

Definition 2.9 (Conjugacy Class, Centraliser, Centre)

The orbit of the conjugation action is called the **conjugacy class** of a given element $x \in G$, written $\mathrm{ccl}_G(x)$. The stabiliser of the conjugation action is the set C_x of elements which commute with a given element x, called the **centraliser** of x in G. The kernel of φ is the set $Z(G)$ of elements which commute with all elements in x, which is the **centre** of G. This is always a normal subgroup.

Remark 6. $\varphi\colon G \to G$ satisfies

$$\varphi(g)(h_1h_2) = gh_1h_2g^{-1} = hh_1g^{-1}gh_2g^{-1} = \varphi(g)(h_1)\varphi(g)(h_2)$$

Hence $\varphi(g)$ is a group homomorphism for all g. It is also a bijection, hence $\varphi(g)$ is an isomorphism from $G \to G$.

Definition 2.10 (Automorphism)

An isomorphism from a group to itself is known as an **automorphism**. We define $\mathrm{Aut}(G)$ to be the set of all group automorphisms of a given group. This set is a group. Note, $\mathrm{Aut}(G) \leq \mathrm{Sym}(G)$, and the $\varphi\colon G \to \mathrm{Sym}(G)$ above has image in $\mathrm{Aut}(G)$.

Example 2.6

Let X be the set of subgroups of G. Then G acts on X by conjugation: $g * H = gHg^{-1}$. The stabiliser of a subgroup H is $\{g \in G\colon gHg^{-1} = H\} = N_G(H)$, called

the **normaliser** of H in G. The normaliser of H is the largest subgroup of G that contains H as a normal subgroup. In particular, $H \triangleleft G$ if and only if $N_G(H) = G$.

§3 Alternating groups

§3.1 Conjugation in alternating groups

We know that elements in S_n are conjugate if and only if they have the same cycle type. However, elements of A_n that are conjugate in S_n are not necessarily conjugate in A_n. Let $g \in A_n$. Then $C_{A_n}(g) = C_{S_n}(g) \cap A_n$. There are two possible cases.

- If there exists an odd permutation that commutes with g, then $2|C_{A_n}(g)| = |C_{S_n}(g)|$. By the orbit-stabiliser theorem, $|\mathrm{ccl}_{A_n}(g)| = |\mathrm{ccl}_{S_n}(g)|$.
- If there is no odd permutation that commutes with g, we have $|C_{A_n}(g)| = |C_{S_n}(g)|$. Similarly, $2|\mathrm{ccl}_{A_n}(g)| = |\mathrm{ccl}_{S_n}(g)|$.

Example 3.1

For $n = 5$, the product $(1\ 2)(3\ 4)$ commutes with $(1\ 2)$, and $(1\ 2\ 3)$ commutes with $(4\ 5)$. Both of these elements are odd. So the conjugacy classes of the above inside S_5 and A_5 are the same. However, $(1\ 2\ 3\ 4\ 5)$ does not commute with any odd permutation. Indeed, if that were true for some h, we would have

$$(1\ 2\ 3\ 4\ 5) = h(1\ 2\ 3\ 4\ 5)h^{-1} = (h(1)\ h(2)\ h(3)\ h(4)\ h(5))$$

Hence h must be a 5-cycle so $h \in \langle g \rangle \leq A_5$. So $|\mathrm{ccl}_{A_5}(g)| = \frac{1}{2}|\mathrm{ccl}_{S_5}(g)| = 12$. We can then show that A_5 has conjugacy classes of size $1, 15, 20, 12, 12$.

If $H \trianglelefteq A_5$, H is a union of conjugacy classes so $|H|$ must be a sum of the sizes of the above conjugacy classes. By Lagrange's theorem, $|H|$ must divide 60. We can check explicitly that this is not possible unless $|H| = 1$ or $|H| = 60$. Hence A_5 is simple.

§3.2 Simplicity of alternating groups

Lemma 3.1

A_n is generated by 3-cycles.

Proof. Each $\sigma \in A_n$ is a product of an even number of transpositions. It therefore suffices to show that a product of any two transpositions can be written as a product of 3-cycles. For a, b, c, d distinct,

$$(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d); \quad (a\ b)(b\ c) = (a\ b\ c)$$

□

Lemma 3.2

If $n \geq 5$, all 3-cycles in A_n are conjugate (in A_n).

Proof. We claim that every 3-cycle is conjugate to $(1\ 2\ 3)$. If $(a\ b\ c)$ is a 3-cycle, we have $(a\ b\ c) = \sigma(1\ 2\ 3)\sigma^{-1}$ for some $\sigma \in S_n$. If $\sigma \in A_n$, then the proof is finished. Otherwise, $\sigma \mapsto \sigma(4\ 5) \in A_n$ suffices, since $(4\ 5)$ commutes with $(1\ 2\ 3)$. □

Theorem 3.1

A_n is simple for $n \geq 5$.

Proof. Suppose $1 \neq N \triangleleft A_n$. To disprove normality, it suffices to show that N contains a 3-cycle by the lemmas above, since the normality of N would imply N contains all 3-cycles and hence all elements of A_n.

Let $1 \neq \sigma \in N$, writing σ as a product of disjoint cycles.

1. Suppose σ contains a cycle of length $r \geq 4$. Without loss of generality, let $\sigma = (1\ 2\ 3 \ldots r)\tau$ where τ fixes $1, \ldots, r$. Now, let $\delta = (1\ 2\ 3)$. We have

$$\underbrace{\sigma^{-1}}_{\in N}\underbrace{\delta^{-1}\sigma\delta}_{\in N} = (r \ldots 2\ 1)\tau^{-1}(1\ 3\ 2)(1\ 2 \ldots r)\tau(1\ 2\ 3) = (2\ 3\ r)$$

   So N contains a 3-cycle.

2. Suppose σ contains two 3-cycles, which can be written without loss of generality as $(1\ 2\ 3)(4\ 5\ 6)\tau$. Let $\delta = (1\ 2\ 4)$, and then

$$\sigma^{-1}\delta^{-1}\sigma\delta = (1\ 3\ 2)(4\ 6\ 5)(1\ 4\ 2)(1\ 2\ 3)(4\ 5\ 6)(1\ 2\ 4) = (1\ 2\ 4\ 3\ 6)$$

   Therefore, there exists an element of N which contains a cycle of length $5 \geq 4$. This reduces the problem to case (i).

3. Finally, suppose σ contains two 2-cycles, which will be written $(1\ 2)(3\ 4)\tau$. Then let $\delta = (1\ 2\ 3)$ and

$$\sigma^{-1}\delta^{-1}\sigma\delta = \underbrace{(1\ 2)(3\ 4)(1\ 3\ 2)(1\ 2)(3\ 4)}_{(2\ 4\ 1)}(1\ 2\ 3) = (1\ 4)(2\ 3) = \pi$$

   Let $\varepsilon = (2\ 3\ 5)$. Then

$$\underbrace{\pi^{-1}}_{\in N}\underbrace{\varepsilon^{-1}\pi\varepsilon}_{\in N} = (1\ 4)(2\ 3)(2\ 5\ 3)(1\ 4)(2\ 3)(2\ 3\ 5) = (2\ 5\ 3)$$

   Thus N contains a 3-cycle.

There are now three remaining cases, where σ is a transposition, a 3-cycle, or a transposition composed with a 3-cycle. Note that the remaining cases containing transpositions cannot be elements of A_n. If σ is a 3-cycle, we already know A_n contains a 3-cycle, namely σ itself. $\square$

§4 p-groups

§4.1 p-groups

Definition 4.1 (p-group)

Let p be a prime. A finite group G is a **p-group** if $|G| = p^n$ for $n \geq 1$.

Theorem 4.1

If G is a p-group, the centre $Z(G)$ is non-trivial.

Proof. For $g \in G$, due to the orbit-stabiliser theorem, $|\text{ccl}(g)||C(g)| = p^n$. In particular, $|\text{ccl}(g)|$ divides p^n, and they partition G. Since G is a disjoint union of conjugacy classes, modulo p we have

$$|G| \equiv \text{number of conjugacy classes of size } 1 \equiv 0 \implies |Z(G)| \equiv 0$$

Hence $Z(G)$ has order zero modulo p so it cannot be trivial. We can check this by noting that $g \in Z(G) \iff x^{-1}gx = g$ for all x, which is true if and only if $\text{ccl}_G(g) = \{g\}$. □

Corollary 4.1

The only simple p-groups are the cyclic groups of order p.

Proof. Let G be a simple p-group. Since $Z(G)$ is a normal subgroup of G, we have $Z(G) = 1$ or $Z(G) = G$. But $Z(G)$ may not be trivial, so $Z(G) = G$. This implies G is abelian. The only abelian simple groups are cyclic of prime order by lemma 1.1, hence $G \cong C_p$. □

Corollary 4.2

Let G be a p-group of order p^n. Then G has a subgroup of order p^r for all $r \in \{0, \ldots, n\}$.

Proof. Recall from lemma 1.2 that any group G has a composition series $1 = G_1 \triangleleft \cdots \triangleleft G_N = G$ where each quotient G_{i+1}/G_i is simple.

Since G is a p-group, G_{i+1}/G_i is also a p-group. Each successive quotient is an order p group by the previous corollary, so we have a composition series of nested subgroups of order p^r for all $r \in \{0, \ldots, n\}$. □

Lemma 4.1

Let G be a group. If ${}^{G}\!/_{Z(G)}$ is cyclic, then G is abelian. This then implies that $Z(G) = G$, so in particular ${}^{G}\!/_{Z(G)} = 1$.

Proof. Let $gZ(G)$ be a generator for ${}^{G}\!/_{Z(G)}$. Then, each coset of $Z(G)$ in G is of the form $g^r Z(G)$ for some $r \in \mathbb{Z}$. Thus, $G = \{g^r z \colon r \in \mathbb{Z}, z \in Z(G)\}$. Now, we multiply two elements of this group and find

$$g^{r_1} z_1 g^{r_2} z_2 = g^{r_1+r_2} z_1 z_2 = g^{r_1+r_2} z_2 z_1 = z_2 z_1 g^{r_1+r_2} = g^{r_2} z_2 g^{r_1} z_1$$

So any two elements in G commute. □

Corollary 4.3

Any group of order p^2 is abelian.

Proof. Let G be a group of order p^2. Then $|Z(G)| \in \{1, p, p^2\}$. The centre cannot be trivial as proven above, since G is a p-group. If $|Z(G)| = p$, we have that ${}^{G}\!/_{Z(G)}$ is cyclic as it has order p. Applying the previous lemma, G is abelian. However, this is a contradiction since the centre of an abelian group is the group itself. If $|Z(G)| = p^2$ then $Z(G) = G$ and then G is clearly abelian. □

§4.2 Sylow theorems

Theorem 4.2 (Sylow Theorems)

Let G be a finite group of order $p^a m$ where p is a prime and p does not divide m. Then:

1. The set $\mathrm{Syl}_p(G) = \{P \leq G \colon |P| = p^a\}$ of Sylow p-subgroups is non-empty.
2. All Sylow p-subgroups are conjugate.
3. The amount of Sylow p-subgroups $n_p = \left|\mathrm{Syl}_p(G)\right|$ satisfies

$$n_p \equiv 1 \mod p; \quad n_p \mid |G| \implies n_p \mid m$$

Proof. 1. Let Ω be the set of all subsets of G of order p^a. We can directly find

$$|\Omega| = \binom{p^a m}{p^a} = \frac{p^a m}{p^a} \cdot \frac{p^a m - 1}{p^a - 1} \cdots \frac{p^a m - p^a + 1}{1}$$

Note that for $0 \leq k < p^a$, the numbers $p^a m - k$ and $p^a - k$ are divisible by the same power of p. In particular, $|\Omega|$ is coprime to p.

Let G act on Ω by left-multiplication, so $g * X = \{gx \colon x \in X\}$. For any $X \in \Omega$, the orbit-stabiliser theorem can be applied to show that

$$|G_X||\mathrm{orb}_G(X)| = |G| = p^a m$$

Since $|\Omega|$ is coprime to p, there must exist an orbit with size coprime to p, since orbits partition Ω. For such an X, $p^a \mid |G_X|$.

Conversely, note that if $g \in G$ and $x \in X$, then $g \in (gx^{-1}) * X$. Hence, we can consider

$$G = \bigcup_{g \in G} g * X = \bigcup_{Y \in \mathrm{orb}_G(X)} Y$$

Thus $|G| \leq |\mathrm{orb}_G(X)| \cdot |X|$, giving $|G_X| = \frac{|G|}{|\mathrm{orb}_G(X)|} \leq |X| = p^a$.

As $p^a \mid |G_X|$ we must have $|G_X| = p^a$. In other words, the stabiliser G_X is a Sylow p-subgroup of G.

2. We will prove a stronger result for this part of the proof.

> **Lemma 4.2**
> If P is a Sylow p-subgroup and $Q \leq G$ is a p-subgroup, then $Q \leq gPg^{-1}$ for some $g \in G$.

Indeed, let Q act on the set of left cosets of P in G by left multiplication. By the orbit-stabiliser theorem, each orbit has size which divides $|Q| = p^k$ for some k. Hence each orbit has size p^r for some r.

Since G/P has size m, which is coprime to p, there must exist an orbit of size 1[a]. Therefore there exists $g \in G$ such that $q * gP = gP$ for all $q \in Q$. Equivalently, $g^{-1}qg \in P$ for all $q \in Q$. This implies that $Q \leq gPg^{-1}$ as required. This then weakens to the second part of the Sylow theorems.

3. Let G act on $\mathrm{Syl}_p(G)$ by conjugation. Part (ii) of the Sylow theorems implies that this action is transitive. By the orbit-stabiliser theorem, $n_p = \left|\mathrm{Syl}_p(G)\right| \mid |G|$.

Let $P \in \mathrm{Syl}_p(G)$. Then let P act on $\mathrm{Syl}_p(G)$ by conjugation. Since P is a Sylow p-subgroup, the orbits of this action have size dividing $|P| = p^a$, so the size is some power of p.
To show $n_p \equiv 1 \mod p$, it suffices to show that $\{P\}$ is the unique orbit of size 1, as the orbits of other sizes are multiples of p.
Suppose $\{Q\}$ is another orbit of size 1, so Q is a Sylow p-subgroup which is preserved under conjugation by P. Thus P normalises Q, so $P \leq N_G(Q)$. Notice that P and Q are both Sylow p-subgroups of $N_G(Q)$. By (ii), P and Q are conjugate inside $N_G(Q)$. Hence $P = Q$ since $Q \trianglelefteq N_G(Q)$. Thus, $|P|$ is the unique orbit of size 1, so $n_p \equiv 1 \mod p$ as required.

□

[a] Sum of the orbit sizes is m, m coprime to p.

Corollary 4.4

If $n_p = 1$, then there is only one Sylow p-subgroup, and it is normal.

Proof. Let $g \in G$ and $P \in \mathrm{Syl}_p(G)$. Then gPg^{-1} is a Sylow p-subgroup, hence $gPg^{-1} = P$. P is normal in G. □

Remark 7. When G acts on $\mathrm{Syl}_p(G)$ by conjugation, the orbit is $\mathrm{Syl}_p(G)$ and the stabiliser is the normaliser.

Example 4.1

Let G be a group with $|G| = 1000 = 2^3 \cdot 5^3$. Here, $n_5 \equiv 1 \mod 5$, and $n_5 \mid 8$, hence $n_5 = 1$. Thus the unique Sylow 5-subgroup is normal. Hence no group of order 1000 is simple.

Example 4.2

Let G be a group with $|G| = 132 = 2^2 \cdot 3 \cdot 11$. n_{11} satisfies $n_{11} \equiv 1 \mod 11$ and $n_{11} \mid 12$, thus $n_{11} \in \{1, 12\}$.

Suppose G is simple.

Then $n_{11} = 12$[a]. The amount of Sylow 3-subgroups satisfies $n_3 \equiv 1 \mod 3$ and $n_3 \mid 44$ so $n_3 \in \{1, 4, 22\}$. Since G is simple, $n_3 \in \{4, 22\}$.

Suppose $n_3 = 4$. Then G acts on $\mathrm{Syl}_3(G)$ by conjugation, and this generates a group homomorphism $\varphi\colon G \to S_4$. But the kernel of this homomorphism is a normal subgroup of G, so $\ker\varphi$ is trivial or G itself as G simple. If $\ker\varphi = G$, then $\mathrm{Im}\,\varphi$

is trivial, contradicting Sylow's second theorem. If $\ker\varphi = 1$, then $\operatorname{Im}\varphi$ has order $132 > |S_4|$ ↯.

Thus $n_3 = 22$ and recall $n_{11} = 12$. This means that G has $22 \cdot (3-1) = 44$ elements of order 3[b], and further G has $12 \cdot (11-1) = 120$ elements of order 11. However, the sum of these two totals is more than the total of 132 elements, so this is a contradiction. Hence G is not simple.

[a] If $n_{11} = 1$ then we have a normal subgroup by the previous corollary.

[b] Each group in $\operatorname{Syl}_3(G)$ intersect trivially, as if they didn't any non trivial element in the intersection would generate both groups as they're all C_3.

§5 Matrix groups

§5.1 Definitions

Let F be a field, such as $\mathbb{C}$ or $\mathbb{Z}/p\mathbb{Z}$.

Definition 5.1 (Gneeral Linear Group)
Let $GL_n(F)$ be set of $n \times n$ invertible matrices over F, which is called the **general linear group**.

Definition 5.2 (Special Linear Group)
Let $SL_n(F)$ be set of $n \times n$ matrices with determinant one over F, which is called the **special linear group**.

Remark 8. $SL_n(F)$ is the kernel of the determinant homomorphism on $GL_n(F)$, so $SL_n(F) \triangleleft GL_n(F)$.

Definition 5.3 (Scalar Matrices)
Let $Z \triangleleft GL_n(F)$ denote the subgroup of **scalar matrices**, the group of nonzero multiples of the identity.

Remark 9. Z is the centre of $GL_n(F)$.

Definition 5.4 (Projective General Linear Group)
The group $PGL_n(F) = GL_n(F)/Z$ is called the **projective general linear group**.

Definition 5.5 (Projective Special Linear Group)
The **projective special linear group** is $PSL_n(F) = SL_n(F)/Z \cap SL_n(F)$.

Remark 10. By the second isomorphism theorem, $PSL_n(F)$ is isomorphic to $Z \cdot SL_n(F)/Z$, which is a subgroup of $PGL_n(F)$.

Example 5.1
Consider the finite group $G = GL_n\left(\mathbb{Z}/p\mathbb{Z}\right)$. A list of n vectors in $\mathbb{Z}/p\mathbb{Z}$ are the columns of a matrix $A \in G$ iff the vectors are linearly independent. Hence, by

considering dimensionality of subspaces generated by each column,

$$\begin{aligned}|G| &= (p^n-1)(p^n-p)(p^n-p^2)\cdots(p^n-p^{n-1}) \\ &= p^{1+2+\cdots+(n-1)}(p^n-1)(p^{n-1}-1)\cdots(p-1) \\ &= p^{\binom{n}{2}}\prod_{i=1}^{n}(p^i-1)\end{aligned}$$

Hence the Sylow p-subgroups have size $p^{\binom{n}{2}}$. Let U be the set of upper triangular matrices with ones on the diagonal. This forms a Sylow p-subgroup of G, since there are $\binom{n}{2}$ entries in a given upper triangular matrix, and there are p choices for such an entry.

§5.2 Möbius maps in modular arithmetic

Recall that $PGL_2(\mathbb{C})$ acts on $\mathbb{C}\cup\{\infty\}$ by Möbius transformations. Likewise, $PGL_2\left(\mathbb{Z}/p\mathbb{Z}\right)$ acts on $\mathbb{Z}/p\mathbb{Z}\cup\{\infty\}$ by Möbius transformations. For a matrix

$$A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in GL_2\left(\mathbb{Z}/p\mathbb{Z}\right);\quad A\colon z\mapsto\frac{az+b}{cz+d}$$

Since the scalar matrices act trivially, we obtain an action on the projective general linear group instead of the general linear group by quotienting out the scalar matrices.

We can represent ∞ as an integer, say, p, for the purposes of constructing a permutation representation.

Lemma 5.1

The permutation representation $PGL_2\left(\mathbb{Z}/p\mathbb{Z}\right)\to S_{p+1}$ is injective (and is an isomorphism if $p=2$ or $p=3$).

Proof. Suppose that $\frac{az+b}{cz+d}=z$ for all $z\in\mathbb{Z}/p\mathbb{Z}\cup\{\infty\}$.
Since $z=0$, we have $b=0$.
Since $z=\infty$, we find $c=0$.
Thus the matrix is diagonal.
Finally, since $z=1$, $\frac{a}{d}=1$ hence $a=d$.
Thus the matrix is scalar. So the permutation representation from $PGL_2\left(\mathbb{Z}/p\mathbb{Z}\right)$ has trivial kernel, giving injectivity as required.

If $p=2$ or $p=3$ we can compute the orders of relevant groups manually and show that the permutation representation is an isomorphism. □

Lemma 5.2

Let p be an odd prime. Then

$$\left|PSL_2\left(\mathbb{Z}/p\mathbb{Z}\right)\right| = \frac{(p-1)p(p+1)}{2}$$

Proof. By example 5.1,

$$\left|GL_2\left(\mathbb{Z}/p\mathbb{Z}\right)\right| = p(p^2-1)(p-1)$$

The homomorphism $GL_2\left(\mathbb{Z}/p\mathbb{Z}\right) \to \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ given by the determinant is surjective. Since $SL_2\left(\mathbb{Z}/p\mathbb{Z}\right)$ is the kernel of this homomorphism, we have

$$\left|SL_2\left(\mathbb{Z}/p\mathbb{Z}\right)\right| = \frac{GL_2\left(\mathbb{Z}/p\mathbb{Z}\right)}{p-1} = p(p-1)(p+1)$$

Now, if $\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}$ is an element of the special linear group, then $\lambda^2 \equiv 1 \mod p$. Then, $p \mid (\lambda-1)(\lambda+1)$ hence $\lambda \equiv \pm 1 \mod p$. Thus,

$$Z \cap SL_2\left(\mathbb{Z}/p\mathbb{Z}\right) = \{\pm I\}$$

and $\pm I$ are distinct since $p > 2$.

Hence the order of the projective special linear group is half the order of the special linear group as required. □

Example 5.2

Let $G = PSL_2\left(\mathbb{Z}/5\mathbb{Z}\right)$. Then by the previous lemma, $|G| = 60$. Let G act on $\mathbb{Z}/5\mathbb{Z} \cup \{\infty\}$ by Möbius transformations. The permutation representation $\varphi\colon G \to \mathrm{Sym}(\{0,1,2,3,4,\infty\}) \cong S_6$ is injective by Lemma 5.1.

Claim 5.1

$\operatorname{Im}\varphi \subseteq A_6$, i.e. $\psi : G \xrightarrow{\varphi} S_6 \xrightarrow{\text{sgn}} \{\pm 1\}$ is trivial.

Proof. Let $h \in G$, and suppose h has order $2^n m$ for odd m and so $o(h^m) = 2^n$. If $\psi(h^m) = 1$, then since ψ is a group homomorphism we have $\psi(h)^m = 1$ giving $\psi(h) \neq -1 \implies \psi(h) = 1$.

So to show ψ is trivial, it suffices to show $\psi(g) = 1$ for all $g \in G$ with order a power of 2.

By Lemma 4.2, if g has order a power of 2, it is contained in a Sylow 2-subgroup. Then it suffices to show that $\psi(H) = 1$ for all Sylow 2-subgroups H. But since $\ker \psi \triangleleft G$ and all Sylow 2-subgroups are conjugate, it suffices to show $\psi(H) = 1$ for a single Sylow 2-subgroup H.

The Sylow 2-subgroup must have order 4. Hence consider

$$H = \left\langle \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \{\pm I\}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \{\pm I\} \right\rangle$$

Both of these elements square to the identity element inside the projective special linear group. This generates a group of order 4 which is necessarily a Sylow 2-subgroup. We can explicitly compute the action of H on $\{0, 1, 2, 3, 4, \infty\}$.

$$\varphi\left(\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}\right) = (1\ 4)(2\ 3); \quad \varphi\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = (0\ \infty)(1\ 4)$$

These are products of two transpositions, hence even permutations. Thus $\psi(H) = 1$, proving the claim that $G \leq A_6$. □

We can prove that for any $G \leq A_6$ of order 60, we have $G \cong A_5$; this is a question from the example sheets.

§5.3 Properties

The following properties will not be proven in this course.

- $PSL_n\left(\mathbb{Z}/p\mathbb{Z}\right)$ is simple for all $n \geq 2$ and p prime, except where $n = 2$ and $p = 2, 3$. Such groups are called finite groups of *Lie type*.
- The smallest non-abelian simple groups are $A_5 \cong PSL_2\left(\mathbb{Z}/5\mathbb{Z}\right)$, then $PSL_2\left(\mathbb{Z}/7\mathbb{Z}\right) \cong GL_3\left(\mathbb{Z}/2\mathbb{Z}\right)$ which has order 168.

§6 Finite abelian groups

§6.1 Products of cyclic groups

Theorem 6.1

Every finite abelian group is isomorphic to a product of cyclic groups.

The proof for this theorem will be provided later in the course. Note that the isomorphism provided for by the theorem is not unique. An example of such behaviour is the following lemma.

Lemma 6.1

Let $m, n \in \mathbb{N}$ be coprime integers. Then $C_m \times C_n \cong C_{mn}$.

Proof. Let g, h be generators of C_m and C_n. Then consider the element $(g,h)^k = (g^k, h^k)$, which has order mn. Thus $\langle (g,h) \rangle$ has order mn. So every element in $C_m \times C_n$ is expressible in this way, giving $\langle (g,h) \rangle = C_m \times C_n$. □

Corollary 6.1

Let G be a finite abelian group. Then $G \cong C_{n_1} \times \cdots \times C_{n_k}$ where each n_i is a power of a prime.

Proof. If $n_i = p_1 a^1 \cdots p^r a^r$ where the p_i are distinct primes, then applying Lemma 6.1 inductively gives C_{n_i} as a product of cyclic groups which have orders that are powers of primes.

We can apply this to the theorem that every finite abelian group is isomorphic to a product of cyclic groups to find the result. □

Later, we will prove the following refinement of Theorem 6.1

Theorem 6.2

Let G be a finite abelian group. Then $G \cong C_{d_1} \times \cdots \times C_{d_t}$ where $d_i \mid d_{i+1}$ for all i.

Remark 11. The integers $n_1, \ldots, n_k$ in Corollary 6.1 are unique up to ordering. The integers $d_1, \ldots, d_t$ in Theorem 6.2 are also unique, assuming that $d_1 > 1$. The proofs will be omitted - but works by counting the number of elements of G of each prime power order.

Example 6.1

The abelian groups of order 8 are exactly C_8, $C_2 \times C_4$, and $C_2 \times C_2 \times C_2$.

Example 6.2

The abelian groups of order 12 are, using the corollary Corollary 6.1, $C_2 \times C_2 \times C_3$, $C_4 \times C_3$, and using Theorem 6.2, $C_2 \times C_6$ and C_{12}. However, $C_2 \times C_3 \cong C_6$ and $C_3 \times C_4 \cong C_{12}$, so the groups derived are isomorphic.

Definition 6.1 (Exponent)

The **exponent** of a group G is the least integer $n \geq 1$ such that $g^n = 1$ for all $g \in G$. Equivalently, the exponent is the lowest common multiple of the orders of elements in G.

Example 6.3

The exponent of A_4 is $\operatorname{lcm}\{2, 3\} = 6$.

Corollary 6.2 (Structure Theorem)

Let G be a finite abelian group. Then G contains an element which has order equal to the exponent of G.

Proof. If $G \cong C_{d_1} \times \cdots \times C_{d_t}$ for $d_i \mid d_{i+1}$, every $g \in G$ has order dividing d_t. Hence the exponent is d_t, and we can choose a generator of C_{d_t} to obtain an element in G of the same order[a]. □

[a] Say $o(h) = d_t$ with $h \in C_{d_t}$ then $(e, e, \ldots, e, h) \in G$ and has order d_t

Part II
Rings

§7 Rings

§7.1 Definitions

Definition 7.1 (Ring)

A **ring** is a triple $(R, +, \cdot)$ where R is a set and $+, \cdot$ are binary operations $R \times R \to R$, satisfying the following axioms.

1. $(R, +)$ is an abelian group, and we will denote the identity element 0 and the inverse of x as $-x$;
2. $(R, \cdot)$ satisfies the group axioms except for the invertibility axiom, and we will denote the identity element 1 and the inverse of x as x^{-1} if it exists;
3. for all $x, y, z \in R$ we have $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$.

If multiplication is commutative, we say that R is a **commutative** ring.

In this course, we will study only commutative rings.

Remark 12. For all $x \in R$,

$$0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x \implies 0 \cdot x = 0$$

Further,

$$0 = 0 \cdot x = (1 + -1) \cdot x = x + (-1 \cdot x) \implies -1 \cdot x = -x$$

Remark 13. Addition being commutative follows from distributive law and the other axioms so not necessary for it to be an abelian group.

Definition 7.2 (Subring)

A subset $S \subset R$ is a **subring**, denoted $S \leq R$, if $(S, +, \cdot)$ is a ring with the same identity elements.

Remark 14. It suffices to check the closure axioms for addition and multiplication; the other properties are inherited.

Example 7.1

$\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ are rings. The set $\mathbb{Z}[i] = \{a + bi \colon a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$. This is known as the ring of Gaussian integers.

Example 7.2

The set $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \colon a, b \in \mathbb{Q}\right\}$ is a subring of $\mathbb{R}$.

Example 7.3

The set $\mathbb{Z}/n\mathbb{Z}$ is a ring.

Example 7.4

Let R, S be rings. Then the **product** $R \times S$ is a ring under the binary operations

$$(a, b) + (c, d) = (a + c, b + d); \quad (a, b) \cdot (c, d) = (a \cdot c, b \cdot d)$$

The additive identity is $(0_R, 0_S)$ and the multiplicative identity is $(1_R, 1_S)$.

Note that the subset $R \times \{0\}$ is preserved under addition and multiplication, so it is a ring, but it is not a subring because the multiplicative identity is different.

§7.2 Polynomials

Definition 7.3 (Polynomial)

Let R be a ring. A **polynomial** f over R is an expression

$$f = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

for $a_i \in R$. The term X is a formal symbol, no substitution of X for a value will be made. We could alternatively define polynomials as finite sequences of terms in R.

The **degree** of a polynomial f is the largest n such that $a_n \neq 0$. A degree-n polynomial is **monic** if $a_n = 1$. We write $R[X]$ for the set of all such polynomials over R.

Let $g = b_0 + b_1 X + \cdots + b_n X^n$. Then we define

$$f + g = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_n + b_n)X^n; \quad f \cdot g = \sum_i \left(\sum_{j=0}^{i} a_j b_{i-j} \right) X^i$$

Then $(R[X], +, \cdot)$ is a ring. The identity elements are the constant polynomials 0 and 1. We can identify the ring R with the subring of $R[X]$ of constant polynomials.

Definition 7.4 (Unit)

An element $r \in R$ is a **unit** if r has a multiplicative inverse. The units in a ring, denoted $R^\times$, form an abelian group under multiplication.

For instance, $\mathbb{Z}^\times = \{\pm 1\}$ and $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$.

Definition 7.5 (Field)

A **field** is a ring where all nonzero elements are units and $0 \neq 1$.

Example 7.5

$\mathbb{Z}/n\mathbb{Z}$ is a field iff n is a prime.

Remark 15. If R is a ring such that $0 = 1$, then every element in the ring is equal to zero. Indeed, $x = 1 \cdot x = 0 \cdot x = 0$. Thus, the exclusion of rings with $0 = 1$ in the definition of a field simply excludes the trivial ring.

Proposition 7.1

Let $f, g \in R[X]$ such that the leading coefficient of g is a unit. Then there exist polynomials $q, r \in R[X]$ such that $f = qg + r$, where $\deg r < \deg q$.

Remark 16. This is the Euclidean algorithm for division, adapted to polynomial rings.

Proof. Let $n = \deg f$ and $m = \deg g$, so by induction on n

$$f = a_n X^n + \cdots + a_0; \quad g = b_m X^m + \cdots + b_0$$

By assumption, $b_m \in R^\times$.

If $n < m$ then let $q = 0$ and $r = f$.

Conversely, we have $n \geq m$. Consider the polynomial $f_1 = f - a_n b_m^{-1} X^{n-m} g$. This has degree at most $n - 1$. Hence, we can use induction on n to decompose f_1 as $f_1 = q_1 g + r$. Thus $f = (q_1 + a_n b_m^{-1} X^{n-m})g + r$ as required. □

Remark 17. If R is a field, then every nonzero element of R is a unit. Therefore, the above algorithm can be applied for all polynomials g unless g is the constant polynomial zero.

Example 7.6

Let R be a ring and X be a set. Then the set of functions $X \to R$ is a ring under

$$(f+g)(x) = f(x) + g(x); \quad (f \cdot g)(x) = f(x) \cdot g(x)$$

The set of continuous functions $\mathbb{R} \to \mathbb{R}$ is a subring of the ring of all functions $\mathbb{R} \to \mathbb{R}$, since they are closed under addition and multiplication. The set of polynomial functions $\mathbb{R} \to \mathbb{R}$ is also a subring, and we can identify this with the ring $\mathbb{R}[X]$.

Example 7.7

Let R be a ring. Then the *power series ring* $R[\![X]\!] = \{a_0 + a_1X + a_2X^2 + \dots a_i \in R\}$ is the set of power series over R. This is defined similarly to the polynomial ring, but we permit infinitely many nonzero elements in the expansion. The power series is defined formally; we cannot actually carry out infinitely many additions in an arbitrary ring. We instead consider the power series as a sequence of numbers.

Example 7.8

Let R be a ring. Then the ring of *Laurent polynomials* is $R[X, X^{-1}] = \{\sum_{i\in\mathbb{Z}} a_iX^i : a_i \in \mathbb{R}\}$ with the restriction that $a_i \neq 0$ only for finitely many i.

§8 Homomorphisms, Ideals and Quotients

§8.1 Homomorphisms

Definition 8.1 (Ring Homomorphism)

Let R and S be rings. A function $\varphi\colon R \to S$ is a **ring homomorphism** if

1. $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$;
2. $\varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2)$;
3. $\varphi(1_R) = 1_S$.

We can derive that $\varphi(0_R) = 0_S$ from (i).

Definition 8.2 (Isomorphism)

A ring homomorphism is an **isomorphism** if it is bijective.

Definition 8.3 (Kernel)

The **kernel** of a ring homomorphism is $\ker \varphi = \{r \in R : \varphi(r) = 0\}$.

Lemma 8.1

Let R, S be rings. Then a ring homomorphism $\varphi\colon R \to S$ is injective iff $\ker \varphi = \{0\}$.

Proof. Let $\varphi\colon (R,+) \to (S,+)$ be the induced group homomorphism on addition. The result then follows from the corresponding fact about group homomorphisms. □

§8.2 Ideals

Definition 8.4 (Ideal)

A subset $I \subseteq R$ is an **ideal**, written $I \triangleleft R$, if

1. I is a subgroup of $(R,+)$;
2. if $r \in R$ and $x \in I$, then $rx \in I$.

Definition 8.5 (Proper Ideal)

We say that an ideal is **proper** if $I \neq R$.

Lemma 8.2

Let $\varphi\colon R \to S$ be a ring homomorphism. Then $\ker \varphi$ is an ideal of R.

Proof. Considering the induced group homomorphism on addition, $\varphi\colon (R,+) \to (S,+)$, $\ker \varphi$ is a subgroup of $(R,+)$.

If $r \in R$ and $x \in \ker \varphi$, then

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

Hence $rx \in \ker \varphi$. □

Remark 18. If I contains a unit, then the multiplicative identity lies in I. Then all elements lie in I. In particular, if I is a proper ideal, $1 \notin I$. Hence a proper ideal I is not a subring of R.

Lemma 8.3

The ideals in $\mathbb{Z}$ are precisely the subsets of the form $n\mathbb{Z}$ for any $n = 0, 1, 2, \ldots$.

Proof. First, we can check directly that any subset of the form $n\mathbb{Z}$ is an ideal. Now, let I be any nonzero ideal of $\mathbb{Z}$ and let n be the smallest positive element in I. Then $n\mathbb{Z} \subseteq I$. Let $m \in I$. Then by the Euclidean algorithm, $m = qn + r$ for $q, r \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, n-1\}$. Then $r = m - qn$. We know $qn \in I$ since $n \in I$, so $r \in I$. If $r \neq 0$, this contradicts the minimality of n as chosen above. So $I = n\mathbb{Z}$ exactly. □

Definition 8.6 (Generated Ideals)

For an element $a \in R$, we write (a) to denote the subset of R given by multiples of a; that is $(a) = \{ra : r \in R\}$. This is an ideal, known as the **ideal generated by** a. More generally, if $a_1, \ldots, a_n \in R$, then $(a_1, \ldots, a_n) = \{r_1a_1 + \ldots r_na_n : r_i \in R\}$ is the set of elements in R given by linear combinations of the a_i. This is also an ideal.

Definition 8.7 (Prinipal Ideal)

Let $I \triangleleft R$. Then I is **principal** if there exists some $a \in R$ such that $I = (a)$.

§8.3 Quotients

Theorem 8.1

Let $I \triangleleft R$. Then the set R/I of cosets[a] of I in $(R, +)$ forms the **quotient ring** under the operations

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I; \quad (r_1 + I) \cdot (r_2 + I) = (r_1 \cdot r_2) + I$$

This ring has the identity elements

$$0_{R/I} = 0_R + I; \quad 1_{R/I} = 1_R + I$$

Further, the map $R \to R/I$ defined by $r \mapsto r + I$ is a ring homomorphism called the **quotient map**. The kernel of the quotient map is I. Hence any ideal is the kernel of some homomorphism.

[a] Left or right cosets, doesn't matter which.

Proof. From the analogous result from groups, the addition defined on the set of

cosets yields the group $\left(R/I, +\right)$. If $r_1 + I = r_1' + I$ and $r_2 + I = r_2' + I$, then $r_1' = r_1 + a_1$ and $r_2' = r_2 + a_2$ for some $a_1, a_2 \in I$. Then

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

Hence $(r_1' r_2') + I = (r_1 r_2) + I$. So the operations are well defined.

Remaining properties for R/I follows from those for R. The remainder of the proof is trivial. □

[a] Recall we only consider commutative rings in this course so $a_1 r_2 = r_2 a_1$.

Example 8.1

In the integers $\mathbb{Z}$, the ideals are $n\mathbb{Z}$. Hence we can form the quotient ring $\mathbb{Z}/n\mathbb{Z}$. The ring $\mathbb{Z}/n\mathbb{Z}$ has elements $n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}$. Addition and multiplication behave like in modular arithmetic modulo n.

Example 8.2

Consider the ideal (X) inside the polynomial ring $\mathbb{C}[X]$. This ideal is the set of polynomials with zero constant term. Let $f(X) = a_n X^n + \cdots + a_0$ be an arbitrary element of $\mathbb{C}[X]$, $a_n X^n, \ldots, a_1 X^1 \in (X)$. Then $f(X) + (X) = a_0 + (X)$.
Thus, there exists a bijection between $\mathbb{C}[X]/(X)$ and $\mathbb{C}$, defined by $f(x) + (X) \mapsto f(0)$, with inverse $a \mapsto a + (X)$. This bijection is a ring homomorphism, hence $\mathbb{C}[X]/(X) \cong \mathbb{C}$.

Example 8.3

Consider $(X^2+1) \triangleleft \mathbb{R}[X]$, $\mathbb{R}[X]/(X^2+1) = \{f(X) + (X^2+1) : f(X) \in \mathbb{R}[X]\}$. For $f(X) = a_n X^n + \cdots + a_0 \in \mathbb{R}[X]$, by Proposition 7.1 we can apply the Euclidean algorithm to write $f(X) = q(X)(X^2+1) + r(X)$ where $\deg r < 2$. Hence $r(X) = a + bX$ for $a, b \in \mathbb{R}$.

Thus, any element of $\mathbb{R}[X]/(X^2+1)$ can be written $a + bX + (X^2+1)$. Suppose a coset can be represented by two representatives: $a + bX + (X^2+1) = a' + b'X + (X^2+1)$. Then,

$$a + bX - a' - b'X = (a - a') - (b - b')X = g(X)(X^2+1)$$

Hence $g(X) = 0$, giving $a - a' = 0$ and $b - b' = 0$. Hence the coset representative is unique.

Consider the bijection φ between this quotient ring and the complex numbers given by $a+bX+(X^2+1) \mapsto a+bi$. We can show that φ is a ring homomorphism. Indeed, it preserves addition, and $1+(X^2+1) \mapsto 1$, so it suffices to check that multiplication is preserved.

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

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

§8.4 Isomorphism theorems

Theorem 8.2 (First Isomorphism Theorem)

Let $\varphi\colon R \to S$ be a ring homomorphism. Then,

$$\ker\varphi \triangleleft R; \quad \operatorname{Im}\varphi \leq S; \quad R/\ker\varphi \cong \operatorname{Im}\varphi$$

Proof. We already saw that $\ker\varphi \triangleleft R$, Lemma 8.2.

We know that $\operatorname{Im}\varphi \leq (S,+)$. Now we show that $\operatorname{Im}\varphi$ is closed under multiplication.

$$\varphi(r_1)\varphi(r_2) = \varphi(r_1r_2) \in \operatorname{Im}\varphi$$

Finally,

$$1_S = \varphi(1_R) \in \operatorname{Im}\varphi$$

Hence $\operatorname{Im}\varphi$ is a subring of S.

Let $K = \ker\varphi$. Then, we define $\Phi\colon R/K \to \operatorname{Im}\varphi$ by $r+K \mapsto \varphi(r)$. By appealing to the first isomorphism theorem from groups, this is well-defined, a bijection, and a group homomorphism under addition. It therefore suffices to show that Φ preserves multiplication and maps the multiplicative identities to each other.

$$\begin{aligned}\Phi(1_R+K) &= \varphi(1_R) = 1_S \\ \Phi((r_1+K)(r_2+K)) &= \Phi(r_1r_2+K) \\ &= \varphi(r_1r_2)\end{aligned}$$

$$= \varphi(r_1)\varphi(r_2)$$
$$= \Phi(r_1 + K)\Phi(r_2 + K).$$

The result follows as required. □

Theorem 8.3 (Second Isomorphism Theorem)
Let $R \leq S$ and $J \triangleleft S$. Then,

$$R \cap J \triangleleft R$$
$$R + J = \{r + a : r \in R, a \in J\} \leq S$$
$$R/R \cap J \cong (R + J)/J \leq S/J$$

Proof. By the second isomorphism theorem for groups, $R + J \leq (S, +)$. Further, $1_S = 1_S + 0_S$, and since R is a subring, $1_S + 0_S \in R + J$ hence $1_S \in R \cap J$.

If $r_1, r_2 \in R$ and $a_1, a_2 \in J$, we have

$$(r_1 + a_1)(r_2 + a_2) = \underbrace{r_1 r_2}_{\in R} + \underbrace{r_1 a_2}_{\in J} + \underbrace{r_2 a_1}_{\in J} + \underbrace{a_1 a_2}_{\in J} \in R + J$$

Hence $R + J$ is closed under multiplication, giving $R + J \leq S$.

Let $\varphi : R \to S/J$ be defined by $r \mapsto r + J$. This is a ring homomorphism, since it is the composite of the inclusion homomorphism $R \subseteq S$[a] and the quotient map $S \to S/J$. The kernel of φ is the set $\{r \in R : r + J = J\} = R \cap J$. Since this is the kernel of a ring homomorphism, $R \cap J$ is an ideal in R. The image of φ is

$$\{r + J \mid r \in R\} = (R + J)/J \leq S/J.$$

By the first isomorphism theorem, $R/R \cap J \cong (R + J)/J$ as required. □

[a] This is just $r \mapsto r$ for $r \in R$.

Remark 19. If $I \triangleleft R$, there exists a bijection between ideals in R/I and the ideals of R containing I. Explicitly,

$$K \hookleftarrow \{r \in R \mid r + I \in K\}$$
$$J/I \mapsto J$$

Theorem 8.4 (Third Isomorphism Theorem)

Let $I \triangleleft R$ and $J \triangleleft R$ with $I \subseteq J$. Then,

$$J/I \triangleleft R/I$$
$$R/I/J/I \cong R/J$$

Proof. Let $\varphi\colon R/I \to R/J$ defined by $r + I \mapsto r + J$. We can check that this is a surjective ring homomorphism (well-defined since $I \subseteq J$) by considering the third isomorphism theorem for groups. Its kernel is $\{r + I\colon r \in J\} = J/I$, which is an ideal in R/I, and we conclude by use of the first isomorphism theorem. □

Remark 20. J/I is not a quotient ring, since J is not in general a ring; this notation should be interpreted as a set of cosets.

Example 8.4

Consider the surjective ring homomorphism $\varphi\colon \mathbb{R}[X] \to \mathbb{C}$ which is defined by

$$f = \sum_n a_n X^n \mapsto f(i) = \sum_n a_n i^n$$

Its kernel can be found by the Euclidean algorithm due to Proposition 7.1, yielding $\ker \varphi = (X^2 + 1)$. Applying the first isomorphism theorem, we immediately find $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$.

Example 8.5

Let R be a ring. Then there exists a unique ring homomorphism $i\colon \mathbb{Z} \to R$. Indeed, we must have

$$0_\mathbb{Z} \mapsto 0_R; \quad 1_\mathbb{Z} \mapsto 1_R$$

This inductively defines

$$n \mapsto \underbrace{1_R + \cdots + 1_R}_{n \text{ times}}$$

The negative integers are also uniquely defined, since any ring homomorphism is a group homomorphism.

$$-n \mapsto -(\underbrace{1_R + \cdots + 1_R}_{n \text{ times}})$$

We can show that any such construction is a ring homomorphism as required.

Then, the kernel of the ring homomorphism is an ideal of $\mathbb{Z}$, hence it is $n\mathbb{Z}$ for some n. Hence, by the first isomorphism theorem, any ring contains a copy of $\mathbb{Z}/n\mathbb{Z}$, since it is isomorphic to the image of i. If $n = 0$, then the ring contains a copy of $\mathbb{Z}$ itself, and if $n = 1$, then the ring is trivial since $0 = 1$.

Definition 8.8 (Characteristic)

The number n is known as the **characteristic** of R.

Example 8.6

For example, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristic zero. The rings $\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}[X]$ have characteristic p.

§9 Integral domains, maximal ideals and prime ideals

§9.1 Integral domains

Definition 9.1 (Integral Domain)

An **integral domain** is a ring R with $0 \neq 1$ such that for all $a, b \in R$, $ab = 0$ implies $a = 0$ or $b = 0$.

Definition 9.2 (Zero-Divisor)

A **zero divisor** in a ring R is a nonzero element $a \in R$ such that $ab = 0$ for some nonzero $b \in R$.

A ring is an integral domain iff it has no zero divisors.

Example 9.1

All fields are integral domains (if $ab = 0$ with $b \neq 0$, multiply by b^{-1} to get $a = 0$).

Example 9.2

Any subring of an integral domain is an integral domain. For instance, $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Z}[i] \leq \mathbb{C}$ are integral domains.

Example 9.3

The ring $\mathbb{Z} \times \mathbb{Z}$ is not an integral domain. Indeed, $(1,0) \cdot (0,1) = (0,0)$.

Lemma 9.1

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

Proof. We will show that any two nonzero elements produce a nonzero element. In particular, let

$$f = \sum_n a_n X^n; \quad g = \sum_n b_n X^n$$

Since these are nonzero, the leading coefficients a_n and b_m are nonzero. Here, the leading term of the product fg has form $a_n b_m X^{n+m}$. Since R is an integral domain, $a_n b_m \neq 0$, so fg is nonzero.

Further, the degree of fg is $n+m$, the sum of the degrees of f and g. □

Lemma 9.2

Let R be an integral domain, and $f \neq 0$ be a nonzero polynomial in $R[X]$. We define $\text{roots}(f) = \{a \in R \colon f(a) = 0\}$. Then $|\text{roots}(f)| \leq \deg(f)$.

Proof. Exercise on the Sheet 2. The main idea is to use the Euclidean algorithm on a root to extract out the linear factors. □

Theorem 9.1

Let F be a field. Then any finite subgroup G of $(F^\times, \cdot)$ is cyclic.

Proof. G is a finite abelian group. If G is not cyclic, we can apply Theorem 6.2 for finite abelian groups to show that there exists $H \leq G$ such that $H \cong C_{d_1} \times C_{d_1}$ [a] for some integer $d_1 \geq 2$. The polynomial $f(X) = X^{d_1} - 1 \in F[X]$ has degree d_1, but has at least d_1^2 roots, since any element of H is a root. This contradicts the previous lemma, Lemma 9.2. □

[a] We get from the theorem $G \cong \prod_i C_{d_i}$, as G not cyclic wlog $d_1 \mid d_2$ and so there exists a subgroup $C_{d_1} \leq C_{d_2}$.

Example 9.4

$\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ is cyclic.

Proposition 9.1

Any finite integral domain is a field.

Proof. Let $0 \neq a \in R$, where R is an integral domain. Consider the map $\varphi\colon R \to R$ given by $x \mapsto ax$.

If $\varphi(x) = \varphi(y)$, then $a(x-y) = 0$. But $a \neq 0$, hence $x - y = 0$ as R is an integral domain. Hence φ is injective. Since R is finite, φ is surjective so $\exists\, b$ s.t. $ab = 1$, i.e. a is a unit. This may be repeated for all a, thus R is a field. □

Theorem 9.2

Let R be an integral domain then $\exists$ a field F s.t.

1. $R \leq F$
2. Every element of F can be written in the form ab^{-1} where $a, b \in R$ and $b \neq 0$.

Such a field F is called the **field of fractions** of R.

Proof. Consider the set $S = \{(a,b) \in R^2 \colon b \neq 0\}$. We can define an equivalence relation

$$(a,b) \sim (c,d) \iff ad = bc$$

This is reflexive and symmetric. We can show directly that it is transitive.

$$\begin{aligned}(a,b) \sim (c,d) \sim (e,f) &\implies ad = bc;\ cf = de \\ &\implies adf = bcf = bde \\ &\implies d(af - be) = 0 \\ &\implies (a,b) \sim (e,f) \text{ as } d \neq 0 \text{ and } R \text{ an integral domain.}\end{aligned}$$

Hence $\sim$ is indeed an equivalence relation. Now, let $F = {}^{S}\!/_{\sim}$, and we write $\frac{a}{b}$ for the class $[(a,b)]$. We define the ring operations

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}; \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

These can be shown to be well-defined. Thus, F is a ring with identities $0_F = \frac{0_R}{1_R}$ and $1_F = \frac{1_R}{1_R}$.

If $\frac{a}{b} \neq 0_F$, then $a \neq 0$. Thus, $\frac{b}{a}$ exists, and $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1_R}{1_R} = 1_F$. Hence F is a field.

1. We can identify R with the subring of F given by $\left\{\frac{r}{1_R} : r \in R\right\} \leq F$. This is clearly isomorphic to R.

2. Further, any element of F can be written as $\frac{a}{b} = ab^{-1}$ as required. □

This is analogous to the construction of the rationals using the integers.

Example 9.5

$\mathbb{Z}$ is an integral domain with field of fractions $\mathbb{Q}$.

Example 9.6

Consider $\mathbb{C}[X]$. This has field of fractions $\mathbb{C}(X)$, called the field of *rational functions* in X.

§9.2 Maximal ideals

Definition 9.3 (Maximal Ideal)

An ideal $I \triangleleft R$ is **maximal** if $I \neq R$ and, if $I \subseteq J \triangleleft R$, we have $J = I$ or $J = R$.

So a maximal ideal is the largest proper ideal.

Lemma 9.3

A nonzero ring R is a field iff its only ideals are zero or R.

Proof. ($\implies$): Suppose R is a field. If $0 \neq I \triangleleft R$, then I contains a nonzero element, which is a unit since R is a field. We have seen that an ideal containing a unit implies it is the whole ring, hence $I = R$.

($\impliedby$): Now, suppose a ring R has ideals that are only zero or R. If $0 \neq x \in R$, consider (x). This is nonzero since it contains x. By assumption, $(x) = R$. Thus, the element 1 lies in (x). Hence, there exists $y \in R$ such that $xy = 1$, and hence this y is the multiplicative inverse as required. □

Proposition 9.2

Let $I \triangleleft R$. Then I is maximal iff R/I is a field.

Proof. R/I is a field iff its ideals are either zero, denoted I/I[a], or R/I itself. By Remark 19, I and R are the only ideals in R which contain I. Equivalently, $I \triangleleft R$

is maximal. □

[a] This is not a ring but the set of cosets given by elements of I.

§9.3 Prime ideals

Definition 9.4 (Prime Ideals)

An ideal $I \triangleleft R$ is **prime** if $I \neq R$ and for all $a, b \in R$ such that $ab \in I$, we have $a \in I$ or $b \in I$.

Example 9.7

The ideals in the integers are $n\mathbb{Z}$ for some $n \geq 0$. $n\mathbb{Z}$ is a prime ideal iff n is prime or zero.

The case for $n = 0$ is trivial.

If $n \neq 0$ we can use the property that $p \mid ab$ implies either $p \mid a$ or $p \mid b$. So if $ab \in p\mathbb{Z}$ then $a \in p\mathbb{Z}$ or $b \in b\mathbb{Z}$.

Conversely, if n is composite, we can write $n = uv$ for $u, v > 1$. Then $uv \in n\mathbb{Z}$ but $u, v \notin n\mathbb{Z}$.

Proposition 9.3

Let $I \triangleleft R$. Then I is prime iff R/I is an integral domain.

Proof. If I is prime, then for all $ab \in I$ we have $a \in I$ or $b \in I$. Equivalently, for all $a + I, b + I \in R/I$, we have $(a + I)(b + I) = 0 + I$ if $a + I = 0 + I$ or $b + I = 0 + I$. This is the definition of an integral domain. □

Remark 21. If I is a maximal ideal, then R/I is a field by proposition 9.2. A field is an integral domain. Hence any maximal ideal is prime.

Remark 22. If the characteristic of a ring is n, then $\mathbb{Z}/n\mathbb{Z} \leq R$. In particular, if R is an integral domain, then $\mathbb{Z}/n\mathbb{Z}$ must be an integral domain. Equivalently, $n\mathbb{Z} \triangleleft \mathbb{Z}$ is a prime ideal. Hence n is zero or prime. Thus, in an integral domain, the characteristic must either be zero or prime.
In particular, a field always has a characteristic, which is either zero (in which case it contains $\mathbb{Z}$ and hence $\mathbb{Q}$) or prime (in which case it contains $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ which is already a field).

§10 Factorisation in integral domains

In this section, let R be an integral domain.

§10.1 Prime and irreducible elements

Recall that an element $a \in R$ is a unit if it has a multiplicative inverse in R. Equivalently, an element a is a unit if and only if $(a) = R$. Indeed, if $(a) = R$, then $1 \in (a)$ hence there exists a multiple of a equal to 1. We denote the set of units in R by $R^\times$.

Definition 10.1 (Divides)

An element $a \in R$ **divides** $b \in R$, written $a \mid b$, if there exists $c \in R$ such that $b = ac$. Equivalently, $(b) \subseteq (a)$.

Definition 10.2 (Associates)

Two elements $a, b \in R$ are **associates** if $a = bc$ where c is a unit. Informally, the two elements differ by multiplication by a unit. Equivalently, $(a) = (b)$.

Definition 10.3

An element $r \in R$ is **irreducible** if $r \neq 0$ is not a unit, and $r = ab$ implies a or b is a unit.

Definition 10.4 (Prime)

An element $r \in R$ is **prime** if $r \neq 0$ is not a unit and $r \mid ab$ implies $r \mid a$ or $r \mid b$.

Remark 23. These properties depend on the ambient ring R; for instance, 2 is prime and irreducible in $\mathbb{Z}$, but neither prime nor irreducible in $\mathbb{Q}$ as it's a unit.
The polynomial $2X$ is irreducible in $\mathbb{Q}[X]$, but not in $\mathbb{Z}[X]$.

Lemma 10.1

$(r) \lhd R$ is a prime ideal iff $r = 0$ or r is prime.

Proof. ($\implies$): Suppose (r) is a prime ideal with $r \neq 0$. Since prime ideals are proper, r cannot be a unit. Suppose $r \mid ab$, or equivalently, $ab \in (r)$. By the definition of a prime ideal, $a \in (r)$ or $b \in (r)$. Hence, $r \mid a$ or $r \mid b$. By definition of a prime element, r is prime.

($\Longleftarrow$): Conversely, first note that the zero ideal $(0) = \{0\}$ is a prime ideal, since R is an integral domain.
Suppose r is prime. We know $(r) \neq R$ since r is not a unit. If $ab \in (r)$, then $r \mid ab$, so $r \mid a$ or $r \mid b$, giving $a \in (r)$ or $b \in (r)$ as required for (r) to be a prime ideal. □

Lemma 10.2

Prime elements are irreducible.

Proof. Let r be prime. Then r is nonzero and not a unit. Suppose $r = ab$. Then, in particular, $r \mid ab$, so $r \mid a$ or $r \mid b$ by primality. Let $r \mid a$ without loss of generality. Hence $a = rc$ for some element $c \in R$. Then, $r = ab = rcb$, so $r(1 - cb) = 0$. Since R is an integral domain, and $r \neq 0$, we have $cb = 1$, so b is a unit. □

Example 10.1

The converse does not hold in general. Let

$$R = \mathbb{Z}[\sqrt{-5}] = \left\{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\right\} \leq \mathbb{C}; \quad R \cong \mathbb{Z}[X]/(X^2 + 5)$$

Since R is a subring of the field $\mathbb{C}$, it is an integral domain. We can define the *norm* $N \colon R \to \mathbb{Z}$ by $N(a + b\sqrt{-5}) = a^2 + 5b^2 \geq 0$. Note that this norm is multiplicative: $N(z_1 z_2) = N(z_1)N(z_2)$.

We claim that the units are exactly ± 1. Indeed, if $r \in R^\times$, then $rs = 1$ for some element $s \in R$. Then, $N(r)N(s) = N(1) = 1$, so $N(r) = N(s) = 1$. But the only elements $r \in R$ with $N(r) = 1$ are $r = \pm 1$.

We will now show that the element $2 \in R$ is irreducible. Suppose $2 = rs$ for $r, s \in R$. By the multiplicative property of N, $N(2) = 4 = N(r)N(s)$ can only be satisfied by $N(r), N(s) \in \{1, 2, 4\}$. Since $a^2 + 5b^2 = 2$ has no integer solutions, R has no elements of norm 2. Hence, either r or s has unit norm and is thus a unit by the above discussion. We can show similarly that $3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are irreducible, as there exist no elements of norm 3.

We can now compute directly that $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$, hence $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$. But $2 \nmid (1 + \sqrt{-5})$ and $2 \nmid (1 - \sqrt{-5})$, which can be checked by taking norms. Hence, 2 is irreducible but not a prime.

Takeaways
So here is an example showing irreducible $\not\Longrightarrow$ prime
In order to construct this example, we have exhibited two factorisations of 6 into irreducibles: $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$. Since $R^\times = \{\pm 1\}$, these irreducibles in the factorisations are not associates.

§10.2 Principal ideal domains

Definition 10.5 (Principal Ideal Domain)

An integral domain R is a **principal ideal domain** (PID) if all ideals are principal ideals. In other words, for all ideals $I \triangleleft R$, there exists an element r such that $I = (r)$.

Example 10.2

$\mathbb{Z}$ is a principal ideal domain by Lemma 8.3.

Proposition 10.1

In a principal ideal domain, all irreducible elements are prime.

Proof. Let $r \in R$ be irreducible, and suppose $r \mid ab$. If $r \mid a$, the proof is complete, so suppose $r \nmid a$.

Since R is a principal ideal domain, the ideal (a, r) is generated by a single element $d \in R$. In particular, since $r \in (d)$, we have $d \mid r$ so $r = cd$ for some $c \in R$.

Since r is irreducible, either c or d is a unit. If c is a unit, $(a, r) = (d) = (r)$, so in particular $r \mid a$, which contradicts the assumption that $r \nmid a$, so c cannot be a unit. Thus, d is a unit. In this case, $(a, r) = R$. By definition of (a, r), there exist $s, t \in R$ such that $1 = sa + tr$. Then, $b = sab + trb$. We have $r \mid sab$ since $r \mid ab$, and we know $r \mid trb$. Hence $r \mid b$ as required. □

Lemma 10.3

Let R be a principal ideal domain and $0 \neq r \in R$ Then r is irreducible iff (r) is maximal.

Proof. ($\implies$): Since r is not a unit, $(r) \neq R$.
Suppose $(r) \subseteq J \subseteq R$ where J is an ideal in R. Since R is a principal ideal domain, $J = (a)$ for some $a \in R$. In particular, $r = ab$ for some $b \in R$, since $(r) \subseteq J$. Since r is irreducible, either a or b is a unit. But if a is a unit, we have $J = R$. If b is a unit, then a and r are associates so they generate the same ideal. Hence, (r) is maximal.

($\impliedby$): Note that r is not a unit, since $(r) \neq R$. Suppose $r = ab$. Then $(r) \subseteq (a) \subseteq R$. But since (r) is maximal, either $(a) = (r)$ or $(a) = R$. If $(a) = (r)$, then b is a unit. If $(a) = R$, then a is a unit. Hence r is irreducible. □

Remark 24. 1. The converse direction doesn't depend on R being a PID only that it's an integral domain.

2. If R is a PID and $0 \neq r \in R$. Then, (r) is maximal iff r is irreducible (Lemma 10.3), which is true iff r is prime (Lemma 10.2 and proposition 10.1), which is equivalent to the fact that (r) is prime (Lemma 10.1). Hence, the maximal ideals are the nonzero prime ideals.

Definition 10.6 (Euclidean Domain)

An integral domain is a **Euclidean domain** if there exists a function $\varphi\colon R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that, for all $a, b \in R$.

1. If $a \mid b$ then $\varphi(a) \leq \varphi(b)$;
2. If $b \neq 0$ then $\exists\, q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\varphi(r) < \varphi(b)$.

Such a φ is called a **Euclidean function**.

Example 10.3

$\mathbb{Z}$ is a Euclidean domain, where the Euclidean function φ is the absolute value function.

Proposition 10.2

Euclidean domains are principal ideal domains.

Proof. Let R have Euclidean function φ. Let $I \triangleleft R$ be a nonzero ideal.
Let $b \in I \setminus \{0\}$ that minimises $\varphi(b)$. Then $(b) \subseteq I$.
For any element $a \in I$, we can use the Euclidean algorithm to show $a = bq + r$ where $r = 0$ or $\varphi(r) < \varphi(b)$. But since $r = a - bq \in I$, $\varphi(r)$ cannot be lower than the minimal element $\varphi(b)$. Thus $r = 0$, so $a = bq$. Hence, $I = (b)$, so all ideals are principal. □

Remark 25. In the above proof, only the second property of the Euclidean function was used. The first property is included in the definition since it will allow us to easily describe the units in the ring.

$$R^\times = \{u \in R\colon u \neq 0, \varphi(u) = \varphi(1)\}$$

It can be shown that, if there exists a function φ satisfying (ii), there exists a (possibly not unique) function φ' satisfying (i) and (ii).

Example 10.4

Let F be a field. Then $F[X]$ is a Euclidean domain with Euclidean function $\varphi(f) = \deg(f)$. The second property of Euclidean domains is proven using Proposition 7.1

whilst the first is easy to check.

So $F[X]$ is a PID by Proposition 10.2

Example 10.5

The ring $R = \mathbb{Z}[i]$ is a Euclidean domain with $\varphi(u+iv) = N(u+iv) = u^2+v^2$. Since the norm is multiplicative, $N(zw) = N(z)N(w)$ which immediately gives property (i) in the definition.
Consider $z, w \in \mathbb{Z}[i]$ where $w \neq 0$. Consider $\frac{z}{w} \in \mathbb{C}$. This has distance less than 1 from the nearest element q of R, i.e. $|z/w - q| < 1$ as R is every complex point with integer components.
Let $r = z - wq \in R$. Then $z = wq + r$ where

$$\varphi(r) = |r|^2 = |z - wq|^2 < |w|^2 = \varphi(w)$$

So property (ii) is satisfied.

So $\mathbb{Z}[i]$ is a PID by Proposition 10.2

Example 10.6

Let A be a nonzero $n \times n$ matrix over a field F. Let $I = \{f \in F[X] \colon f(A) = 0\}$.

I is an ideal. Indeed, if $f, g \in I$, then $(f-g)(A) = f(A) - g(A) = 0$, and for $f \in I$ and $g \in F[X]$, we have $(f \cdot g)(A) = f(A) \cdot g(A) = 0$ as required.

Since $F[X]$ is a principal ideal domain, $I = (f)$ for some polynomial $f \in F[X]$. All units in $F[X]$ are the nonzero constant polynomials[a]. Hence, the polynomial of smallest degree in I is unique up to multiplication by a unit, so without loss of generality we may assume f is monic.

Then for $g \in F[X]$, $g(A) = 0 \iff g \in I = (f)$, i.e. $f \mid g$. Thus f is the minimal polynomial of A.

[a] Can check by looking at the first property of a Euclidean domain.

Example 10.7 (Field of order 8)

Let $\mathbb{F}_2$ be the finite field of order 2, which is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Let $f(X)$ be the polynomial $X^3 + X + 1 \in \mathbb{F}_2[X]$.

We claim that f is irreducible. Suppose $f = gh$ where the degrees of g, h are positive. Since the degree of f is 3, one of g, h must have degree 1. Hence f has a root. But we can check that $f(0) = f(1) = 1$[a] so f has no root in $\mathbb{F}_2$. Hence f is irreducible as required.

Since $\mathbb{F}_2[X]$ is a principal ideal domain, we have that $(f) \triangleleft \mathbb{F}_2[X]$ is a maximal ideal by Lemma 10.3. Hence, $\mathbb{F}_2[X]/(f)$ is a field. We can verify that this field has order 8, using the Euclidean algorithm. Any element in this quotient is $aX^2+bX+c+(f)$ for $a, b, c \in \mathbb{F}_2$. We can show that all 8 of these possibilities yields different polynomials. So we have constructed a field of order 8. This technique will be explored further in Part II Galois Theory.

[a] Note you need to check $f(1) = f(3) = f(5) = \cdots = 0$ in $\mathbb{Z}$ i.e. $f(1) = 0$ in $\mathbb{F}_2$.

Example 10.8

The ring $\mathbb{Z}[X]$ is not a principal ideal domain. Consider the ideal $I = (2, X) \triangleleft \mathbb{Z}[X]$. We can write

$$I = \{2f_1(X) + Xf_2(X) \colon f_1, f_2 \in \mathbb{Z}[X]\} = \{f \in \mathbb{Z}[X] \colon 2 \mid f(0)\}$$

Suppose $I = (f)$ for some element f. Since $2 \in I$, we must have $2 = fg$ for some polynomial g. By comparing degrees, the degrees of f and g must be zero, since $\mathbb{Z}$ is an integral domain. Hence f is an integer, so $f = \pm 1$ or $f = \pm 2$. If $f = \pm 1$ then $I = \mathbb{Z}[X]$, and if $f = \pm 2$ then $I = 2\mathbb{Z}[X]$. These both lead to contradictions, since $1 \in I$ and $X \notin I$ respectively.

§10.3 Unique factorisation domains

Definition 10.7 (Unique Factorisation Domain)

An integral domain is a **unique factorisation domain** (UFD) if

1. Every nonzero, non-unit element is a product of irreducibles;
2. If $p_1 \cdots p_m = q_1 \cdots q_n$ where p_i, q_i are irreducible, then $m = n$, and p_i, q_i are associates, up to reordering.

GOAL: Show PID $\implies$ UFD.

Remark 26. Any field is a UFD as there are no non-unit elements.

Proposition 10.3

Let R be an integral domain satisfying property (1) above (every nonzero, non-unit element is a product of irreducibles). Then R is a unique factorisation domain iff every irreducible is prime.

Proof. ($\implies$): Let $p \in R$ be irreducible, and $p \mid ab$. Then $ab = pc$ for some $c \in R$. Writing a, b, c as products of irreducibles, it follows from uniqueness of factorisation (2) that $p \mid a$ or $p \mid b$. Hence p is prime.

($\impliedby$): Suppose $p_1 \cdots p_m = q_1 \cdots q_n$ where p_i, q_i are irreducible and hence prime. Since $p_1 \mid q_1 \cdots q_n$, we have $p_1 \mid q_i$ for some i. After reordering, we may assume that $p_1 \mid q_1$, so $p_1 u = q_1$ for $u \in R$. Since q_1 is irreducible, u is a unit since p_1 cannot be a unit. Hence p_1, q_1 are associates. Cancelling p_1 from both sides, we find $p_2 \cdots p_m = u q_2 \cdots q_n$. We may absorb this unit into q_2 without loss of generality. Inductively, all p_i and q_i are associates, for each i. Hence R is a unique factorisation domain. □

Definition 10.8 (Noetherian)

Let R be a ring. Suppose, for all nested sequences of ideals in R written $I_1 \subseteq I_2 \subseteq \cdots$, $\exists\, N$ such that $I_n = I_{n+1}$ for all $n \geq N$. Then, we say that R is a **Noetherian** ring.

This condition is known as the 'ascending chain condition'. In other words, we cannot infinitely nest distinct ideals in a Noetherian ring.

Lemma 10.4

Principal ideal domains are Noetherian rings.

Proof. Let $I = \bigcup_{i=1}^{\infty} I_i$. Then, I is an ideal in R (Sheet 2). Since R is a principal ideal domain, $I = (a)$ for some $a \in R$. Then $a \in \bigcup_{i=1}^{\infty} I_i$, so in particular $a \in I_N$ for some N. But then for all $n \geq N$, $(a) \subseteq I_N \subseteq I_n \subseteq I_{n+1} \subseteq I = (a)$. So all inclusions are equalities, so in particular $I_n = I_{n+1}$. □

Theorem 10.1

If R is a principal ideal domain, then it is a unique factorisation domain.

Proof. First, we verify property (1) of UFD, that every nonzero, non-unit element is a product of irreducibles. Let $x \neq 0$ be an element of R which is not a unit. Suppose x does not factor as a product of irreducibles. This implies that x is not irreducible. By definition of irreducibility, we can write x as the product of two elements x_1, y_1 where x_1, y_1 are not units. Then either x_1 or y_1 is not a product of irreducibles, so wlog we can suppose x_1 is not a product of irreducibles. We have $(x) \subseteq (x_1)$. This inclusion is strict, since y_1 is not a unit. Now, we can write $x_1 = x_2 y_2$ where x_2, y_2 are not units, and inductively we can create $(x) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \cdots$. But R is Noetherian, so this is a contradiction to Lemma 10.4. So every nonzero, non-unit

element is indeed a product of irreducibles.

By Proposition 10.3, it suffices to show that every irreducible is prime. This has already been shown previously by Proposition 10.1. Hence R is a unique factorisation domain. □

Example 10.9

We have shown that ED $\implies$ PID $\implies$ UFD $\implies$ UFD. We now provide examples for counterexamples to the converses.

The ring $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain since 2 is a zero divisor, hence it is not a ED, PID or UFD either.

The ring $\mathbb{Z}[\sqrt{-5}] \leq \mathbb{C}$ is integral, but not a unique factorisation domain and hence not ED or PID.

The ring $\mathbb{Z}[X]$ has been shown to be not a principal ideal domain. We can show using later results that this is a unique factorisation domain.

We can construct the ring $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$, which can be shown to be not a Euclidean domain, but is a principal ideal domain. This will be proved in Part II Number Fields.

Finally, $\mathbb{Z}[i]$ is a Euclidean domain, and is hence a principal ideal domain, a unique factorisation domain, and an integral domain.

Definition 10.9 (Common Divisors and Multiples)

Let R be an integral domain.

1. $d \in R$ is a **common divisor** of $a_1, \ldots, a_n \in R$ if $d \mid a_i$ for all i;
2. $d \in R$ is a **greatest common divisor** of $a_1, \ldots, a_n$ if for all common divisors d', we have $d' \mid d$;
3. $m \in R$ is a **common multiple** of $a_1, \ldots, a_n$ if $a_i \mid m$ for all i;
4. $m \in R$ is a **least common multiple** of $a_1, \ldots, a_n$ if for all common multiples m', we have $m \mid m'$.

Warning 10.1

These do not need to exist in a given ring.

Remark 27. Greatest common divisors and lowest common multiples are unique up to associates, if they exist.

Proposition 10.4

In unique factorisation domains, greatest common divisors and least common multiples always exist.

Proof. Let $a_i = u_i \prod_j p_j^{n_{ij}}$ where the p_j are irreducible and pairwise non-associate, u_i is a unit, and $n_{ij} \in \mathbb{Z}_{\geq 0}$. We claim that $d = \prod_j p_j^{m_j}$, where $m_j = \min_{1 \leq i \leq n} n_{ij}$, is the greatest common divisor. Certainly d is a common divisor. If d' is a common divisor, then d' can be written as a product of irreducibles, which will be denoted $d' = w \prod_j p_i^{t_j}$ for a unit w. We can see that $t_j \leq n_{ij}$ for all i, so in particular, $t_j \leq m_j$. This implies $d' \mid d$. Hence d is a greatest common divisor. The argument for the least common multiple is similar, replacing minima with maxima. □

§11 Factorisation in polynomial rings

Theorem 11.1

Let R be a unique factorisation domain. Then $R[X]$ is also a unique factorisation domain.

The proof for this theorem will require a number of key lemmas. In this subsection, R will denote a unique factorisation domain, with field of fractions F. We have $R[X] \leq F[X]$. Since polynomial rings over fields are Euclidean domains, $F[X]$ is a principal ideal domain, and hence a unique factorisation domain. This does not immediately imply that $R[X]$ is a unique factorisation domain, however.

Definition 11.1 (Content)

The **content** of a polynomial $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ is $c(f) = \gcd\{a_0, \ldots, a_n\}$. This is well-defined up to multiplication by a unit.

Definition 11.2 (Primitive)

We say that f is **primitive** if $c(f)$ is a unit.

Lemma 11.1

The product of primitive polynomials is primitive. Further, for $f, g \in R[X]$, $c(fg)$ and $c(f)c(g)$ are associates.

Proof. Let $f = \sum_{i=0}^{n} a_i X^i$ and $g = \sum_{i=0}^{m} b_i X^i$. Suppose fg is not primitive, so $c(fg)$ is not a unit. This implies that there exists a prime p such that $p \mid c(fg)$. Since f, g are primitive, $p \nmid c(f)$ and $p \nmid c(g)$.

p does not divide all of the a_k or the b_ℓ. Let k, ℓ be the smallest values such that $p \nmid a_k$ and $p \nmid b_\ell$. Then, the coefficient of $X^{k+\ell}$ in fg is given by

$$\sum_{i+j=k+\ell} a_i b_j = \underbrace{\cdots + a_{k-1} b_{\ell+1}}_{\text{divisible by } p} + a_k b_\ell + \underbrace{a_{k+1} b_{\ell-1} + \cdots}_{\text{divisible by } p}$$

Thus $p \mid a_k b_\ell$ as $p \mid c(fg)$. This implies $p \mid a_k$ or $p \mid b_\ell$ as p prime ↯.

To prove the second part, let $f = c(f) f_0$ for some $f_0 \in R[X]$. Here, f_0 is primitive. Similarly, $g = c(g) g_0$ for a primitive g_0. Thus $fg = c(f)c(g) f_0 g_0$. The expression $f_0 g_0$ is a primitive polynomial by the first part, so $c(fg)$ is equal to $c(f)c(g)$ up to associates. □

Corollary 11.1

If $p \in R$ is prime in R, then p is prime in $R[X]$.

Proof. Since R is an integral domain, we have $R[X]^\times = R^\times$ [a], so p is not a unit. Let $f \in R[X]$. Then $p \mid f$ in $R[X] \iff p \mid c(f)$ in R. Thus, if $p \mid gh$ in $R[X]$, we have $p \mid c(gh) =$ [b] $c(g)c(h)$. In particular, since p is prime in R, we have $p \mid c(g)$ or $p \mid c(h)$, so $p \mid g$ or $p \mid h$. So p is prime in $R[X]$. □

[a] Suppose $a, b \in R[X]$ s.t. $ab = 1$ then as degrees of polynomials add under multiplication $\deg a = \deg b = 0$ so $a, b \in R$.

[b] When we use equality with contents, we implicitly mean they are associates.

Lemma 11.2

Let $f, g \in R[X]$, where g is primitive. Then if $g \mid f$ in $F[X]$, then $g \mid f$ in $R[X]$.

Proof. Let $f = gh$, where $h \in F[X]$. We can find a nonzero $a \in R$, such that $ah \in R[X]$. In particular, we can multiply the denominators of the coefficients of h to form a. Now, $ah = c(ah)h_0$ where h_0 is primitive. Then $af = c(ah)h_0 g$. Since h_0 and g are primitive, so is $h_0 g$. Thus, taking contents, $a \mid c(ah)$. This implies $h \in R[X]$. Hence $g \mid f$ in $R[X]$. □

Lemma 11.3 (Gauss' lemma)

Let $f \in R[X]$ be primitive. Then if f is irreducible in $R[X]$, we have that f is

irreducible in $F[X]$.

Proof. Since $f \in R[X]$ is irreducible and primitive, its degree must be larger than zero[a]. Hence f is not a unit in $F[X]$.

Suppose f is not irreducible in $F[X]$, so $f = gh$ for $g, h \in F[X]$ with degrees larger than zero. Let $\lambda \in F^\times$ such that $\lambda^{-1}g \in R[X]$ is primitive. (For example, let $b \in R$ such that $bg \in R[X]$ clears out denominators, then $bg = c(bg)g_0$, giving $\lambda = c(bg)b^{-1}$.) Replacing g by $\lambda^{-1}g$ and h by λh, we still have a factorisation of f. Hence, we may assume without loss of generality that $g \in R[X]$ and is primitive. By Lemma 11.2, we have that $h \in R[X]$, and we already saw that $\deg h > 0$. This contradicts irreducibility ↯. □

[a] If $\deg f = 0$ and f primitive, f is a unit but this contradicts it being irreducible.

Remark 28. We will see that the reverse implication in Gauss' lemma also holds.

Lemma 11.4

Let $g \in R[X]$ be primitive. If g is prime in $F[X]$, then g is prime in $R[X]$.

Proof. It suffices to show that if $f_1, f_2 \in R[X]$, then $g \mid f_1 f_2$ implies $g \mid f_1$ or $g \mid f_2$. Since g is prime in $F[X]$, $g \mid f_1$ or $g \mid f_2$ in $F[X]$. By Lemma 11.2, $g \mid f_1$ or $g \mid f_2$ in $R[X]$ as required. □

We can now prove Theorem 11.1, that polynomial rings over unique factorisation domains are unique factorisation domains.

Proof. Let $f \in R[X]$. Then, $f = c(f)f_0$ for f_0 primitive in $R[X]$. Since R is a unique factorisation domain, $c(f)$ is a product of irreducibles in R. If an element of R is irreducible, it is irreducible as an element of $R[X]$. Hence, it suffices to find a factorisation of f_0.

Suppose f_0 is not irreducible, so $f_0 = gh$ for $g, h \in R[X]$. Since f_0 is primitive, g and h are primitive and $\deg g, \deg h > 0$[a]. By induction on the degree, we can factor f_0 as a product of primitive irreducibles in $R[X]$. So property (1) of UFD is shown.

It now suffices to show uniqueness of the factorisation. By Proposition 10.3, it in fact suffices to show that every irreducible element of $R[X]$ is prime. Let f be irreducible. Write $f = c(f)f_0$, where f_0 is primitive. Since f is irreducible, either f_0 a unit so f must be constant or $c(f)$ a unit so f primitive.

Suppose f is constant. Since f is irreducible in $R[X]$, it must be irreducible in R. As R is a unique factorisation domain, f is prime in R. By Corollary 11.1, f is prime in $R[X]$.

Now, suppose f is primitive. Since f is irreducible in $R[X]$, we can use Gauss' lemma to show that f is irreducible in $F[X]$. Thus, f is prime in $F[X]$, as $F[X]$ is a unique factorisation domain. Finally, we can see that f is prime in $R[X]$ by Lemma 11.4. □

[a] If $\deg g = 0$, as g primitive it must be a unit but we assume it is not.

Remark 29. By Lemma 10.2, we know that the prime elements in an integral domain are irreducible. This implies that the implications in the last paragraph above are in fact equivalences. In particular, in Gauss' lemma, the implication is an equivalence.

Example 11.1

Theorem 11.1 implies that $\mathbb{Z}[X]$ is a unique factorisation domain.

Example 11.2

Let $R[X_1, \ldots, X_n]$ be the ring of polynomials in n variables. Define inductively $R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$. Applying Theorem 11.1 inductively $\implies$ $R[X_1, \ldots, X_n]$ is a UFD if R is.

§11.1 Eisenstein's criterion

Proposition 11.1 (Eisenstein's Criterion)

Let R be a unique factorisation domain, and $f(X) = \sum_{i=0}^{n} a_i X^i \in R[X]$ be a primitive polynomial. Let $p \in R$ be irreducible (or, equivalently, prime) such that

1. $p \nmid a_n$;
2. $p \mid a_i$ for all $i < n$; and
3. $p^2 \nmid a_0$.

Then f is irreducible in $R[X]$.

Proof. Suppose $f = gh$ for $g, h \in R[X]$ not units. Since f is primitive, g, h must have positive degree. Let $g(X) = \sum_{i=0}^{k} r_i X^i$ and $h(X) = \sum_{i=0}^{\ell} s_i X^i$, so $k + \ell = n$. Then $p \nmid a_n = r_k s_\ell$, so $p \nmid r_k$ and $p \nmid s_\ell$. Further, $p \mid a_0 = r_0 s_0$ so $p \mid r_0$ or $p \mid s_0$. Wlog, we may assume $p \mid r_0$. There exists a minimal $j \leq k$ such that $p \mid r_i \ \forall\ i < j$ but $p \nmid r_j$.

$$a_j = \underbrace{r_0 s_j + r_1 s_{j-1} + \cdots + r_{j-1} s_1}_{p \mid r_i \ \forall\, i<j} + r_j s_0$$

By assumption, a_j is divisible by p since $j < n$. Further, the first j terms in the expansion are divisible by p. Thus, $p \mid r_j s_0$. By assumption, $p \nmid r_j$, so $p \mid s_0$, so $p^2 \mid r_0 s_0 = a_0$, contradicting the third criterion ↯. □

Example 11.3

Let $f(X) = X^3 + 2X + 5 \in \mathbb{Z}[X]$. We will show this is irreducible as a polynomial over $\mathbb{Q}$. If f is reducible in $\mathbb{Z}[X]$, then it factorises as $f(X) = (X + a)(X^2 + bX + c)$ up to multiplication by units. Here, $ac = 5$. But $\pm 1, \pm 5$ are not roots of f ↯, so this is irreducible in $\mathbb{Z}[X]$. By Gauss' lemma, f is irreducible in $\mathbb{Q}[X]$, since $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$. In particular, $\mathbb{Q}[X]/(f)$ is a field by Lemma 10.3, since the ideal (f) is maximal.

Example 11.4

Let $p \in \mathbb{Z}$ be a prime, and let $f(X) = X^n - p$. By Eisenstein's criterion, f is irreducible in $\mathbb{Z}[X]$. It is then irreducible in $\mathbb{Q}[X]$ by Gauss' lemma.

Example 11.5

Consider $f(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Z}[X]$, where p is prime. Eisenstein's criterion does not apply directly. Consider

$$f(X) = \frac{X^p - 1}{X - 1}; \quad Y = X - 1$$

By using this substitution of Y,

$$f(Y + 1) = \frac{(Y+1)^p - 1}{Y - 1 + 1} = Y^{p-1} + \binom{p}{1} Y^{p-2} + \cdots + \binom{p}{p-2} Y + \binom{p}{p-1}$$

We can apply Eisenstein's criterion to this new polynomial, since $p \mid \binom{p}{i}$ for all $1 \leq i \leq p - 1$, and $p^2 \nmid \binom{p}{p-1} = p$. Thus, $f(Y + 1)$ is irreducible in $\mathbb{Z}[Y]$, so $f(X)$ is irreducible in $\mathbb{Z}[X]$. Of course, $f(X)$ is therefore irreducible in $\mathbb{Q}[X]$ as before.

§12 Algebraic integers

§12.1 Gaussian integers

Recall the ring of Gaussian integers $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\} \leq \mathbb{C}$. There is a norm function $N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$ given by $a + bi \mapsto a^2 + b^2$, and $N(xy) = N(x)N(y)$. This norm is a Euclidean function, giving the Gaussian integers the structure of a Euclidean domain and hence a PID and UFD. So the primes are the irreducibles in $\mathbb{Z}[i]$. The units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$, since they are the only elements of unit norm.

Example 12.1

2 is not irreducible in $\mathbb{Z}[i]$, since it factors as $(1+i)(1-i)$. 5 is not irreducible, since it factors as $(2+i)(2-i)$. These are nontrivial factorisations since the norms of the factors are not unit length.

3 is a prime, since it is irreducible. Indeed, $N(3) = 9$, so if 3 were reducible it would factor as ab where $N(a) = N(b) = 3$. But $\mathbb{Z}[i]$ has no elements of norm 3. Similarly, 7 is a prime.

Proposition 12.1

Let $p \in \mathbb{Z}$ be a prime. Then, the following are equivalent.

1. p is not prime in $\mathbb{Z}[i]$;
2. $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$;
3. $p = 2$ or $p \equiv 1 \mod 4$.

Proof. (1) $\implies$ (2): Let $p = xy$ for $x, y \in \mathbb{Z}[i]$ not units. Then, $p^2 = N(p) = N(x)N(y)$. Since x, y are not units, $N(x), N(y) > 1$ and in particular $N(x) = N(y) = p$. Writing $x = a + bi$ for $a, b \in \mathbb{Z}$, we have $p = N(x) = a^2 + b^2$, which is the condition in (2).

(2) $\implies$ (3): The only squares modulo 4 are 0 and 1. Since $p \equiv a^2 + b^2 \mod 4$, we have that p cannot be congruent to 3, modulo 4.

(3) $\implies$ (1): We have already observed above that 2 is not prime in $\mathbb{Z}[i]$. It hence suffices to consider the case where $p \equiv 1 \mod 4$. We have that $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ is cyclic of order $p-1$ by Theorem 9.1. Hence, if $p \equiv 1 \mod 4$, we have that $4 \mid p-1$, and hence $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ contains an element of order 4, i.e. $\exists\, x \in \mathbb{Z}$ with $x^4 \equiv 1 \mod p$, but $x^2 \not\equiv 1 \mod p$[a]. Then $x^2 \equiv -1 \mod p$, or in other words, $p \mid (x^2+1)$. But this factorises as $p \mid (x+i)(x-i)$. We can see that $p \nmid x+i$, $p \nmid x-i$, so p cannot

be prime. □

[a] Otherwise x would be order 2

Remark 30. The proof that (iii) implies (ii) is entirely nontrivial. It required lots of theory in order to reach the result, even though its statement did not require even the notion of a complex number.

Theorem 12.1

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

1. $a + bi$, where $a, b \in \mathbb{Z}$ and $a^2 + b^2 = p$[a] is a prime in $\mathbb{Z}$ with $p = 2$ or $p \equiv 1 \mod 4$; and
2. the primes p in $\mathbb{Z}$ satisfying $p \equiv 3 \mod 4$.

[a] Previous theorem implies p not prime in $\mathbb{Z}[i]$, but $a + bi \neq p$ and we care about $a + bi$.

Proof. First, we must check that all such elements are prime. For (1), note that $N(a+bi) = p$ is prime, so if $a + bi = uv$ then either $N(u)$ or $N(v) = 1$. Thus $a + bi$ is irreducible, hence prime.
(2) follows from Proposition 12.1.

It now suffices to show that any prime in the Gaussian integers satisfies one of the two above conditions. Let z be prime in $\mathbb{Z}[i]$. We note that $\overline{z}$ is also irreducible. Now, $N(z) = z\overline{z}$, which is a factorisation of the norm into irreducibles.
$N(z)$ a non-unit integer so let p be a prime in $\mathbb{Z}$ dividing $N(z)$.
If $p \equiv 3 \mod 4$, p is prime in $\mathbb{Z}[i]$. As $p \mid N(z) = z\overline{z}$, $p \mid z$ or $p \mid \overline{z}$ so p is associate to z or $\overline{z}$[a]. If p associate to $\overline{z}$ it is also associate to z by taking conjugates.
Otherwise, $p = 2$ or $p \equiv 1 \mod 4$ and $p = a^2 + b^2 = (a + bi)(a - bi)$ where $a \pm bi$ are irreducible in $\mathbb{Z}[i]$ as they have norm p. So we have $p = (a + bi)(a - bi) \mid z\overline{z}$, so z is an associate of $a + bi$ or $a - bi$ by uniqueness of factorisation. □

[a] If two primes divide each other they must be associates.

Remark 31. In the above theorem, if $p = a^2 + b^2$, $a + bi$ and $a - bi$ are not associate unless $p = 2$.

Corollary 12.1

An integer $n \geq 1$ is the sum of two squares if and only if every prime factor p of n with $p \equiv 3 \mod 4$ divides n to an even power.

Proof. Suppose $n = a^2 + b^2$. So $n = N(a + bi)$. Hence n is a product of norms of primes in the Gaussian integers. By the classification above, those norms are

1. the primes $p \in \mathbb{Z}$ with $p \not\equiv 3 \mod 4$; and
2. squares of primes $p \in \mathbb{Z}$ with $p \equiv 3 \mod 4$.

The result follows. □

Example 12.2

We can write $65 = 5 \cdot 13$ as the sum of two primes since $5, 13 \equiv 1 \mod 4$. We first factorise 5 and 13 into primes in the Gaussian integers.

$$5 = (2+i)(2-i); \quad 13 = (2+3i)(2-3i)$$

Thus, the factorisation of 65 into irreducibles in $\mathbb{Z}[i]$ is

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

This was dependent on the choice of grouping of terms. Alternatively,

$$65 = N((2+i)(2-3i)) = N(7+4i) = 7^2 + 4^2$$

§12.2 Algebraic integers

Definition 12.1

A number $\alpha \in \mathbb{C}$ is *algebraic* if α is a root of some nonzero polynomial $f \in \mathbb{Q}[X]$. α is an *algebraic integer* if it is a root of some monic polynomial $f \in \mathbb{Z}[X]$.

Let $R \leq S$, and $\alpha \in S$. We write $R[\alpha]$ to denote the smallest subring of S containing R and α. Alternatively, $R[\alpha]$ is the intersection of all subrings of S containing R and α. Further, $R[\alpha] = \operatorname{Im} \varphi$ where $\varphi \colon R[X] \to S$ is the homomorphism $g(X) \mapsto g(\alpha)$.

Definition 12.2

Let α be an algebraic number. Consider the homomorphism $\varphi \colon \mathbb{Q}[X] \to \mathbb{C}$ where $g(X) \mapsto g(\alpha)$. Since $\mathbb{Q}[X]$ is a a principal ideal domain, $\ker \varphi = (f)$ for some $f \in \mathbb{Q}[X]$. This ideal contains a nonzero element since α is an algebraic number, hence f is nonzero. Multiplying f by a unit, we may assume f is monic without loss of generality. This unique f is known as the *minimal polynomial* of α.

Corollary 12.2

All minimal polynomials are irreducible. By the isomorphism theorem, $\mathbb{Q}[X]/(f) \cong \mathbb{Q}[\alpha] \leq \mathbb{C}$. Any subring of a field is an integral domain. Hence (f) is a prime ideal in $\mathbb{Q}[X]$, and hence f is irreducible. In particular, this implies that $\mathbb{Q}[\alpha]$ is a field.

Proposition 12.2

Let α be an algebraic integer, and $f \in \mathbb{Q}[X]$ be its minimal polynomial. Then $f \in \mathbb{Z}[X]$, and $(f) = \ker\theta \triangleleft \mathbb{Z}[X]$ where $\theta\colon \mathbb{Z}[X] \to \mathbb{C}$ is given by $g(X) \mapsto g(\alpha)$.

Remark 32. If α is an algebraic integer, then the polynomial in the definition can be taken to be minimal without loss of generality. $\mathbb{Z}[X]$ is not a principal ideal domain, so the above argument cannot work verbatim.

Proof. Let f be the minimal polynomial of α. Let $\lambda \in \mathbb{Q}^\times$ such that λf has coefficients in $\mathbb{Z}$ and is primitive. Then $\lambda f(\alpha) = 0$, so $\lambda f \in \ker\theta$.

Let $g \in \ker\theta$, so in particular $g \in \mathbb{Z}[X]$. Then $g \in \ker\varphi$, and hence $\lambda f \mid g$ in $\mathbb{Q}[X]$. By a previous lemma, $\lambda f \mid g$ in $\mathbb{Z}[X]$. Thus, $\ker\theta = (\lambda f)$.

Now, since α is an algebraic integer, we know that there exists a monic polynomial $g \in \ker\theta$ such that $g(\alpha) = 0$. Then $\lambda f \mid g$ in $\mathbb{Z}[X]$, so $\lambda = \pm 1$ as both f, g are monic. Hence, $f \in \mathbb{Z}[X]$, and $(\lambda f) = (f) = \ker\theta$. □

Let $\alpha \in \mathbb{C}$ be an algebraic integer. Then, applying the isomorphism theorem to θ, $\mathbb{Z}[X]/(f) \cong \mathbb{Z}[\alpha]$. For example:

$$\begin{aligned}
\mathbb{Z}[X]/(X^2+1) &\cong \mathbb{Z}[i] \\
\mathbb{Z}[X]/(X^2-2) &\cong \mathbb{Z}\left[\sqrt{2}\right] \\
\mathbb{Z}[X]/(X^2+X+1) &\cong \mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right] \\
\mathbb{Z}[X]/(X^n-p) &\cong \mathbb{Z}[\sqrt[n]{p}]
\end{aligned}$$

Corollary 12.3

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

Proof. Let $\alpha \neq 0$, since the case where $\alpha = 0$ is trivial. Then the minimal polynomial of α has coefficients in $\mathbb{Z}$. Since α is rational, the minimal polynomial is $X - \alpha$. Hence

$\alpha \in \mathbb{Z}$ as it is a coefficient of the minimal polynomial. $\square$