Groups, Rings and Modules *

Zhiyuan Bai

Compiled on June 14, 2021

This document serves as a set of revision materials for the Cambridge Mathematical Tripos Part IB course *Groups, Rings and Modules* in Lent 2020. However, despite its primary focus, readers should note that it is NOT a verbatim recall of the lectures, since the author might have made further amendments in the content. Therefore, there should always be provisions for errors and typos while this material is being used.

Contents

*Based on the lectures under the same name taught by Dr. T. A. Fisher in Lent 2020.

0 Introduction

In this course, we will continue the analysis of groups from last year, to topics like simple groups, p-(sub)groups. The main highlight in this part will be the Sylow's Theorems.
Second, we will look into another algebraic structure, rings, where you have two operations linked together by certain axioms (like you can add, substract and multiply). Examples include $\mathbb{Z}$, $\mathbb{C}[x]$ and so on. More important examples are "rings of integers" (rings that behave like integers), like $\mathbb{Z}[i]$ or $\mathbb{Z}[\sqrt{2}]$. The unique (or not unique) factorizations in these rings give rise to methods in number theories. Another important thing is the ring of polynomials, which is the core object studies in Algebraic Geometry.
Fields, where divisions are possible for nonzero elements and multiplications commute, are also studied. Examples are $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$.
Lastly, we study modules, which are like vector spaces where one replace the underlying field by a ring. In particular, every vector space is a module. We will classify finitely generated modules over certain rings, which allows us to prove Jordan Normal Form for modules and to classify finite abelian groups.

1 Groups

1.1 Basics

Definition 1.1. A group is a pair $(G, \cdot)$ consisting of a set G and a function $\cdot : G \times G \to G$ such that
1. $\forall a, b, c \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
2. $\exists e \in G, \forall g \in G, e \cdot g = g \cdot e = e$.
3. $\forall g \in G, \exists g^{-1} \in G, g \cdot g^{-1} = g^{-1} \cdot g = e$.

Remark. 1. To check something is a group, we need also to check that $\cdot$ is well-defined. This is sometimes called the closure axiom, i.e. $\forall a, b \in G, a \cdot b \in G$.
2. If using additive notation, we write 0 for e and if we are using mutiplicative notation we write 1 for e.

Definition 1.2. For a group $(G, \cdot)$, a subset $H \subset G$ is a subgroup if $(H, \cdot|_{H\times H})$ is a well-defined group. In this case, we write $H \leq G$.

Remark. A nonempty subset $H \subset G$ is a subgroup iff $\forall a, b \in H, ab^{-1} \in H$.

Example 1.1. 1. $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq \cdots$.
2. The cyclic group C_n of order n and the dihedral group D_{2n} of isometries preserving a regular n-gon.
3. Symmetric groups S_n of the permutations of n letters and alternatig groups A_n containing all even permutations of those n letters.
4. The quarterion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.
5. The group $\mathrm{GL}_n(\mathbb{F})$ of all invertible matrices over a field $\mathbb{F}$ is a group. We can also get $\mathrm{SL}_n(\mathbb{F})$ consisting of those with determinant 1.

Definition 1.3. The direct product of groups G, H is a group $G \times H$ under the operation

$$\forall g, g' \in G, h, h' \in H, (g, h)(g', h') = (gg', hh')$$

For a subgroup H of G, the left cosets of H are the sets of the form $gH, g \in G$. It is obvious that cosets partition G and all of them have the same cardinality. So immediately,

Theorem 1.1 (Lagrange's Theorem)**.** *If G is finite and $H \leq G$, then $|H|$ divides $|G|$.*

Definition 1.4. The value $|G|/|H|$ is called the index $|G : H|$ of H in G.

There is a partial converse to this theorem which we shall introduce soon.

Theorem 1.2 (First Sylow's Theorem)**.** *If $|G| = p^n m$ where p is a prime and $p \nmid m$, there is a subgroup $H \leq G$ such that $|H| = p^n$*

From which Cauchy's Theorem is immediate.

Definition 1.5. For $g \in G$, the least n such that $g^n = 1$ is called the order of g. If there is no such integer, we say g has infinite order.

Remark. 1. If g has order d, then $g^n = 1 \iff d|n$.
2. $n||G|$ by considering the subgroup $\langle g \rangle$ generated by g.

Definition 1.6. A subgroup $H \leq G$ is called a normal subgroup of G, written as $H \trianglelefteq G$, if $\forall g \in G, gHg^{-1} = H$.

Proposition 1.3. *If $H \trianglelefteq G$, then the set of left cosets gH is a group, called the quotient group G/H, under the operation $(aH)(bH) = abH$.*

Proof. Trivial to check that the operation is well-defined. The rest is obvious. □

1.2 The Isomorphism Theorems

Definition 1.7. Let G, H be groups, a map $\phi : G \to H$ is called a group homomorphism if $\forall g, g' \in G, \phi(gg') = \phi(g)\phi(g')$. The kernel of ϕ is defined as $\ker\phi = \{g \in G : \phi(g) = 1\} \leq G$. The image of ϕ is defined as $\operatorname{Im}\phi = \{h \in H : \exists g \in G, \phi(g) = h\} \leq H$

Obviously $\ker\phi \trianglelefteq G$. The concerse is also true: any normal subgroup of G is the kernel of the canonical projection of G to the quotient.

Definition 1.8. An isomorphism is a bijective homomorphism. We say G, H are isomorphic, or $G \cong H$, if there is an isomorphism between them.

Proposition 1.4. *If ϕ is an isomorphism, so is ϕ^{-1}.*

Proof. Trivial. □

Theorem 1.5 (Isomorphism Theorem)**.** *Let $\phi : G \to H$ be a group homomorphism, then $G/\ker\phi \cong \operatorname{Im}\phi$.*

Proof. The map $\tilde{\phi} : G/\ker\phi \to \operatorname{Im}\phi$ by $g\ker\phi \mapsto \phi(g)$ is a well-defined isomorphism. □

Example 1.2. The function $\exp : \mathbb{C} \to \mathbb{C}^\star$ is a homomorphism with kernel

$$\ker\exp = \{z \in C : \exp(z) = 1\} = 2\pi\mathbb{Z}, \operatorname{Im}\exp = \mathbb{C}^\star$$

Hence $\mathbb{C}/2\pi\mathbb{Z} = \mathbb{C}^\star$.

The Isomorphism Theorem is sometimes called the *First* Isomorphism Theorem. There are other isomorphism theorems, but they are all corollaries of the first one.

Corollary 1.6 (Second Isomorphism Theorem)**.** *Consider a group G and subgroups $H \leq G, K \trianglelefteq G$, then the set $HK = \{hk : h \in H, k \in K\}$ is a subgroup of G. Also $H \cap K \trianglelefteq H$. Then we have $HK/K \cong H/H \cap K$.*

Proof. The (normal) subgroup conditions in $HK, H\cap K$ are trivial. The function $\phi : H \to G/K$ by $h \mapsto hK$ is a homomorphism because it is the composition of the inclusion $H \to G$ and the projection $G \to G/K$. So immediately $\ker\phi = H \cap K$ and $\operatorname{Im}\phi = HK/K$, and the result follows. □

Remark. There is a natural bijection from the subgroups of G/K and the subgroups of G containing K by $X \mapsto \{g \in G : gK \in X\}$. How about normal subgroups? Turns out we have the Third Isomorphism Theorem to describe this.

Corollary 1.7 (Third Isomorphism Theorem)**.** *Suppose H, K are normal subgroups of G and $K \subset H$. SO $K \trianglelefteq H$ and $H/K \trianglelefteq G/K$ with*

$$G/H \cong (G/K)/(H/K)$$

Proof. Let $\phi : G/K \to G/H$ by $gK \mapsto gH$ which is clearly a well-defined surjective homomorphism, then $\ker\phi = H/K$. The result then follows from the First Isomorphism Theorem. □

1.3 Simple Groups

If $K \trianglelefteq G$, then the study of the groups K and G/K gives some information about G (but not all). But sometimes this approach fails due to the lack of normal proper subgroups.

Definition 1.9. A group is called simple if it has no normal proper subgroups.

Lemma 1.8. *An abelian group G is simple if and only if it is isomorphic to the cyclic group of order p for some prime p.*

Proof. An abelian group is simple if and only if it has no proper subgroup. It is obvious that for any prime p, C_p has no proper subgroup due to Lagrange's Theorem, so we proceed to the converse. Note that any nonidentity element $x \in G$ must generate G, otherwise the subgroup generated by it will be a proper subgroup of G. However this means that G is cyclic, so immediately to make it simple G must be isomorphic to C_p for some prime p. □

Lemma 1.9. *If G is a finite group, then it has a composition series*

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_m = G$$

with G_i/G_{i-1} is simple for each i.

Proof. Induction on $|G|$. By the Third Isomorphism Theorem a normal proper subgroup $H \lhd G$ with maximal order must have G/H simple, so the result follows. □

2 Group Actions

Definition 2.1. Let X be a set and let $\operatorname{Sym} X$ be the group of all bijections $X \to X$ under composition.

Definition 2.2. A group G is a permutation group if it is a subgroup of $\operatorname{Sym} X$ for some set X. We say it is a permutation group of degree n if X is finite and $|X| = n$.

Example 2.1. 1. $S_n = \operatorname{Sym}\{1, 2, \ldots, n\}$ is a permutation group of degree n. So is A_n.
2. The group D_{2n} is a permutation group of degree n by thinking about the way it transforms the vertices of a regular n-gon.

Definition 2.3. Let G be a group and X be a set. An action of G on X is a function $\star : G \times X \to X$ satisfying:
1. $\forall x \in X, 1 \star x = x$.
2, $\forall g, h \in G, x \in X, (gh) \star x = g \star (h \star x)$.

Proposition 2.1. *An action $\star : G \times X \to X$ is equivalent to a homomorphism $\phi : G \to \operatorname{Sym} X$.*

Proof. Take $\phi(g)(x) = g \star x$. □

Definition 2.4. We say such a homomorphism ϕ a permutation representation of G.

In particular, if ϕ is injective, then G is isomorphic to a subgroup of $\operatorname{Sym} X$.

Definition 2.5. Let $\star : G \times X \to X$ be a group action, then the orbit of an element $x \in X$ is defined by

$$\operatorname{Orb}_G(x) = \{g \star x : g \in G\}$$

The stabiliser of it is defined by

$$G_x = \{g \in G : g \star x = x\}$$

Theorem 2.2. *Let $\star : G \times X \to X$ be a group action, then for any $x \in X$ there is a bijection $\operatorname{Orb}_G(x) \to G/G_x$.*

Proof. Take $g \star x \mapsto gG_x$. □

Corollary 2.3. *If G is finite, then $|\operatorname{Orb}_G(x)||G_x| = |G|$.*

Proof. Follows directly. □

Remark. 1. $\ker \phi = \bigcap_{x \in X} G_x$ is called the kernel of the action.
2. The orbits partition X. If there is only one orbit, then we say the action is transitive.
3. The stabilisers of x, y in the same orbit are conjugate subgroups of each other. That is, $G_{g \star x} = gG_x g^{-1}$.

Example 2.2. 1. Given a group G, it can act on itself by left multiplication. This is called the left regular action. The kernel of the action is obviously just the identity. So the induced permutation representation makes G isomorphic to a subgroup of $\operatorname{Sym} G$. In particular, if $|G| = n$, then G is isomorphic to a subgroup of the symmetric group S_n. This is known as Cayley's Theorem.
2. Consider a group G and a subgroup $H \leq G$, then G can act on G/H by left multiplication. This action is transitive. Also the stabiliser of xH is xHx^{-1}, so the kernel of the action becomes $\bigcap_{x \in X} xHx^{-1}$, the largest normal subgroup of G contained in H.
3. Let G acts on itself by conjugation, so $g \star x = gxg^{-1}$. In this case, the orbit containing x is called the conjugacy class containing x, $\operatorname{ccl}_G(x)$, and the stabiliser of x is called the centraliser $C_G(x)$ of x. The kernel $Z(G)$ of the action is called the centre of G. Note that G can also act by conjugation on any of its normal subgroup.
4. Let X be the set of subgroups of the group G, then G acts on X by conjugation: $g \star H = gHg^{-1}$. So the stabiliser of H is called the normalizer $N_G(H)$ of H. It is the largest subgroup of G to contain H as a normal subgroup.

Theorem 2.4. *Let G be a nonabelian simple group, and $H < G$ has index $n > 1$, then $n \geq 5$ and G is isomorphic to a subgroup of A_n.*

Proof. Consider the action of G acting on the set of left cosets of H by left multiplication. This gives a homomorphism $\phi : G \to S_n$. But $\ker \phi$ is normal in G. It is obviously not the entire group, so ϕ has to be injective, so G is isomorphic to a subgroup of S_n. We know that $A_n \lhd S_n$, so $A_n \cap G \lhd G$, so either $G \subset A_n$ or $G \cap A_n = 1$ since G is simple. If $G \cap A_n = 1$, we have $G \cong G/(G \cap A_n) \cong GA_n/A_n \leq S_n/A_n \cong C_2$ by Second Isomorphism Theorem, contradiction.
Therefore $G \leq A_n$. Finally if $n \leq 4$, A_n does not have a nonabelian simple subgroup by simple exhaustion. So $n \geq 5$. □

Example 2.3. Consider the group of rotational symmetries of the icosahedron with 20 faces, 12 vertices and 30 edges with each face an equilateral triangle. We have the following table

Order	Number
1	1
2	15
3	20
5	24
Total	60

Note that G acts on the set of vertices transitively, so $|G| = 12 \times 5 = 60$, hence these are all.
The elements of order 2 are all conjugates, same for elements of order 3. The elements of order 5 splits into two conjugacy classes, each of size 12.
If $H \lhd G$, then it must be a union of conjugacy classes including the identity one, but they must have a sum that divides 60. One can check that it can happen iff H is trivial. Thus G is simple.
We want to show that G is isomorphic to A_5. We claim that the set of subgroups H of order 4 removing the identity partitions the 16 elements of order at most 2. Note that we must have $H \cong C_2 \times C_2$ since G does not have element of order 4, so each such subgroups contains 3 involutions. If $g \in G$ has order 2, then $g \in C_G(g)$, so $|C_G(g)| = |G|/|\operatorname{ccl}_G(g)| = 4$, so every involution is contained in a subgroup of order 4.
Suppose $1 \neq g \in H \cap K$ where H, K are subgroups of order 4. But the centralizer of g has order 4 and contains both H and K since H, K are abelian, but they all have size 4, hence $H = K$.
Let G act on the 5 subgroups of order 4 by conjugation. This gives a homomorphism $\phi : G \to \operatorname{Sym}(X) \cong S_5$, but since G is simple, ϕ is injective. So $G \leq S_5$. But again $G \cap A_5$ can only be A_5 by exactly the same trick as the proof of the preceding theorem. Since $|G| = |A_5| = 60$, we have $G = A_5$.

3 Alternating Groups

Conjugation in S_n is relatively easy: They preserve the cycle type and act transitively on the same cycle types.

Example 3.1. In S_5, we have

Cycle Type	Number of Elements
1	1
2^1	10
2^2	15
3^1	20
$2^1 3^1$	20
4^1	30
5^1	24
Total	120

Let $g \in A_n$, then $C_{A_n}(g) = C_{S_n}(g) \cap A_n$. So if there is an odd permutation

that commutes with g, then

$$|C_{A_n}(g)| = \frac{1}{2}|C_{S_n}(g)|, |\operatorname{ccl}_{A_n}(g)| = |\operatorname{ccl}_{S_n}(g)|$$

Otherwise,

$$|C_{A_n}(g)| = |C_{S_n}(g)|, |\operatorname{ccl}_{A_n}(g)| = \frac{1}{2}|\operatorname{ccl}_{S_n}(g)|$$

Example 3.2. Consider $(12)(34) \in A_5$. It commutes with (12), so the conjugacy class stays the same.
Similar for (123) which commutes with (45).
But if we consider (12345), things go different. Note that if h is in its centralizer, then $h(12345)h^{-1} = (h(1)h(2)h(3)h(4)h(5))$, so h has to be some power of (12345), in particular h is even. Therefore in this case the conjugacy class splits into two.
So the conjugacy classes of A_5 have sizes $1, 15, 20, 12, 12$, so by the same trick we used, A_5 is simple.

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. So it suffices to prove that the product of any two transpositions is a product of 3-cycles.
For a, b, c, d different, we have

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

As desired. □

Lemma 3.2. *If $n \geq 5$, then all 3-cycles in A_n are conjugate to each other.*

Proof. We claim that any 3-cycle is conjugate to (123). Note that for a, b, c different, $(abc) = \sigma(123)\sigma^{-1}$. If σ is odd, then we still have $(abc) = \pi(123)\pi^{-1}$ where $\pi = \sigma(45)$ and π is even. □

Theorem 3.3. *A_n is simple for $n \geq 5$.*

Proof. Let $1 \neq N \trianglelefteq A_n$. It suffices to show that N contains a 3-cycle. We start by choosing a non-trivial element $1 \neq \sigma \in N$ and write it as a product of disjoint cycles.
Case 1: σ contains an r-cycle where $r \geq 4$. WLOG $\sigma = (12 \dots r)\tau$ where τ fixes $1, 2, \dots, r$. And let $\delta = (123)$, we compute

$$N \ni \sigma^{-1}\delta^{-1}\sigma\delta = (r \dots 21)(132)(12 \dots r)(123) = (23r)$$

So $N = A_n$.
Case 2: σ contains two 3-cycles. WLOG $\sigma = (123)(456)\tau$ where τ fixes $1, 2, \dots, 6$. We let $\delta = (124)$, then $N \ni \sigma^{-1}\delta^{-1}\sigma\delta = (12436)$ which is a 5-cycle. By Case 1, N also contains a 3-cycle.
Case 3: σ contains two 2-cycles, where we set WLOG $\sigma = (12)(34)\tau$ where τ fixes $1, 2, 3, 4$. We let $\delta = (123)$, so $N \ni \sigma^{-1}\delta^{-1}\sigma\delta = (14)(23) = \pi$. Then let $\epsilon = (235)$ (note that we used $n \geq 5$ here), then $N \ni \pi^{-1}\epsilon^{-1}\pi\epsilon = (253)$, which is a 3-cycle.
It remains to consider cycle types $2^1, 3^1, 2^1 3^1$. But $2^1, 2^1 3^1$ are not in A_n since they are not even, and for 3^1 it follows immediately. □

4 (Sub-)Groups with prime power order

4.1 Elementary Properties

Definition 4.1. Let G be a group. We say G is a p-group for a prime p if $|G| = p^n$ for some $n \in \mathbb{N}$.

Theorem 4.1. *Let G be a p-group, then $Z(G) \neq 1$.*

Proof. Consider the partition of G by conjugacy classes, which are either 1 or divisible by p. Note that $Z(G)$ is the union of all 1-classes. But if $|Z(G)| = 1$, then

$$0 \equiv p^n = |G| = 1 + \sum_{\exists g \notin Z(G), C = \mathrm{ccl}_G(g)} |C| \equiv 1 \pmod{p}$$

which is a contradiction. □

In particular $|Z(G)| \equiv 0 \pmod{p}$.

Corollary 4.2 (Classification of Simple p-groups)**.** *If G is a simple p-group, then $G \cong C_p$.*

Proof. $1 \neq Z(G) \trianglelefteq G$. Since G is simple we must have $Z(G) = G$, hence G is abelian, but then necessarily $G \cong C_p$ since G cannot have any proper subgroup to be simple. □

Corollary 4.3. *Let G be a p-group of order p^n, then G contains a subgroup of order p^r for any $0 \leq r \leq n$.*

Proof. Consider the composition series of G

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_m = G$$

where each G_{i+1}/G_i is necessarily a simple p-group, so we must have $G_{i+1}/G_i \cong C_p$ for any i. The claim follows. □

Lemma 4.4. *For any group G, if $G/Z(G)$ is cyclic, then G is abelian.*

Proof. Let $gZ(G)$ be a generator of $G/Z(G)$. Then every element of G is of the form $p^i z$ where $z \in Z$. But for $z, z' \in Z(G)$, $g^i z g^j z' = g^{i+j} z z' = g^j z' g^i z$, so G is abelian. □

Corollary 4.5. *Any group G with order p^2 for a prime p is abelian.*

Proof. We already know that $Z(G) \neq 1$. For $|Z(G)| = p$ then we have $G/Z(G) \cong C_p$, so G is abelian by the preceding lemma, contradiction. For $|Z(G)| = p^2$ we have $Z(G) = G$, which means that G is abelian. There are no other possibilities, so the proof is done. □

Sadly (or not) there are nonabelian groups of order p^3, e.g. D_8 (for $p = 2$) and the Heisenberg group over $\mathbb{Z}/3\mathbb{Z}$ (for $p = 3$).

4.2 Sylow's Theorems

Theorem 4.6 (Sylow's Theorems)**.** *Let G be a finite group with order $p^a m$ where p is a prime and $p \nmid m$. Then*
1. The set $\mathrm{Syl}_p(G) = \{P \leq G : |P| = p^a\}$ is nonempty.
2. All elements of $\mathrm{Syl}_p(G)$ are conjugate.
3. The number $n_p = |\mathrm{Syl}_p(G)|$ satisfies $n_p \equiv 1 \pmod p$ and $n_p | m$.

Corollary 4.7. *If $n_p = 1$, then there is a normal Sylow p-subgroup.*

Proof. Let $g \in G$ and P be a Sylow p-subgroup of G. But then $gPg^{-1} \in \mathrm{Syl}_p(G) = \{P\}$, hence $gPg^{-1} = P \implies P \trianglelefteq G$. □

Example 4.1. There is no simple group of order 1000. Suppose G is a group of order $1000 = 2^3 5^3$, then $n_5 \equiv 1 \pmod 5$ and $n_5 | 8$, but then we must have $n_5 = 1$. So there is a normal Sylow 5-subgroup of G which is obviously not the identity or G, hence G is not normal.

Proof. 1. Consider the action of the group G on the set Ω of all subsets of G of size p^a by $g \star X = \{gx : x \in X\}$. We have

$$|\Omega| = \binom{p^a m}{p^a} \not\equiv 0 \pmod p$$

Hence this action has an orbit, say the orbit of $X \in \Omega$, whose order is not a multiple of p. Then $|G_X| |\operatorname{orb}_G(X)| = |G| = p^a m$ gives $p^a | |G_X|$. On the other hand, $\bigcup_{g \in G} g \star X = G$, so $|G| \leq |\operatorname{orb}_G(X)||X|$, so $|G_X| = |G|/|\operatorname{orb}_G(X)| \leq |X| = p^a$, but $|G_X| \geq p^a$, therefore $|G_X| = p^a$.
2. We shall prove a stronger statement: suppose $P \in \mathrm{Syl}_p(G)$ and $Q \leq G$ is a p-subgroup, then $Q \leq gPg^{-1}$ for some $g \in G$. Consider the action of Q on the set of left cosets G/P by left multiplication. By orbit-stabiliser, the size of any orbit divides $|Q|$, i.e. it is either 1 or a multiple of p. But $|G/P| = m$ which is coprime to p, hence there is at least one orbit $\operatorname{orb}_Q(gP)$ of size 1. This means that for any $q \in Q$, $g^{-1}qg \in P \implies Q \leq gPg^{-1}$.
3. By part 2 of the theorem, G acts transitively on $\mathrm{Syl}_p(G)$ by conjugation, so $n_p | |G|$ by orbit-stabiliser. Hence it suffices to show that $n_p \equiv 1 \pmod p$. Choose any $P \in \mathrm{Syl}_p(G)$ and consider its action on $\mathrm{Syl}_p(G)$ by conjugation. Any orbit of this action would divide $|P| = p^a$, so is either 1 or divisible by p. We shall show that there is exactly one orbit of size 1, which will establish the theorem.
There is at least one such orbit, namely $\operatorname{orb}_P(P)$. If $\operatorname{orb}_P(Q)$ is also an orbit of size 1, then $P \leq N_G(Q)$. P, Q are Sylow p-subgroups of $N_G(Q)$, so they are conjugate in it, therefore there is some $g \in N_G(Q)$ with $Q = gQg^{-1} = P$. □

Example 4.2. Suppose G is a simple group, then $|G| \neq 132$. Assume there is a simple group of order $132 = 2^2 \cdot 3 \cdot 11$, then by Sylow's Third Theorem, $n_3 = 1, 4, 22$ and $n_{11} = 1, 12$, but by simplicity neither of them is 1, so $n_{11} = 12$ If $n_3 = 4$, then letting G act on $\mathrm{Syl}_3(G)$ by conjugation gives a group homomorphism $G \to S_4$, but its kernel is not all G, so G is isomorphic to a subgroup of S_4, but $|S_4| = 24 < 132$, contradiction.
So $n_3 = 22$. Now the Sylow 3-subgroups are all of order 3, this means that there are $22 \times (3 - 1) = 44$ elements of order 3. Similarly $n_{11} = 12$ gives $(11-1) \times 12 = 120$ elements of order 11, but then $132 = |G| \geq 120+44+1 = 165$, contradiction.

For the sake of example sheets, we mention the following definition.

Definition 4.2. The automorphism group $\mathrm{Aut}(G) \leq \mathrm{Sym}\, G$ of a group G is the group of all isomorphisms from G to itself.

5 Some Matrix Groups

Definition 5.1. Let $\mathbb{F}$ be a field (e.g. $\mathbb{C}, \mathbb{Z}/p\mathbb{Z}$). We define

$$\mathrm{GL}_n(\mathbb{F}) = \{M \in \mathcal{M}_{n\times n}(\mathbb{F}) : \det M \neq 0\}$$

$$\mathrm{SL}_n(\mathbb{F}) = \{M \in \mathcal{M}_{n\times n}(\mathbb{F}) : \det M = 1\} = \ker \det|_{\mathrm{GL}_n(\mathbb{F})} \trianglelefteq \mathrm{GL}_n(\mathbb{F})$$

Note that $Z = Z(\mathrm{GL}_n(\mathbb{F}))$ is the set of scalar matrices.

Definition 5.2.

$$\mathrm{PGL}_n(\mathbb{F}) = \mathrm{GL}_n(\mathbb{F})/Z$$

$$\mathrm{PSL}_n(\mathbb{F}) = \mathrm{SL}_n(\mathbb{F})/(Z \cap \mathrm{SL}_n(\mathbb{F})) \cong Z\,\mathrm{SL}_n(\mathbb{F})/Z \leq \mathrm{PGL}_n(\mathbb{F})$$

Example 5.1. Let $G = \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. A list of n vectors in $(\mathbb{Z}/p\mathbb{Z})^n$ are the columns of some $A \in G$ iff they are linearly independent. Hence

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

So the Sylow p-subgroups have order $p^{n(n-1)/2}$. Indeed, the subgroup of upper-triangular matrices with 1's on the diagonal gives one (hence all by conjugation) of such subgroups.

Just like $\mathrm{PSL}_2(\mathbb{C})$ act on $\mathbb{C} \cup \{\infty\}$ by Mobius transformations, the group $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ can act on $\mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$ in this way as well:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \mapsto \frac{az+b}{cz+d}$$

where the infinity cases are dealt with in the same way.

Lemma 5.1. *The permutation representation* $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z}) \to S_{p+1}$ *by Mobius transformation is injective.*

And indeed this is an isomorphism for $p = 2, 3$ by considering the size.

Proof. Suppose there is some a, b, c, d such that $\forall z \in \mathbb{C}, z = (az+b)/(cz+d)$, then putting $z = 0$ gives $b = 0$, and $z = \infty$ gives $c = 0$, and $z = 1$ gives $a = d$, but these only gives one element that is the identity of $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$. Done. □

Lemma 5.2. *If p is an odd prime, then* $|\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})| = p(p-1)(p+1)/2$.

Proof. We already know that

$$|\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})| = p(p-1)(p^2-1)$$

Then by Isomorphism Theorem

$$|\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})| = |\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})|/|(\mathbb{Z}/p\mathbb{Z})^\star| = p(p-1)(p+1)$$

And

$$|\operatorname{PSL}_2(\mathbb{Z}/p\mathbb{Z})| = |\operatorname{SL}_2(\mathbb{Z}/p\mathbb{Z})|/|\{\pm I\}| = \frac{p(p-1)(p+1)}{2}$$

Here $Z \cap \operatorname{SL}_2(\mathbb{Z}/p\mathbb{Z}) = \{\pm I\}$ because $a^2 \equiv 1 \pmod{p}$ only has two solutions, namely ± 1, as p is prime. □

Note that for $p = 2$, things go wrong on the fact that in this case $I = -I$.

Example 5.2. Consider the group $G = \operatorname{PSL}_2(\mathbb{Z}/5\mathbb{Z})$, then $|G| = 60 = 2^2 \cdot 3 \cdot 5$. We shall show that G is simple, and in fact, it is isomorphic to A_5.
Let G act on $\mathbb{Z}/5\mathbb{Z} \cup \{\infty\}$ by Mobius transformation. By Lemma 5.1, we have an injective group homomorphism $\phi : G \to S_6$.
Our first claim that, if we embed G into S_6, then $G \leq A_6$. Equivalently the map $\psi : G \to S_6 \to \{\pm 1\}$ is trivial, where the first arrow is ϕ and the second is the signature.
Note that for odd m, we have $\psi(g) = 1 \iff \psi(g^m) = 1$, so it suffices to study the elements of order being a power of 2, but this means to study the elements contained in every Sylow 2-subgroup of G, but all of them are conjugate, it is enough to check one of them (since $\{\pm 1\}$ is abelian). We spot the following one

$$H = \left\{ \pm \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ 4 & 0 \end{pmatrix} \right\}$$

By simple computation, ψ does vanish on H, so indeed we have $G \leq A_6$. By a result in Example Sheet 1, if $G \leq A_6$ and $|G| = 60$, then $G \cong A_5$, which completes the proof.

The following facts will not be proved in the course, but are very important:

Proposition 5.3. $\operatorname{PSL}_n(\mathbb{Z}/p\mathbb{Z})$ *is simple for* $n \geq 2$ *and* p *prime except if* $(n, p) = (2, 2)$ *or* $(n, p) = (2, 3)$. *Also, the two smallest nonabelian simple groups are* $A_5 \cong \operatorname{PSL}_2(\mathbb{Z}/5\mathbb{Z})$ *with order* 60 *and* $\operatorname{PSL}_2(\mathbb{Z}/7\mathbb{Z}) \cong \operatorname{GL}_3(\mathbb{Z}/2\mathbb{Z})$ *with order* 168.

6 The Classification of Finite Abelian Groups

We will prove (the generalization of) the following theorem later when we look at modules:

Theorem 6.1. *Every finite abelian group is isomorphic to a product of cyclic groups.*

In this section, we shall look at the uniqueness criterion of this statement. In fact, this representation is not unique in general, but we can get some sort of a uniqueness statement.

Lemma 6.2. *If* m, n *are coprime, then* $C_m \times C_n \cong C_{mn}$.

Proof. Let g_m be the generator of C_m and g_n be that of C_n, then $(g_m, g_n) \in C_m \times C_n$ has order $\gcd(m, n) = mn$. □

Corollary 6.3. *Let* G *be a finite abelian group, then* $G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_k}$ *such that any* n_i *is a prime power*

Proof. Let n be a positive integer, then $n = p_1^{e_1} \cdots p_r^{e_r}$ where p_i are distinct primes, then

$$C_n \cong C_{p_1^{e_1}} \times \cdots \times C_{p_r^{e_r}}$$

by the preceding lemma. Combining this with the theorem gives the result. □

In fact, what we will prove is the following refinement of Theorem 6.1.

Theorem 6.4. *Let G be a finite abelian group, then $G \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_t}$ such that $1 < d_1 | d_2 | d_3 | \cdots | d_{t-1} | d_t$.*

Remark. The integers $n_1, n_2, \ldots$ are up to a reordering, and $d_1, d_2, \ldots$ are uniquely determined by the group G. The proof (which we omit) works by counting the elements of G with every possible order (it is enough to consider prime powers though).

Example 6.1. 1. Abelian groups of order 8 can only be $C_8, C_2 \times C_4, C_2 \times C_2 \times C_2$.
2. Abelian groups of order 12 can only be $C_2 \times C_2 \times C_3 \cong C_2 \times C_6, C_4 \times C_3 \cong C_{12}$

7 Rings

Definition 7.1. A ring is a triple $(R, +, \cdot)$ consisting of a set R and two binary operations $+, \cdot : R \times R \to R$, called addition and multiplication, such that
1. $(R, +)$ is an abelian group. Its identity is called $0 = 0_R$.
2. $\cdot$ is associative and has an identity called $1 = 1_R$.
3. $\forall x, y, z \in R, x \cdot (y + z) = x \cdot y + x \cdot z, (x + y) \cdot z = x \cdot z + y \cdot z$.

Remark. 1. Again closure is not explicitly listed as an axiom, but it is included in the well-definedness of $+, \cdot$, so to verify something is a ring, we still have to check the closure.
2. For $x \in R$, we write $-x$ for its additive inverse and abbreviate $x + (-y) = x - y$.
3. $0 = 0 \cdot x - 0 \cdot x = (0 + 0) \cdot x - 0 \cdot x = 0 \cdot x + 0 \cdot x - 0 \cdot x = 0 \cdot x$. Similarly $x \cdot 0 = 0$.
4. $-x = 0 - x = 0 \cdot x - x = (1 + (-1)) \cdot x - x = x + (-1) \cdot x - x = (-1) \cdot x$.
5. Using 4 and other axioms, we can deduce back the property that addition is commutative.

Definition 7.2. If $\cdot$ is commutative as well, we say R is a commutative ring.

In this course, we are only interested in commutative rings. When we say "ring" afterwards, we will always imply commutativity.

Definition 7.3. Given a ring R, a subring S is a subset of R such that S is a ring under the same addition and multiplication restricted to $S \times S$ and the same identity elements.

Example 7.1. 1. $\mathbb{Z}$ is a ring under the familiar operations.
2. The Gaussian integers $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ is a ring and is a subring of $\mathbb{C}$.
3. The set $\mathbb{Q}[\sqrt{2}] = \{p + q\sqrt{2} : p, q \in \mathbb{Q}\}$.
4. $\mathbb{Z}[1/p] = \{m/p^n : m \in \mathbb{Z}, n \in \mathbb{N}\}$ where p is a prime gives a ring that is a subring of $\mathbb{Q}$.
5. $\mathbb{Z}/n\mathbb{Z}$ is a ring for any natural number n.

We can also construct new rings from old.

Definition 7.4. Given rings R, S, the product ring is the Cartesian product $R \times S$ with operations

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2), (r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$$

So $0_{R\times S} = (0_R, 0_S)$ and $1_{R\times S} = (1_R, 1_S)$.

Definition 7.5. Let R be a ring and X a set, then the set of functions $X \to R$ is a ring under pointwise operations. So $(f + g)(x) = f(x) + g(x), (f \cdot g)(x) = f(x) \cdot g(x)$.

Further interesting examples appear as subrings of it. For example, the set of all continuous functions $\mathbb{R} \to \mathbb{R}$ is a ring.

Definition 7.6. Let R be a ring and S the set of all sequences of elements $r_0, r_1, r_2, \ldots$ of R that is eventually zero. Consider the operations

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots)$$

and

$$(a_0, a_1, \ldots) \cdot (b_0, b_1, \ldots) = (c_1, c_2, \ldots), c_n = \sum_{i=0}^{n} a_i b_{n-i}$$

One can verify that this is indeed a ring. We can identify R as a subring of S by $r \mapsto (r, 0, 0, \ldots)$. Define $X = (0, 1, 0, 0, \ldots)$, so $X^n = (0, \ldots, 0, 1, 0, 0, \ldots)$ where the 1 occurs as the n^{th} entry (counting from 0). So S is generated by X and R, hence every element of S can be identifies as a sum

$$\sum_{i=0}^{n} a_i X^i, a_i \in \mathbb{R}$$

So this ring $S = R[X]$ is called the polynomial ring over R. We define the degree of a polynomial to be the largest i such that the coefficient a_i is nonzero.
We can obviously identify each polynomial $a_0 + a_1 X + \cdots + a_n X^n$ as a function $x \mapsto a_0 + a_1 x + \cdots + a_n x^n$, however

Remark. Let $R = \mathbb{Z}/p\mathbb{Z}$ where p is a prime, and $f(X) = X^p - X$, so we can identify a function $R \to R$ by $x \mapsto x^p - x = 0$.

Definition 7.7. For a ring R, we can define multivariate polynomial ring $R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$ inductively.

Definition 7.8. Given a ring, we can define the power series ring $R[[X]]$ that is all power series in X, which are formal sequence of coefficient following the same operation as polynomial rings.

Definition 7.9. The Laurent polynomials $R[X, X^{-1}]$ is defined as functions from $\mathbb{Z} \to R$ taking finitely many nonzero values following yet again the same operation. We write the elements in the form $\cdots + a_{-2}X^{-2} + a_{-1}X^{-1} + a_0 + a_1 X + a_2 X^2 + \cdots$ where only finitely many a_i is nonzero.

Definition 7.10. Given a ring R, an element $r \in R$ is called a unit if it has a multiplicative inverse. We write r^{-1} for that inverse.

A warning is that whether or not an element is a unit depends on the ring, for example 2 is a unit in $\mathbb{Q}$ but not in $\mathbb{Z}$.
The set of all inverse in a ring forms a group $R^\times$ under multiplication. So $\mathbb{Z}^\times = \{\pm 1\}$ and $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$. Sometimes we write $R^\times$ as $R^\star$.

Definition 7.11. A field is a ring with $0 \neq 1$ and that every nonzero element is a unit.

Example 7.2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ (p prime) are fields.

There is obviously a reason why we need $0 \neq 1$.

Remark. If R is a ring such that $0 = 1$, then $\forall x \in R, x = 1 \cdot x = 0 \cdot x = 0$, so every element of this ring is zero.

Lemma 7.1. *Let $f, g \in R[X]$ be polynomials, and suppose that g is nonconstant and that the leading coefficient of g is a unit, then there exists a quotient with remainder. That is, $\exists q, r \in R[X]$ such that $f = qg + r$ with $\deg r < \deg g$.*

Proof. Simple induction. □

8 Ideals, Quotients, and Isomorphism Theorems

8.1 Definitions

Definition 8.1. Let R, S be rings. A function $\phi : R \to S$ is called a ring homomorphism if it for any $r_1, r_2 \in R$
1. $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$.
2. $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$.
3. $\phi(1_R) = 1_S$.
If additionally this map is bijective, we call this an isomorphism.
The kernel of ϕ is the set $\ker \phi = \{r \in R : \phi(r) = 0_S\}$.

Lemma 8.1. *A ring homomorphism $\phi : R \to S$ is injective iff $\ker \phi = \{0_R\}$.*

Proof. ϕ is also a group homomorphism $(R, +) \to (S, +)$. □

Definition 8.2. A subset $I \subset R$ is called an ideal, written as $I \trianglelefteq R$, if $(I, +) \leq (R, +)$ and $\forall r \in R, rI \subset I$.

Remark. Note that an ideal needs not to be a subring since it might not contain 1. In fact, if $1 \in I$, then $\forall r \in R, r = r1 \in I$, so $I = R$. In general, if I contains a unit u, then $\forall r \in R, r = (ru^{-1})u \in I$, so again $I = R$.
Therefore, a field can only have two ideals, $\{0\}$ and itself.

An ideal $I \neq R, \{0\}$ is called proper.

Lemma 8.2. *Let $\phi : R \to S$ be a ring homomorphism, then $\ker \phi \trianglelefteq R$.*

Proof. $\ker \phi$ is obviously an additive subgroup of R. Also $\forall r \in R, i \in I, \phi(ri) = \phi(r)\phi(i) = \phi(r)0_S = 0_S \implies ri \in \ker \phi$. Hence $\ker \phi \trianglelefteq R$. □

Lemma 8.3. *The only ideals of $\mathbb{Z}$ are $n\mathbb{Z}, n \in \mathbb{Z}$.*

Proof. All of them are ideals and these are all possible additive subgroups. □

Definition 8.3. For $a \in R$, the ideal generated by a is the ideal $(a) = \{ra : r \in R\}$.

Note that (a) is the smallest ideal that contains a. More generally,

Definition 8.4. For $a_1, \ldots, a_n \in R$, the ideal generated by them is the ideal $(a_1, \ldots, a_n) = \{r_1 a_1 + \cdots + r_n a_n : r_i \in R\}$.

Definition 8.5. An ideal $I \trianglelefteq R$ is principle if $I = (a)$ for some $a \in R$.

So every ideal of $\mathbb{Z}$ is principle.

Theorem 8.4. *Let I be an ideal of R, then we take the quotient R/I as if they are additive groups. We can define the multiplication on R/I by defining $(a+I)(b+I) = ab+I$ which is well-defined and makes R/I a ring.*

Such R/I is called the quotient ring. Note that the canonical projection (or quotient map) $\pi : R \to R/I$ becomes a ring homomorphism with kernel I, hence every ideal is the kernel of a homomorphism.

Proof. If $a + I = a' + I, b + I = b' + I$, then $a - a', b - b' \in I$, so $ab - a'b' = a(b - b') + (a - a')b' \in I$, therefore $ab + I = a'b' + I$, hence this multiplication is well-defined. The rest follows. □

Example 8.1. 1. For $R = \mathbb{Z}$, then the quotients are $\mathbb{Z}/n\mathbb{Z}$ with modulo n addition and multiplication.
2. Consider the ideal generated by X inside the poynomial $R[X]$, then (X) consists of polynomials without a constant term. The quotient is then $R[X]/(X) \cong R$ with the isomorphism $r(X) \mapsto r$.
3. Consider the ring of real polynomials $\mathbb{R}[X]$ and the ideal $(X^2 + 1)$, then $\mathbb{R}[X]/(X^2 + 1) = \{f(X) + (X^2 + 1) : f(X) \in R[X]\}$. Now $\mathbb{R}$ is a field, so every nonzero element is a unit, hence we can always do division algorithm. So by applying this algorithm on $f(X)$, we have $\mathbb{R}[X]/(X^2+1) = \{a+bX+(X^2+1) : f(X) \in R[X]\}$. Now suppose $a + bX + (X^2 + 1) = a' + b'X + (X^2 + 1)$, then $(b - b')X + (a - a') = Q(X)(X^2 + 1)$ for some polynomial Q, but by looking at the degree, we must have $Q = 0$, therefore $a = a', b = b'$, so each cosets are uniquely represented like this. We then identify $a+bX+(X^2+1) \mapsto a+bi \in \mathbb{C}$, but this is a ring isomorphism, so $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$.

8.2 Isomorphism Theorems of Rings

Theorem 8.5 ((First) Isomorphism Theorem)**.** *Let $\phi : R \to S$ be a ring homomorphism, then $\ker \phi$ is an ideal of R and the quotient ring $R/\ker \phi$ is isomorphic to $\operatorname{Im} \phi \leq S$.*

Proof. We already saw that the kernel is an ideal and the quotient as additive group is isomorphic to $\operatorname{Im} \phi$ which we know is a subgroup of $(S, +)$. Also $\operatorname{Im} \phi$ is closed under multiplication since $\phi(r)\phi(s) = \phi(rs)$. In addition $\phi(1_R) = 1_S$, so it is a subring of S. Consider $\Phi : R/\ker \phi \to \operatorname{Im} \phi$ which takes a coset $r + \ker \phi$ to $\phi(r)$. This is well defined from results in groups. It is obviously also a bijection and a group homomorphism under addition. To check it is a ring homomorphism, we have $\Phi(1_R + \ker \phi) = \phi(1_R) = 1_S$. Also, $\Phi((r + \ker \phi)(s + \ker \phi)) = \Phi(rs + \ker \phi) = \phi(rs) = \phi(r)\phi(s) = \Phi(r + \ker \phi)\Phi(s + \ker \phi)$. So it is a ring isomorphism. □

Corollary 8.6 (Second Isomorphism Theorem)**.** *Let $R \leq S$ and $J \trianglelefteq S$, then $R \cap I \trianglelefteq R$ and $R + J \leq S$ and*

$$R/(R \cap J) \cong (R + J)/J \leq S/J$$

Proof. $R \cap I \trianglelefteq R$ and $R + J \leq S$ are trivial. Now consider the map $\phi : R \to S/J$ by $\phi(r) = r + J$. It is obviously a well-defined ring homomorphism as the composition of the inclusion $R \to S$ and the quotient map $S \to S/J$. Its image is $(S + J)/J$ and its kernel is $R \cap J$. The result follows from Theorem 8.5. □

Analogous to the situation in groups, we have (or want to have) a bijection between certain ideals of the ring R and the ideals of the quotient ring R/I. Start with an ideal K containing I, we can send it to $\{r \in R : r + I \in K\}$. Its inverse is just $J \mapsto J/I$. This motivates the Third Isomorphism Theorem.

Corollary 8.7 (Third Isomorphism Theorem)**.** *Let $I, J \trianglelefteq R$ such that $I \subset J$, then $J/I \trianglelefteq R/I$ and*

$$(R/I)/(J/I) \cong R/J$$

Proof. Consider $\phi : R/I \to R/J$ by $r + I \mapsto r + J$. Since $I \subset J$, this is well-defined and obviously a ring homomorphism with kernel J/I. Finish by Theorem 8.5. □

Example 8.2. There is a surjective ring homomorphism $\mathbb{R}[X] \to \mathbb{C}$ by

$$\sum_{k=0}^{n} a_k X^k \mapsto \sum_{k=0}^{n} a_k i^k$$

Then the kernel, by division algorithm, would be (X^2+1), hence we immediately obtain $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$ by Thoerem 8.5

Example 8.3 (Characteristic of a Ring)**.** For a ring R, there is an unique ring homomorphism $\mathbb{Z} \to R$. The uniqueness is obvious since a ring homomorphism must map the multiplicative identity to multiplicative identity. The existence can be shown by simply constructing $\iota : n \mapsto 1_R + 1_R + \cdots + 1_R$ where there are n of 1_R's added together. Similarly $\iota : -n \mapsto -(1_R + 1_R + \cdots + 1_R)$ where again there are n of 1_R's in the bracket. So $\ker \iota \trianglelefteq \mathbb{Z}$, hence $\ker \iota = n\mathbb{Z}$ for some $n \in \mathbb{N}_0$.

Definition 8.6. We say n is the characteristic $\operatorname{char}(R)$ of R.

By Theorem 8.5, $\mathbb{Z}/n\mathbb{Z} \cong \operatorname{Im} \iota \leq R$.

Example 8.4. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ all have characteristic 0, and $\mathbb{Z}/p\mathbb{Z}$ has characteristic p.

9 Integral Domains, Maximal and Prime Ideals

9.1 Integral Domains

Definition 9.1. An integral domain is a ring R with $0 \neq 1$ and $ab = 0$ implies $a = 0$ or $b = 0$.

Definition 9.2. In a ring R, an element $a \neq 0$ is called a zero divisor if $\exists b \in R, b \neq 0, ab = 0$.

So an integral domain is a ring without zero divisors.

Example 9.1. 1. All fields are integral domains.
2. Any subring of an integral domain is an integral domain. Hence $\mathbb{Z}[i] \leq \mathbb{C}$ is an integral domain.
3. (non-example) $\mathbb{Z} \times \mathbb{Z}$ is not an integral domain since $(1,0)(0,1) = (0,0)$.

Lemma 9.1. *If R is an integral domain, so is $R[X]$.*

Proof. Let $f, g \in R[X]$ be nonzero polynomials. Suffice to show that $\deg(fg) = \deg(f) + \deg(g)$. Indeed, if

$$f(X) = \sum_{k=0}^{n} a_k X^k, g(X) = \sum_{k=0}^{m} b_k X^k, a_n, b_m \neq 0$$

Then $f(X)g(X) = a_n b_m X^{n+m} + \cdots$, but since R is an integral domain, $a_n b_m \neq 0$, therefore $\deg(fg) = n + m = \deg(f) + \deg(g)$. □

Lemma 9.2. *Let R be an integral domain and $0 \neq f \in R[X]$. Then the number of roots of f in R is at most n.*

Proof. Exercise. □

Theorem 9.3. *Any finite subgroup of the multiplicative group of a field is cyclic.*

Example 9.2. $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.
Also, $U_m = \{x^m = 1 : x \in \mathbb{C}\}$ is cyclic.

Proof. Let F be a field and A a finite subgroup of $F^\times$. So A is a finite abelian group, and if it is not cyclic, then by Theorem 6.4, it contains a subgroup isomorphic to $C_m \times C_m$ for some $m \geq 2$, but then $f(X) = X^m - 1$ has at least m^2 roots, contradicting the preceding lemma. □

Proposition 9.4. *Any finite integral domain is a field.*

Proof. Let R be a finite integral domain. For any $0 \neq a \in \mathbb{R}$, the map $\phi : R \to R$ by $r \mapsto ra$ is injective since R is an integral domain, hence is surjective since R is finite. In particular, there is some r such that $ra = 1$. □

Combining these two shows that every finite integral domain has cyclic multiplicative group.

Theorem 9.5. *Let R be an integral domain, then there is a field F with the following properties:*
1. $R \leq F$.
2. Every element of F can be written as ab^{-1} where $a, b \in R$.

Consequently, such an F is the unique minimal field containing R. F is called the field of fractions of R.

Example 9.3. The field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$.

Proof. Consider the set $F = (R \times R \setminus \{0\})/\sim$ where

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

We write the equivalence class containing (a,b) as a/b. One can show that this is an equivalence relation since R is an integral domain and that the following operations are well-defined:

$$(a/b) + (c/d) = (ad+bc)/(bd), (a/b)(c/d) = (ac)/(bd)$$

F is obviously a field under these two operations. Also we can embed R into F by $r \mapsto r/1$ and we have $a/b = (a/1)(1/b) = (a/1)(b/1)^{-1} = ab^{-1}$, so this is the field we want. □

Example 9.4. 1. The field of fraction of the Gaussian integers $\mathbb{Z}[i]$ is the set $\{ab^{-1} : a, b \in \mathbb{Z}[i] \leq \mathbb{C}\}$. More precisely, F consists of complex numbers in the form $p + iq, p, q \in \mathbb{Q}$.
2. The field of fraction of the polynomial ring $R[X]$ over a ring R is called the field of rational functions $R(X)$ of R.

9.2 Prime and Maximal Ideals

Lemma 9.6. *A ring R is a field iff its only ideals are $\{0\}, R$.*

Proof. Trivial. □

Definition 9.3. Let S be a collection of subsets of a set X. $A \in S$ is maximal if there does not exists $B \in S$ such that $A \subsetneq B$.
An ideal $I \trianglelefteq R$ is maximal if it is maximal in the set of all proper ideals $\mathcal{I}_R = \{J \trianglelefteq R : J \neq R\}$.

Proposition 9.7. *Let $I \trianglelefteq R$ be a proper ideal, then R/I is a field iff I is maximal.*

Proof. R/I is a field iff $I/I, R/I$ are the only ideals of R/I, which happens iff I and R are the only ideals of R containing I iff I is maximal. □

Definition 9.4. An ideal $I \trianglelefteq R$ is prime if $I \neq R$ and $ab \in I$ implies that at least one of a, b is in I.

Example 9.5. The prime ideals of $\mathbb{Z}$ are $p\mathbb{Z}$ with p prime or 0. Incidentally, $p\mathbb{Z}$ are also all maximal ideals of $\mathbb{Z}$.

Proposition 9.8. *Let $I \trianglelefteq R$ be a proper ideal, then I is prime iff R/I is an integral domain.*

Proof. I is prime iff $ab \in I \implies a \in I \vee b \in I$ iff $ab + I = I \implies a + I = I \vee b + I = I$ iff R/I is an integral domain. □

Remark. Combining the results reveals that every maximal ideal is prime.

Remark. If $\text{char}(R) = n \geq 2$, then $\mathbb{Z}/n\mathbb{Z} \leq R$, hence n is prime. In particular, the characteristic of a field F is either 0 or a prime number. When the field has characteristic 0, then $\mathbb{Z} \leq F$, hence $\mathbb{Q} \leq F$ since F is a field.

10 Factorization in Integral Domains

In this section, R will always denote an integral domain.

10.1 Prime and Irreducible Elements

Definition 10.1. $a \in R$ is said to divide $b \in R$, written as $a|b$, if $\exists c \in R, b = ac$. Or equivalently, $(b) \subset (a)$.
$a, b \in R$ are associates if $a = bc$ for some unit $c \in R$. Equivalently, $(a) = (b)$.
A nonzero nonunit element $r \in R$ is irreducible if $ab = r$ implies that at least one of a, b is a unit. It is prime if $r|ab \implies r|a \vee r|b$.

Note that these properties depend on the underlying ring R. For example, 2 is irreducible and prime in $\mathbb{Z}$ but not in $\mathbb{Q}$. Also $2X$ is irreducible in $\mathbb{Q}[X]$ but not in $\mathbb{Z}[X]$.

Lemma 10.1. *For any $r \in R$, (r) is prime iff $r = 0$ or r is prime.*

Proof. If (r) is prime and $r \neq 0$, then since (r) is proper r is not a unit, and if $r|ab$, then $ab \in (r)$, so $a \in (r)$ or $b \in (r)$, so $r|a$ or $r|b$, so r is prime.
Conversely, (0) is prime and for r a prime, $ab \in (r) \implies r|ab \implies r|a \vee r|b \implies a \in (r) \vee b \in (r)$, so (r) is a prime ideal. □

One find that an integer is maximal iff it is prime. We want to generalize this to some other integral domains.

Lemma 10.2. *Every prime element is irreducible.*

Proof. Suppose $r \in R$ is prime, then it is nonzero and not a unit. If $r = ab$, then $r|a$ or $r|b$. WLOG $r|a$, then $a = rc$ for some $c \in R$, so $r = rcb \implies r(cb - 1) = 0 \implies cb = 1$, hence b is a unit. Therefore r is irreducible. □

The converse, sadly, does not hold in general.

Example 10.1 (Non-example)**.** Let $R = \mathbb{Z}[\sqrt{-5}]$, which is the subring of the field $\mathbb{C}$, hence is an integral domain. Define the norm $N : R \to \mathbb{Z}_{\geq 0}$ by $a + b\sqrt{-5} \mapsto a^2 + 5b^2$, which one can verify is multiplicative and $N(r) = 1 \implies r = \pm 1$. Now the only units in R are ± 1. Indeed if $rs = 1$, then $1 = N(rs) = N(r)N(s)$, so $N(r) = N(s) = 1$, so $r, s \in \{\pm 1\}$.
We claim that 2 is irreducible in R. Suppose $2 = rs$, then $N(r)N(s) = N(rs) = 4$, but one can show that there is no element with norm 2, so one of $N(r), N(s)$ must be 1, which means that it is a unit. Similarly, $3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are all irreducible using exactly the same way. However, $(1+\sqrt{-5})(1-\sqrt{-5}) = 6 = 2 \cdot 3$, but neither $1 + \sqrt{-5}$ nor $1 - \sqrt{-5}$ is divisible by 2 (by either taking norms or finding out directly), therefore 2 is not prime.

Also, in this particular ring R, unique factorization fails as we can factorize 6 into two different products of irreducibles which cannot be saved by multiplying a unit.

10.2 Principal Ideal Domains

Definition 10.2. An integral domain R is a principal ideal domain (PID) if every ideal of R is principal.

Example 10.2. $\mathbb{Z}$ is a PID.

We will later show that $\mathbb{Z}[i]$ and $\mathbb{F}[X]$ for a field $\mathbb{F}$ are also PIDs.

Lemma 10.3. *Let $0 \neq r \in R$, if (r) is maximal, then r is irreducible. If R is a PID, then the converse holds.*

Proof. We have $(r) \neq 0, R$ by assumption, so r is neither 0 or a unit. If $r = ab$ for some $a, b \in R$, then $(r) \subset (a) \subset R$. Hence $(a) = R$ so a is a unit, or $(r) = (a)$, therefore $r = au$ for a unit u. So $au = ab \implies b = u$ is a unit. Hence r is irreducible. Conversely, given that R is a PID, suppose r is irreducible, then if $(r) \subset J \subset R$ for some ideal $J = (a)$ for some $a \in R$. Then $r = ab$ for some $b \in R$, but r is irreducible, so either b is a unit whence $(r) = (a) = J$, or a is a unit whence $J = R$, therefore (r) is maximal. □

Proposition 10.4. *In a PID, every irreducible element is prime.*

First proof. Let R be the PID. Start with an irreducible $p \in R$. So p is nonzero and not a unit. Suppose $p \mid ab$ and $p \nmid a$. Consider the ideal (a, p), which equals to (d) for some $d \in R$ since R is a PID. Then $p = cd$ for some $c \in R$, so one of c, d is a unit.
If c is a unit, then $(p) = (d) = (a, p)$, therefore $p|a$, contradiction. If d is a unit, then $(a, p) = (d) = R$, so there is some r, s such that $ar + ps = 1$, hence $rab + sbp = b$, so $p|b$. □

Second proof. Given $p \in R$ irreducible, then (p) is maximal by the preceding lemma, so $R/(p)$ is a field which is in particular an integral domain. Hence (p) is a prime ideal, which means that p is prime. □

Definition 10.3. An integral domain R is called an Euclidean domain (ED) if there is a function $\phi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ (the Euclidean function) such that for any $a, b \in R$:
1. If $a, b \neq 0$ and $a|b$, then $\phi(b) \geq \phi(a)$.
2. If $b \neq 0$, then $\exists q, r > 0, a = qb + r$ such that either $r = 0$ or $\phi(r) < \phi(b)$.

Proposition 10.5. *If R is an Euclidean domain, then it is a PID.*

Proof. Let ϕ be the Euclidean function and $0 \neq I \lhd R$ an ideal. Choose $b \in I$ such that it is nonzero and $\phi(b)$ is minimal. We shall show that $I = (b)$. Note that we immediately have $(b) \subset I$. For the other way, choose $0 \neq a \in I$, we write $a = qb + r$ with $q, r \in R$ and either $r = 0$ or $\phi(r) < \phi(b)$. If $r = 0$ then $a \in (b)$. Otherwise, note that $r = a - qb \in I$, but $\phi(r) < \phi(b)$, contradicting the minimality of b. So we must have $a \in (b)$, hence $I = (b)$. □

Remark. Note that we did not use the first criterion to define the Euclidean function in the above proof. The reason for us to include that in the definition of a ED is that it allows us to describe the units in R in the way that $\phi(a) = \phi(1)$ iff a is unit.

Example 10.3. 1. $\mathbb{Z}$ is a ED since we can take $\phi(n) = |n|$.
2. For a field $\mathbb{F}$, $\mathbb{F}[X]$ is a ED by taking $\phi(P) = \deg P$ since we can do division with remainder in the polynomial ring of a field.
3. Consider the Gaussian integer $R = \mathbb{Z}[i] \leq C$ by taking $\phi(a + ib) = a^2 + b^2$, so ϕ is multiplicative therefore we get the first criterion. For the second, let $z_1, z_2 \in R$. Consider $z_1/z_2 \in \mathbb{C}$, which has distance strictly less than 1 from the nearest Gaussian integer, so $z_1/z_2 = q+\epsilon$ where $q \in R$ and $|\epsilon| < 1$, so $z_1 = qz_2+r$ where $r = \epsilon z_2 = z_1 - qz_2 \in R$ and $\phi(r) = |\epsilon z_2|^2 = |\epsilon|^2\phi(z_2) < \phi(z_2)$.

The above examples are all also PIDs by the preceding proposition.

Example 10.4. 1. Let A be an $n \times n$ matrix in the field $\mathbb{F}$, and let I be the set of all $f \in \mathbb{F}[X]$ such that $f(A) = 0$. Now I is trivially an ideal. But this ideal is principal since $\mathbb{F}[X]$ is a ED hence PID. Suppose $I = (f)$, then for any $g \in \mathbb{F}[X]$ such that $g(A) = 0$, we have $f|g$. So f is the minimal polynomial of A.
2. Consider $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ and let $f(X) = X^3 + X + 1 \in \mathbb{F}_2[X]$. We want to show that f is irreducible. Suppose $f(X) = g(X)h(X)$ with $\deg g, \deg h > 0$. So one of $\deg g$ and $\deg f$ must be 1 since f has degree 3, so f has a root, but it does not, contradiction.
But $\mathbb{F}_2[X]$ is a ED hence PID, therefore (f) is maximal, so we get to construct a field $\mathbb{F}_2[X]/(X^3+X+1)$. The quotient looks like $\{aX^2+bX+c+(X^3+X+1) : a, b, c \in \mathbb{F}_2\}$, but a, b, c uniquely determines the ideal, so this is a field of order 8.
3. (non-example) The ring $\mathbb{Z}[X]$ is not a PID. Indeed, consider the ideal $I = (2, X)$, then $I = \{2f_1(X) + Xf_2(X) : f_1, f_2 \in \mathbb{Z}[X]\} = \{f(X) \in \mathbb{Z}[X] : f(0) \text{ is even}\}$. Suppose I is generated by some polynomial $f \in \mathbb{Z}[X]$, so $2 = fg$ for some $g \in \mathbb{Z}[X]$. But degrees add when polynomials multiply, hence f, g has to be constant. Therefore I can only be $\mathbb{Z}[X]$ or $2\mathbb{Z}[X]$, but both are impossible since $1 \notin I$ (so I is not the entire ring) and $X \in I$ (but $X \notin 2\mathbb{Z}[X]$).

10.3 Unique Factorization Domains

Definition 10.4. An integral domain R is called a unique factorization domain (UFD) if
1. Every nonzero and nonunit $r \in R$ is a product of irreducibles.
2. If $p_1 \cdots p_m = q_1 \cdots q_n$ where p_i, q_i are irreducibles, then $m = n$ and $\exists \sigma \in S_n$ such that p_i is an associate with $q_{\sigma(i)}$.

Proposition 10.6. *Let R be an integral domain having the first property stated above, then R is a UFD iff every irreducible is prime.*

Proof. If R is a UFD and $r \in R$ is irreducible and $p|ab$, then $pc = ab$ for some $c \in R$. By the first condition, we can write a, b, c as products of irreducibles, so an associate of p must appear in the factorization of a or b by the second condition, so $p|a$ or $p|b$, hence p is prime.
Suppose every irreducible is prime and $p_1 \cdots p_m = q_1 \cdots q_n$. Since p_1 is prime, then $p_1|q_i$ for some i. But q_i, p_1 are both irreducible, so they are associates. By reordering, we can write $i = 1$, and by cancellation law, $p_2 \cdots p_m = q_2 \cdots q_n$. The proof is finished by descent (or, equivalently, induction). □

Lemma 10.7. *Let R be a PID and $I_1 \subset I_2 \subset \cdots$ be a nested sequence of ideals, then there exists some $N \in \mathbb{N}$ such that $I_n = I_N$ for every $n \geq N$.*

Remark. This condition is one of the formulations of the definition of a Noetherian ring.

Proof. Consider the union $I = I_1 \cup I_2 \cup \cdots$. I is obviously an ideal, so $I = (a)$ for some $a \in R$. But $a \in I_N$ for some $N \in \mathbb{N}$, so for any $n \geq N$, we have $(a) \subset I_n \subset I = (a)$, hence $I_n = (a) = I_N$. □

Theorem 10.8. *Every PID is a UFD.*

Proof. Let R be a PID. By Proposition 10.6, since every irreducible in a PID is prime, it suffices to show the first condition of a UFD. Let $x \in R$ be nonzero and nonunit. Suppose x cannot be written as a product of irreducibles, so in particular x is not irreducible. Therefore we can write $x = x_1 y_1$ for nonunit x_1, y_1. But not both of x_1, y_1 can be written as a product of irreducibles. WLOG x_1 is not a product of irreducibles, also we have $(x) \subsetneq (x_1)$ since y_1 is not a unit. Continue the process over and again gives a sequence of strictly nested ideals $(x) \subsetneq (x_1) \subsetneq \cdots$, but this is a sequence of nested ideals that does not terminate, hence contradiction to the preceding lemma. □

Example 10.5. We know that ED implies PID implies UFD implies integral, so we have the following table of examples:

	ED	PID	UFD	Integral	
$\mathbb{Z}/4\mathbb{Z}$				No	
$\mathbb{Z}[\sqrt{5}]$			No	Yes	See later.
$\mathbb{Z}[X]$		No	Yes		See later.
$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$	No	Yes			See in Number Fields.
$\mathbb{Z}[i]$	Yes				

Definition 10.5. Let R be a integral domain. We say d is a greatest common divisor of $a_1, \ldots, a_n \in R$ if $d|a_i$ for each i and if $\forall i, d'|a_i$, then $d'|d$. We say m is a least common multiple of $a_1, \ldots, a_n \in R$ if $a_i|d$ for each i and if $\forall i, a_i|d'$, then $d|d'$.

Both GCDs and LCMs, when they exists, are unique up to associates.

Proposition 10.9. *In a UFD, both LCMs and GCDs exist.*

Proof. Obvious. □

11 Factorization in Polynomial Rings

Theorem 11.1. *If R is a UFD, so is $R[X]$.*

Remark. One can apply this recursively to show that the polynomial ring in n variables over a UFD is a UFD.

In particular, $\mathbb{Z}[X]$ is a UFD and $\mathbb{C}[X_1, \ldots, X_n]$ is a UFD.
In this section, we shall always assume that R is a UFD. It is in particular an integral domain, so it has a field of fraction F whose polynomial ring $F[X]$ is a UFD since it is a ED.

Definition 11.1. The content of a polynomial $f(X) = a_0 + a_1X + \cdots + a_nX^n$ for $a_i \in R$ is $c(f) = \gcd(a_0, \ldots, a_n)$. We say f is primitive if $c(f)$ is a unit, i.e. the coefficients are coprime.

Lemma 11.2. *1. Any prime element in R is also prime in $R[X]$.*
2. If $f, g \in R[X]$ are primitive polynomials, then fg is also primitive.
3. If $f, g \in R[X]$, then $c(fg) = c(f)c(g)$ up to associates.

Proof. 1. Given a prime $p \in R$, $R/(p)$ is an integral domain. For $a \in R$, let $\tilde{a} \in R/(p)$ be its image under the quotient map. Define $\theta : R[X] \to R/(p)[X]$ by

$$a_0 + a_1X + \cdots + a_nX^n \mapsto \tilde{a}_0 + \tilde{a}_1X + \cdots + \tilde{a}_nX^n$$

which is a homomorphism. So for $p|fg$ where $f, g \in R[X]$, we have $\theta(fg) = 0$, so $\theta(f)\theta(g) = 0$. But $R/(p)[X]$ is an integral domain since $R/(p)$ is. Hence WLOG $\theta(f) = 0$, so $p|f$.
2. If f, g are primitive but fg is not, then there is some irreducible $p \in R$ that divides fg. Since R is a UFD, p is prime in R, hence is prime in $R[X]$ by 1, hence $p|f$ or $p|g$, contradiction to their primitivity.
3. Write $f = c(f)f_0$, so f_0 is primitive. Do the same to g gives $g = c(g)g_0$ for a primitive g_0, so $fg = c(f)c(g)(f_0g_0)$. But f_0g_0 is primitive by 2, so $c(fg) = c(f)c(g)$ up to associates. □

Remark. Take a polynomial f in $F[X]$, then we can write $f = ab^{-1}f_0$ where $f_0 \in R[X]$ where $a, b \in R, b \neq 0$ and f_0 is primitive. We can just take b to be a common multiple of the denominators (since F is the field of fractions of R) and the rest follows.

Lemma 11.3. *Let f, g be polynomials in $R[X]$ and g is primitive. If $g|f$ in $F[X]$, then $g|f$ in $R[X]$.*

Proof. If $g|f$ in $F[X]$, then $f = gh$ with $h \in F[X]$. Write $h = ab^{-1}h_0$ for $a, b \in R, b \neq 0$ and $h_0 \in R[X]$ is primitive. So $bf = agh_0$, then by taking content $bc(f) = a$, so $h = c(f)h_0 \in R[X]$ which is what we wanted. □

Lemma 11.4 (Gauss's Lemma)**.** *Let R be a UFD with field of fraction F. Suppose $f \in R[X]$ is primitive and irreducible in $R[X]$, then f is irreducible in $F[X]$.*

Proof. Assume that $\deg f > 0$ since otherwise f has to be constant. Suppose we can write $f = gh$ for $g, h \in F[X]$ with $\deg g, \deg h > 0$. Replacing g, h by λg and $\lambda^{-1}h$ for some $\lambda \in F^\times$, we can assume WLOG that $g \in R[X]$ and is primitive. $g|f$ in $R[X]$ by Lemma 11.3, so $h \in R[X]$, contradiction. □

Lemma 11.5. *Let $g \in R[X]$ be primitive. If g is prime in $F[X]$, then it is prime in $R[X]$.*

Proof. Lemma 11.3. □

Proof of Theorem 11.1. Let $f \in R[X]$, write $f = c(f)f_0$ where f_0 is primitive. Since R is a UFD, we can write $c(f)$ as a product of irreducibles. Also, f_0 can also be written as a product of irreducibles by induction on its degree. So it suffices to show that every irreducible in $R[X]$ is prime.
Take $f \in R[X]$ irreducible, then either f is constant or f must be primitive.

The former case is clear by the first part of Lemma 11.2 since f must be prime in R. Combining Lemma 11.4 and Lemma 11.5 gives the result for the latter case. □

Theorem 11.6 (Eisenstein's Criterion)**.** *Let R be a UFD and $f = a_0 + \cdots + a_n X^n \in R[X]$ be primitive. Suppose $p \in R$ is irreducible, $p \nmid a_n$, $p \mid a_i$ for $0 \leq i \leq n-1$ and $p^2 \nmid a_0$, then f is irreducible.*

Proof. Since R is a UFD, p is prime. Suppose $f = gh$ where $g, h \in R[X]$ are not unit. Since f is primitive, g, h both have positive degree. Write $g(X) = r_0 + \cdots + r_k X^k$ and $h(X) = s_0 + \cdots + s_l X^l$ where $k + l = n$. Now $a_n = r_k s_l$, so $p \nmid r_k, p \nmid s_l$. Also $a_0 = r_0 s_0$, so exactly one of r_0, s_0 is divisible by p. Assume WLOG that $p \mid r_0$. Choose $j \leq k < n$ such that $p \mid r_0, \cdots, p \mid r_{j-1}$ but $p \nmid r_j$ (which we can do since $p \nmid r_k$). Then

$$a_j = r_0 s_j + r_1 s_{j-1} + \cdots + r_j s_0 \in r_j s_0 + (p)$$

So $p \nmid a_j$, contradiction. □

Example 11.1. Consider $f(X) = X^3 + 2X + 5 \in \mathbb{Z}[X]$. If f is reducible, then it must has a root, which is impossible since the only possibilities of root are $\pm 1, \pm 5$. By Guass's Lemma, this is also irreducible in $\mathbb{Q}$. Hence $\mathbb{Q}[X]/(f)$ is a field since $\mathbb{Q}[X]$ is a PID and f is irreducible.

Example 11.2. 1. Let p be a prime number, then the polynomial $X^n - p$ is irreducible by Eisenstein's criterion, hence it is also irreducible in $\mathbb{Q}[X]$, so again $\mathbb{Q}[X]/(X^n - p)$ is a field.
2. Let $f(X) = X^p + \cdots + X + 1 \in \mathbb{Z}[X]$ where p is prime. Although we cannot apply Eisenstein's criterion directly, we can do a substitution.

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

where we can apply Eisenstein's criterion to see that $f(X+1)$ is irreducible, hence $f(X)$ is also irreducible.

12 Algebraic Integers

12.1 The Gaussian Integers

Recall the ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \leq \mathbb{C}$ is a ED due to the norm $N(a+bi) = a^2 + b^2$. Hence $\mathbb{Z}[i]$ is a PID hence UFD. In particular irreducibles and primes are the same. The units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$ by the norm N. By convention, primes in $\mathbb{Z}$ are positive (since others are associates to them), but there is no corresponding convention in the Gaussian Integers.

Lemma 12.1. *If $\pi \in \mathbb{Z}[i]$ is prime, then there is a unique prime $p \in \mathbb{Z}$ with $\pi | p$.*

Proof. Since π is nonzero and nonunit, we can write $N(\pi) = p_1 \cdots p_n$ where $p_i \in \mathbb{Z}$ are (not necessarily distinct) primes. But $\pi | \pi\bar{\pi} = N(\pi) = p_1 \cdots p_n$, so there is some i such that $\pi | p_i$.
For uniqueness, if $\pi | p, \pi | q$ with p, q distinct primes in $\mathbb{Z}$, then there is some $a, b \in \mathbb{Z}$ such that $ap + bq = 1$, so $\pi | 1$, so π is a unit, contradiction. □

Lemma 12.2. *Let $p \in \mathbb{Z}$ be a prime in $\mathbb{Z}$, then the followings are equivalent:*
1. p is not prime in $\mathbb{Z}[i]$.
2. p can be written as the sum of two squares.
3. $p = 2$ or $p \equiv 1 \pmod 4$.

Proof. $1 \implies 2$: Write $p = xy$ where $x, y \in \mathbb{Z}[i]$ are not unit, then $p^2 = N(p) = N(x)N(y)$. But x, y are not unit hence have ≥ 1 norm, therefore $N(x) = N(y) = p$, so p is the sum of two squares.
$2 \implies 3$: Obvious.
$3 \implies 1$: $2 = (1 - i)(1 + i)$, so 2 is not prime. Otherwise, for $p \equiv 1 \pmod 4$, then $-1 = x^2 \pmod p$ is solvable, so $p | (x + i)(x - i)$. If p is prime in $\mathbb{Z}[i]$, then either $p | x + i$ or $p | x - i$, none of which can happen. □

Theorem 12.3. *1. Every prime $p \equiv 1 \pmod 4$ in $\mathbb{Z}$ is the sum of two integer squares $p = a^2 + b^2$.*
2. Primes in the Gaussian Integers (up to associates) are $1 + i$, primes in $\mathbb{Z}$ which congruent to 3 mod 4, and $a \pm bi$ where a, b are as in 1.

Proof. 1. The preceding lemma.
2. Let $\pi \in \mathbb{Z}[i]$ be prime in $\mathbb{Z}[i]$, then $\pi | p$ for some prime $p \in \mathbb{Z}$. If $p \equiv 3 \pmod 4$, then p is prime in $\mathbb{Z}[i]$ and π, p are associates.
Otherwise, $p = (a + ib)(a - ib)$ by the preceding lemma, so each of $a \pm ib$ has norm p hence is prime, so π is associate to one of $a \pm ib$. Note that $1 + i, 1 - i$ are associates but $a \pm ib$ are not associates otherwise by simple calculation. This completes the proof. □

Corollary 12.4. *Any integer $n \geq 1$ is a sum of two squares iff every prime factor p of n with $p \equiv 3 \pmod 4$ divides n to an even power.*

Proof. $\exists a, b \in \mathbb{Z}, n = a^2 + b^2$ if and only if $n = N(x)$ for some $x \in \mathbb{Z}[i]$, which happens iff n is a product of norms of primes in $\mathbb{Z}[i]$, but by preceding theorem, the norms of primes in $\mathbb{Z}[i]$ are either primes in $\mathbb{Z}$ or the squares of primes congurent to 3 mod 4. □

Example 12.1. $65 = 5 \cdot 13$, so 65 is a sum of two squares. Indeed $65 = 1 + 64 = 1 + 8^2$ does it. Another way to get this sum is to write $65 = (2 + i)(2 - i)(2 + 3i)(2 - 3i) = |(2 + i)(2 + 3i)|^2 = |1 + 8i|^2 = 1 + 8^2$. We also have $65 = |(2 + i)(2 - 3i)|^2 = |7 - 4i|^2 = 7^2 + 4^2$.

12.2 Algebraic Integers

Definition 12.1. Suppose $R \leq S$ are rings. Given $\alpha \in S$, we write $R[\alpha]$ for the smallest subring of S containing both R and α.

We know that such a subring exists since we can collect all the candidates and take their intersection. In fact, $R[\alpha] = \phi(R[X])$ where $\phi : R[X] \to S$ is the evaluation homomorphism $f(X) \mapsto f(\alpha)$.

Definition 12.2. If $R \leq S$ are fields and $\alpha \in S$, we write $R(\alpha)$ to denote the smallest subfield of S containing R and α.

In other words, $R(\alpha)$ is the field of fraction of $R[\alpha]$.

Definition 12.3. 1. $\alpha \in \mathbb{C}$ is an algebraic number if $\exists f \in \mathbb{Q}[X] \setminus \{0\}, f(\alpha) = 0$.
2. $\alpha \in \mathbb{C}$ is an algebraic integer if $\exists f \in \mathbb{Z}[X]$ such that the leading coefficient of f is 1 with $f(\alpha) = 0$.

Let α be an algebraic number and $\phi : \mathbb{Q}[X] \to \mathbb{C}$ be the evaluation $f[X] \mapsto f(\alpha)$, then since $\mathbb{Q}[X]$ is a PID, $\ker \phi = (f)$ for some $f \in \mathbb{Q}[X]$. Since α is an algebraic number, $f \neq 0$. We may assume that f is monic (since $\mathbb{Q}$ is a field), so we say f is the minimal polynomial of α. By the isomorphism theorem, we have $\mathbb{Q}[X]/(f) \cong \mathbb{Q}[\alpha] \leq \mathbb{C}$.
But $\mathbb{Q}[\alpha]$ is hence a integral domain, which means that f is prime (hence irreducible as $\mathbb{Q}[X]$ is a UFD), therefore (f) is maximal (since $\mathbb{Q}[X]$ is a PID), which means that $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$.

Lemma 12.5. *Let α be an algebraic number with minimal polynomial $f \in \mathbb{Q}[X]$. Write $f = \lambda f_0$ where $\lambda \in \mathbb{Q}^\times$ and $f_0 \in \mathbb{Z}[X]$ is primitive. Then the ring homomorphism given by $\phi : \mathbb{Z}[X] \to \mathbb{C}$ by $g(X) \mapsto g(\alpha)$ has $\ker \phi = (f_0)$.*

Proof. Clearly $\phi(f_0) = f_0(\alpha) = \lambda^{-1} f(\alpha) = 0$, so $(f_0) \subset \ker \phi$. Suppose we have some other $g \in \ker \phi$, then $f | g$ in $\mathbb{Q}[X]$ and hence $f_0 | g$ in $\mathbb{Q}[X]$, but then $f_0 | g$ in $\mathbb{Z}[X]$ by Lemma 11.3, therefore $g \in (f_0)$. □

Suppose further that α is an algebraic integer, then $\ker \phi = (f_0) \lhd \mathbb{Z}[X]$. But by definition of algebraic integer (f_0) contains a monic polynomial, which must mean that one of $\pm f_0$ is monic. We have $f = \lambda f_0$ with the assumption that f is monic, so $\lambda = \pm 1$, so $f \in \mathbb{Z}[X]$. Consequently, we get $\mathbb{Z}[X]/(f_0) = \mathbb{Z}[X]/(f) \cong \mathbb{Z}[\alpha] \leq \mathbb{C}$.

Example 12.2. $i, \sqrt{2}, (-1 + \sqrt{3})/2, \sqrt[n]{p}$ are all algebraic integers and indeed their minimal polynomials are $X^2 + 1, X^2 - 2, X^2 + X + 1, X^n - p$. In particular, $\mathbb{Z}[X]/(X^2 + 1) \cong \mathbb{Z}[i]$.

Lemma 12.6. *An algebraic number $\alpha \in \mathbb{C}$ is an algebraic integer if and only if its minimal polynomial (which by convention is monic) has integer coefficients.*

Proof. Immediate. □

Corollary 12.7. *If α is an algebraic integer and $\alpha \in \mathbb{Q}$, then $\alpha \in \mathbb{Z}$.*

Proof. By preceding lemma. □

13 Noetherian Rings

We have seen in the proof of PID implying UFD that PIDs has the ascending chain condition:

Definition 13.1. A ring R is said to satisfy the ascending chain condition (ACC) if any ascending chain of ideals $I_1 \subset I_2 \subset \cdots$ eventually terminates.

Lemma 13.1. *A ring R satisfies ACC iff all ideals $I \in R$ are finitely generated.*

Proof. Trivial. □

Definition 13.2. A ring R is called Noetherian if it satisfies ACC.

Theorem 13.2 (Hilbert's Basis Theorem)**.** *If R is Noetherian, then $R[X]$ is also Noetherian.*

Proof. Start with an ideal $J \trianglelefteq R[X]$. Pick $f_1 \in J$ with minimal degree. If $J = (f_1)$, we are done. Otherwise we can pick $f_2 \in J \setminus (f_1)$ with minimal degree. Continuing this, if J is not finitely generated, then there is a nested sequence

$$(f_1) \subsetneq (f_1, f_2) \subsetneq \cdots, \deg f_1 \leq \deg f_2 \leq \cdots$$

Let a_i be the leading coefficient of f_i, then consider a chain of ideals $(a_1) \subset (a_1, a_2) \subset \cdots$. R is Noetherian, so this sequence must eventually terminates, so in particular there is some $m \in \mathbb{N}$ such that $a_{m+1} \in (a_1, \ldots, a_m)$. So $a_{m+1} = \lambda_1 a_1 + \cdots + \lambda_m a_m$. Now consider

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

So g, f_{m+1} has the same degree and leading coefficient, so $\deg(f_{m+1} - g) < \deg f_{m+1}$. But $f_{m+1} - g \in J$, so since we chose f_{m+1} to have the minimal degree in $J \setminus (f_1, \ldots, f_m)$, $f_{m+1} - g \in (f_1 \ldots, f_m)$, so $f_{m+1} \in (f_1, \ldots, f_m)$, contradiction. □

Corollary 13.3. *$R[X_1, \ldots, X_n]$ is Noetherian whenever R is.*

In particular, $\mathbb{Z}[X_1, \ldots, X_n], \mathbb{F}[X_1, \ldots, X_n]$ are Noetherian (where $\mathbb{F}$ is a field).

Proof. Apply the preceding theorem recursively. □

Example 13.1. Let $R = \mathbb{C}[X_1, \ldots, X_n]$. Let $V \subset \mathbb{C}^n$ be of the form

$$V = V(\mathcal{F}) = \{(a_1, \ldots, a_n) \in \mathbb{C}^n : f(a_1, \ldots, a_n) = 0, \forall f \in \mathcal{F}\}$$

for some (possibly infinite) subset $\mathcal{F} \subset R$. Let

$$I = \left\{ \sum_{i=1}^{m} \lambda_i f_i : m \in \mathbb{N}, \lambda_i \in R, f_i \in \mathcal{F} \right\}$$

Then $I \trianglelefteq R$ and $V(I) = V(\mathcal{F})$, but R is Noetherian by the preceding corollary, so I is finitely generated and thus $V = V(\mathcal{F})$ can be defined by only finitely many polynomials.

Lemma 13.4. *Any quotient ring of a Noetherian ring is again Noetherian.*

Proof. Suppose R is Noetherian and $I \trianglelefteq R$ is an ideal. Consider a chain of ideals $J_1 \subset J_2 \subset \cdots$ in R/I. But we know the correspondence between the ideals in R/I and the ideals of R containing I, so there are ideals $I_1, I_2, \ldots$ all containing I with $J_i = I_i/I$. But then $I_1 \subset I_2 \subset \ldots$, so there is $N \in \mathbb{N}$ such that for any $m > N$, $I_m = I_N$, hence $J_m = I_m/I = I_N/I = J_N$, hence the sequence eventually terminates, thus R/I is Noetherian. □

Example 13.2. 1. The Gaussian integers can be written as $\mathbb{Z}[i] \cong \mathbb{Z}[X]/(X^2+1)$ hence is Noetherian.
2. If $R[X]$ is Noetherian, then R is Noetherian since $R \cong R[X]/(X)$, so Hilbert's Basis Theorem is actually an "if and only if".

Example 13.3 (Non-example)**.** We shall give examples of a non-Noetherian rings.
1. We consider the ring as the upper limit

$$R = \mathbb{Z}[X_1, X_2, \ldots] = \bigcup_{n\in\mathbb{N}} \mathbb{Z}[X_1, \ldots, X_n]$$

Then $(X_1) \subsetneq (X_1, X_2) \subsetneq \cdots$, so R is not Noetherian.
2. Consider the ring $R \leq \mathbb{Q}[X]$ by collecting $R = \{f \in \mathbb{Q}[X] : f(0) \in \mathbb{Z}\}$, then R is obviously a ring with

$$(X) \subsetneq (2^{-1}X) \subsetneq (2^{-2}X) \subsetneq \cdots$$

3. Consider the ring R of infinitely differentiable functions $[-1, 1] \to \mathbb{R}$ under pointwise operations, this is also not Noetherian (exercise).

14 Modules

14.1 Definition and Examples

Definition 14.1. A module over a ring R (an R-module) is a triple $(M, +, \cdot)$ where $(M, +, 0)$ for some $0 \in M$ is an abelian group and $\cdot : R \times M \to M$ (called scalar multiplication) satisfies, for any $r, r_1, r_2 \in R, m, m_1, m_2 \in M$:
1. $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$.
2. $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$.
3. $r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m$.
4. $1 \cdot m = m$.

The function $\cdot$ is called the scalar multiplication and is omitted from writing sometimes.

Remark. To show something is a module, we also need to check closure (that is $+, \cdot$ are well-defined).

Example 14.1. 1. If R is a field, then an R-module M is a vector space over R.
2. A $\mathbb{Z}$-module is precisely the same as an abelian group as the scalar multiplication can be uniquely defined by $n \cdot a = a + \cdots + a$ for n many copies of a.
3. Consider the ring $R = \mathbb{F}[X]$ for a field $\mathbb{F}$ and V a vector space over $\mathbb{F}$. Consider $\alpha : V \to V$ an endomorphism. We can make V an R-module over the scalar multiplication $\mathbb{F}[X] \times V \to V$ by $(f, v) \mapsto f(\alpha)(v)$. Note that different choice of α makes V a different module. We sometimes write this as V_α.

There are some general construction methods to produce a module.

Example 14.2. 1. For any ring R, R^n is an R-module by $r \cdot (r_1, \ldots, r_n) = (rr_1, \ldots, rr_n)$ for $r, r_i \in R$. In particular, when $n = 1$, R itself is an R-module.
2. If I is an ideal, then I is an R-module by $r \cdot i = ri$ for $r \in R, i \in I$.

3. If I is an ideal, then R/I is an R-module by $r \cdot (s + I) = rs + I$ for $r, s \in R$.
4. If $\phi : R \to S$ is a ring homomorphism, then any S-module M is also an M-module by $r \cdot m = \phi(r) \cdot m$ for $r \in R, m \in M$. In particular, if $R \leq S$, then any S-module can be viewed as an R-module.

Definition 14.2. Let M be an R-module, a subset $N \subset M$ is called a R-submodule of M, written as $N \leq M$, if $(N, +) \leq (M, +)$ and for any $r \in R, n \in N$, we have $r \cdot n \in N$.

Example 14.3. 1. Any R-submodule of R is an ideal.
2. When R is a field, then an R-module is a vector space, then a submodule is a vector subspace.

Definition 14.3. If N is a R-submodule of M, we can form the quotient M/N by taking the quotient group under addition. We can make it as an R-module by specifying the scalar multiplication $r \cdot (m + N) = r \cdot m + N$.

We can check easily that the scalar multiplication defined in this way is well-defined and makes M/N an R-module.

14.2 Homomorphisms

Definition 14.4. Let M, N be R-modules, then a function $f : M \to N$ is a homomorphism of R-modules (or R-module map) if f is a homomorphism of groups under addition and $\forall r \in R, m \in M, f(r \cdot m) = r \cdot f(m)$.
A bijective homomorphism is called an isomorphism, and two R-modules M, N are called isomorphic (written as $M \cong N$) if there is an isomorphism between them.

Example 14.4. When R is a field, a homomorphism of R-modules is a linear map.

Theorem 14.1 ((First) Isomorphism Theorem for Modules)**.** *Suppose M, N are R-modules and $f : M \to N$ is a homomorphism of R-modules, then* $\ker f \leq M, f(M) \leq N$ *and* $M/\ker f \cong f(M)$.

Proof. Similar to before. □

Theorem 14.2 (Second Isomorphism Theorem)**.** *Let A, B be R-submodules of an R=module M, then $A + B = \{a + b : a \in A, b \in B\} \leq M$ and $A \cap B \leq M$. Moreover, $A/(A \cap B) \cong (A + B)/B$.*

Proof. Use the First Isomorphism Theorem. □

To motivate the Third Isomorphism Theorem, we note that for R-modules $N \leq M$, we have the correspondance between the submodules of M/N and the submodules of M containing N.

Theorem 14.3 (Third Isomorphism Theorem)**.** *Suppose $N \leq L \leq M$ are R-modules, then $M/L \cong (M/N)/(L/N)$.*

Proof. Same. □

In particular, these are all true for vector spaces by taking the ring to be a field. One can compare these results to familiar results in linear algebra (e.g. the First Isomorphism Theorem implies the Rank-Nullity Theorem).

14.3 Finitely Generated Modules

Definition 14.5. Let M be an R-module, and $m \in M$, then the submodule Rm generated by m is the smallest R-submodule of M containing m, i.e. $Rm = \{r \cdot m : r \in R\}$.

Definition 14.6. Let M be an R-module. M is called cyclic if $M = Rm$ for some $m \in M$. M is finitely generated if $\exists m_1, \ldots, m_n \in M$ such that $Rm_1 + \cdots Rm_n = M$.

Lemma 14.4. *An R-module M is cyclic iff M is isomorphic as an R-module to R/I for some $I \trianglelefteq R$.*

Proof. If M is cyclic, write $M = Rm$, then there is a surjective R-module homomorphism $R \to M$ by $r \mapsto r \cdot m$. The claim follows by the First Isomorphism Theorem.
Conversely If $M \cong R/I$, then $M \cong R/I = R(1 + I)$. □

Lemma 14.5. *An R-module M is finitely generated iff there exists a surjective R-module homomorphism from $f : R^n \to M$ for some n.*

Proof. If M is finitely generated, then $M = Rm_1 + \cdots + Rm_n$ where $m_i \in M$, so we can take $f(r_1, \ldots, r_n) = r_1 m_1 + \cdots + r_n m_n$.
Conversely, if such a map f exists, then $M = Rf(e_1) + \cdots + Rf(e_n)$, then e_i has 1 in i^{th} entry and 0 in j^{th} entry for any $j \neq i$. □

Corollary 14.6. *The quotient of a finitely generated R-module is a finitely generated R-module.*

Proof. Obvious from the preceding lemma. □

Remark. A submodule of a finitely generated R-module needs not be finitely generated. For example, we can take a non-Noetherian ring R itself as an R-module and consider a non-finitely generated ideal of it.

Lemma 14.7. *Let R be an integral domain, then every R-submodule of a cyclic R-module is cyclic iff R is a PID.*

Proof. R itself is a cyclic R-module, so if all R-submodules of it are cyclic, then all of its ideals are generated by one element which means that R is a PID.
Conversely, if R is a PID and M is a cyclic R-module, then $M \cong R/I$ for some $I \trianglelefteq R$. The R-submodules of M are in the form J/I for $I \subset J \trianglelefteq R$. Since R is a PID, J is a principal ideal, so J/I is cyclic. □

Theorem 14.8. *Let R be a PID, and M an R-module. Suppose M is generated by n elements, then any R-submodule N of M can also be generated by at most n elements.*

Proof. $n = 1$ is the preceding lemma. For general n, we proceed by induction. Suppose $M = Rx_1 + \cdots Rx_n$. Let $M_i = Rx_1 + \cdots Rx_i$ and $0 = M_0 \leq M_1 \leq \cdots \leq M_n = M$. So we have

$$0 = M_0 \cap N \leq M_1 \cap N \leq \cdots \leq M_n \cap N = N$$

Then the R-module map $M_i \cap N \to M_i/M_{i-1}$ by $m \mapsto m + M_{i-1}$ has kernel $M_{i-1} \cap N$. Hence

$$(M_i \cap N)/(M_{i-1} \cap N) \cong M' \leq M_i/M_{i-1}$$

But since M_i/M_{i-1} is cyclic, $(M_i \cap N)/(M_{i-1} \cap N)$ is also cyclic by the preceding lemma. Say it is generated by $y_i + M_{i-1} \cap N$ for some $y_i \in M_i \cap N$. Therefore $M_i \cap N = M_{i-1} \cap N + Ry_i$. It follows that $M_i \cap N = Ry_1 + \cdots + Ry_i$. In particular, $N = M_n \cap N = Ry_1 + \cdots + Ry_n$, so N is generated by n elements. □

Example 14.5. Take $R = \mathbb{Z}$, then we know that any subgroup of $\mathbb{Z}^n$ can be generated by n elements.

15 Direct Sums and Free Modules

Definition 15.1. If $M_1, \ldots, M_n$ are R-modules, then their direct sum $M_1 \oplus \cdots \oplus M_n$ is the set $M_1 \times \cdots \times M_n$ with entry-wise addition and scalar multiplications.

Example 15.1. 1. R^n is simply $R \oplus \cdots \oplus R$ of n copies of R.
2. If $M_1, M_2 \leq M$, then the R-module homomorphism $M_1 \oplus M_2 \to M$ by $(m_1, m_2) \mapsto m_1 + m_2$ is an isomorphism iff $M_1 \cap M_2 = \varnothing$ and $M_1 + M_2 = M$.

Lemma 15.1. *Suppose $M = \bigoplus_{i=1}^n M_i$ and $N_i \leq M_i$. Let $N = \bigoplus_{i=1}^n N_i$, then*

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

Proof. Apply the first isomorphism theorem to the surjective R-module map $\phi : M \to \bigoplus_{i=1}^n M_i/N_i$ by $(m_1, \ldots, m_n) \mapsto (m_1 + N_1, \ldots, m_n + N_n)$. □

Example 15.2. Taking $R = \mathbb{Z}$ then $\mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$, then we have $(\mathbb{Z} \oplus \mathbb{Z})/(m\mathbb{Z} \oplus n\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$.

Definition 15.2. Let $m_1, \ldots, m_n \in M$. The set $\{m_1, \ldots, m_n\}$ is independent if $r_1 m_1 + \cdots + r_n m_n = 0 \implies \forall i, r_i = 0$.

Definition 15.3. A subset S of an R-module M generates M freely if S generates M and any function $\psi : S \to N$ for another R-module N extends to an R-module homomorphism $M \to N$.

Note that if such an extension exists then it is necessarily unique.

Definition 15.4. A freely-generated R-module is called a free R-module. The corresponding S is called the free basis.

Proposition 15.2. *For an R-module M and a subset $S = \{m_1, \ldots, m_n\} \subset M$, the followings are equivalent:*
1. S generates M freely.
2. S generates M and S is independent.
3. Every $m \in M$ can be written uniquely in the form $m = r_1 m_1 + \cdots + r_n m_n$ for $r_1, \ldots, r_n \in R$.
4. The R-module homomorphism $R^n \to M$ by $(r_1, \ldots, r_n) \mapsto r_1 m_1 + \ldots r_n m_n$ is an isomorphism.

Proof. $1 \implies 2$: We already knows that S generates M, so it suffices to show that S is independent. Suppose for sake of contradiction that $r_1m_1 + \ldots + r_nm_n = 0$ for some $r_i \in R$ and some r_j is nonzero. Consider the function $\psi : S \to R$ by $m_j \mapsto 1$ and $m_i \mapsto 0$ for any $i \neq j$. Suppose this extends to an R-module map $\theta : M \to R$, then $0 = \theta(0) = \theta(r_1m_1 + \cdots + r_nm_n) = r_j$, contradiction.
Remaining implications $2 \implies 3 \implies 1$ and $3 \iff 4$ are just as easy if not easier. □

Sadly not all R-modules are free. Even if it is, the free basis does not behave like what we expect from a vector space.

Example 15.3 (non-example)**.** 1. Suppose we have a nontrivial finite abelian group A, then A is not free as a $\mathbb{Z}$-module since it is not isomorphic to $\mathbb{Z}^n$ which is infinite.
2. The set $\{2, 3\} \subset \mathbb{Z}$ generates $\mathbb{Z}$ as a $\mathbb{Z}$-module, but it is not independent and no subset of it gives a free basis.

Proposition 15.3 (Theorem on Invariant of Dimension)**.** *Let R be a nonzero ring. If $R^m \cong R^n$ as R-modules, then $m = n$.*

We introduce the following general construction: Let R be a ring and $I \trianglelefteq R$ and M is an R-module. We write $IM = \{im : i \in I, m \in M\} \leq M$. Then the quotient $M/(IM)$ is an R/I module by $(r + I)(m + IM) = rm + IM$. Also by Zorn's Lemma, for any proper ideal I in a ring R, there is a maximal ideal containing I (this is obvious when R is Noetherian). [1]

Proof. Return to our proof, suppose $R^m \cong R^n$. Choose $I \trianglelefteq R$ maximal, then we have

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

Both sides can be made into R/I-modules canonically. But R/I is a field, so $m = n$. □

16 The Structure Theorem

Until further notice, we take our ring to be a ED and we denote its Euclidean function by $\phi : R^\times \to \mathbb{Z}_{\geq 0}$. let A be an $m \times n$ matrix with entries in R.

Definition 16.1. The elementary row operations are as follows:
1. Add $\lambda \in R$ times the j^{th} row to the i^{th} row for $i \neq j$.
2. Swap the i^{th} and j^{th} row.
3. Multiply the i^{th} row by a unit u.

Note that all these operations are reversible. Also, each of the operations may be realized by multiplying in the left by an $m \times m$ invertible matrix. To wit, the first operation is the left multiplication of the matrix $I + \lambda E_{ij}$ where E_{ij} is the matrix with 1 on the (i, j) entry and 0 otherwise. The second is $I + E_{ij} + E_{ji} - E_{ii} - E_{jj}$ and the third is $I + (u - 1)E_{ii}$. We can similarly define the column operations, and the realization becomes the matrix multiplication on the right by an $n \times n$ invertible matrix analogous to before.

[1] I think we can prove the proposition without using AC (or equivalence)

Definition 16.2. Two $m \times n$ matrices A, B are equivalent if there is a sequence of elementary row and column operations taking A to B.

It is obvious that this is an equivalence relation due to reversibility. So if A, B are equivalent, there exists invertible square matrices P, Q with $B = QAP$.

Theorem 16.1 (Smith Normal Form)**.** *An $m \times n$ matrix $A = (a_{ij})$ with entries in R is equivalent to a diagonal matrix of the form*

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

where $d_i \neq 0$ for all i and $d_1 | d_2 | \cdots | d_t$.

The d_i's are called covariant factors and are unique up to associates (show later).

Proof. If $A = 0$ then we are done. So assume that $a_{11} \neq 0$. Suppose $a_{11} \nmid a_{1j}$ for some $j \geq 2$, then we use the Euclidean algorithm to get $a_{1j} = qa_{11} + r$ with $q, r \in R$ and $\phi(r) < \phi(a_{11})$. So we substract q times the first column from the j^{th} column and swap them. This makes the top left entry r. Likewise, we can do the same thing if $a_{11} \nmid a_{i1}$ for some $i \geq 2$ by row operations. The cases above each decrease the top left entry (in terms of its value in the Euclidean function), thus it must eventually stops, at which time a_{11} divides everything in the first row or the first column. Then substracting multiples of the first row or first column can clear up every other entry in the first column or first row except a_{11}. Now if a_{11} does not divide a_{ij} for $i, j \geq 2$, then add the i^{th} row to the first row, and so we can do the same column operations to decrease $\phi(a_{11})$ further till it terminates. Do this over and over again (but finitely many times) we can get $a_{11} | a_{ij}$ for any $i, j \geq 2$ and $a_{ij} = 0$ whenever $i \neq j$ and one of i, j is 1. We rename a_{11} as d_1 and repeat the process on the smaller matrix by removing the first row and first column to give the existence. □

Definition 16.3. A $k \times k$ minor of a matrix A is the determinant of a $k \times k$ submatrix of A.

Definition 16.4. For a matrix A over a ring R, we define the k^{th} Fitting ideal $\mathrm{Fit}_k(A)$ be the ideal generated by all the $k \times k$ minors of A.

Lemma 16.2. *If A, B are equivalent matrices, then $\mathrm{Fit}_k(A) = \mathrm{Fit}_k(B)$ for any k (such that the Fitting ideal makes sense).*

Proof. Suffices to show that the elementary operations do not change the Fitting ideal. The second and third row operations are trivial. For the first kind of row operation, suppose we add λ times the second row to the first row so that

$A = (a_{ij})$ becomes

$$A' = \begin{pmatrix} a_1 1 + \lambda a_{21} & a_{12} + \lambda a_{22} & \dots & a_{1n} + \lambda a_{2n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \end{pmatrix}$$

Let C be a $k \times k$ submatrix of A and C' be its correspondent submatrix in A'. If C does not intersect the first row, then $\det C = \det C'$. If C intersect both the first and second row, we also have $\det C = \det C'$ since its simply a row operation on the $k \times k$ submatrix. If C intersects the first but not the second row, then by expanding along the first row, the determinant of $\det C'$ would be $\det C + \lambda \det D$ for some other $k \times k$ submatrix of A. So $\det C' \in \mathrm{Fit}_k(A)$, so $\mathrm{Fit}_k(A') \subset \mathrm{Fit}_k(A)$. Since row operations are reversible, we also have the reverse inclusion. □

Proposition 16.3. *The covarient factors are unique up to associates.*

Proof. Look at the Fitting ideals. □

Example 16.1. Consider the following matrix (here $\to$ represents row/column operations)

$$A = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & -1 \\ 3 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 3 & 5 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}$$

One can also get its Smith normal form by considering the minors. Indeed, $\mathrm{Fit}_1(A) = (1)$, so $d_1 = \pm 1$. Also $\mathrm{Fit}_2(A) = (5)$, hence $d_2 = \pm 5$. So we obtain the Smith normal form.

Theorem 16.4. *Let R be an Euclidean domain and N is an R-submodule of R^n, then there is a free basis $x_1, \dots, x_m$ of R^m such that N is generated as an R-module by $d_1 x_1, \dots, d_t x_t$ for some $t \le m$ and $d_1 | d_2 | \cdots | d_t$.*

Proof. R is a ED hence a PID, hence N is generated by some $y_1, \dots, y_n$ for some $n \le m$. Now each y_i is in R^n, so we can form an $n \times n$ matrix A whose columns are the y_i's. By the preceding theorem, A is equivalent to $A' = \mathrm{diag}(d_1, \dots, d_t, 0, \dots, 0)$ with $t \le n$ and $d_1 | d_2 | \dots | d_t$. Now A' is obtained from A by elementary row and column operations. Each row operation corresponds to changing of our choice of free basis for R^n, and every column operation changes the generating set for R^n. So after changing the free basis for R^n to, say, $x_1, \dots, x_n$, N would be generated by $d_1 x_1, \dots, d_t x_t$. □

Theorem 16.5 (Structure Theorem)**.** *Let R be a Euclidean Domain and M a finitely-generated R-module, then $M \cong R/(d_1) \oplus \cdots \oplus R/(d_t) \oplus R \oplus \cdots \oplus R$ for some $d_i \in R$ and $d_1 | d_2 | \cdots | d_t$.*

These d_i's are called invariant factors.

Proof. Since M is finitely generated, then we can find a surjective R-module map $\phi : R^m \to M$ for some m. Then $M \cong R^m / \ker \phi$, but by the preceding theorem, there exists a free basis $x_1, \dots, x_n$ for R^m such that $N = \ker \phi = Rd_1 x_1 + \cdots Rd_t x_t$ for $d_1 | d_2 | \cdots | d_t$, hence

$$M \cong \frac{R \oplus R \oplus \cdots \oplus R \oplus R \oplus \cdots \oplus R}{Rd_1 \oplus Rd_2 \oplus \cdots \oplus Rd_t \oplus 0 \oplus \cdots \oplus 0} \cong R/(d_1) \oplus \cdots \oplus R/(d_t) \oplus R \oplus \cdots \oplus R$$

which is what we wanted. □

Definition 16.5. Let M be an R-module. An element $m \in M$ is called torsion if $\exists r \in R \setminus \{0\}, rm = 0$.
M is called a torsion module if every $m \in M$ is torsion. M is called torsion-free if the only torsion is 0.

Corollary 16.6. *Let R be an Euclidean domain, then any finitely generated torsion-free R-module is free.*

Proof. By the preceding theorem $M \cong R/(d_1) \oplus \cdots \oplus R/(d_t) \oplus R \oplus \cdots \oplus R$, but as M is torsion-free, it cannot contain any of $R/(d_i)$ as R-submodule as they would contain torsions. Hence $M \cong R \oplus \cdots \oplus R$, therefore M is free. □

Remark. The structure theorem in fact holds whenever R is a PID. Also, there is also a uniqueness statement in the structure theorem: Suppose no d_i's is a unit (otherwise they only contribute 0 factors to the product), then the module M uniquely determines $d_1, \ldots, d_t$.

Example 16.2. Consider an abelian groupn G generated by a, b subject to relations $2a + b = -a + 2b = 0$. So $G \cong \mathbb{Z}^2/N$ where N is generated by $(2, 1), (-1, 2)$, so we take (as in the proof of the structure theorem)

$$A = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}$$

as seen before. So we can change basis for $\mathbb{Z}^2$ to generate N by $(1, 0), (0, 5)$, hence $G \cong \mathbb{Z} \oplus \mathbb{Z}/(\mathbb{Z} \oplus 5\mathbb{Z}) \cong \mathbb{Z}/5\mathbb{Z}$.

More generally, for finitely generated abelian groups, we have the following:

Theorem 16.7. *Any finitely generated abelian group G is isomorphic to*

$$\mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_t\mathbb{Z} \oplus \mathbb{Z}^r$$

where $r \geq 0$ and $d_1 | d_2 | \cdots | d_t$.

The r here stands for the rank of the group.

Proof. Take $R = \mathbb{Z}$ in the structure theorem. □

In the special case that G is finite, we immediately obtain Theorem 6.4.

Remark. Let A, B be square matrices over R, then $\det(AB) = \det A \det B$, also $\operatorname{adj}(A)A = A \operatorname{adj}(A) = \det(A)I$. In particular, A is invertible iff $\det A$ is a unit.

Theorem 16.8 (Cayley-Hamilton)**.** *Let $A = (a_{ij})$ be a $n \times n$ matrix over a field F. Let $\chi_A(X) = \det(XI - A) \in F[X]$, then $\chi_A(A) = 0$.*

Proof. Consider $V = F^n$ as a $F[X]$-module with X acting as A, i.e. $f(X) \cdot v = f(A)v$. Let $e_1, \ldots, e_n$ be the standard basis for F^n, so for any j, $X \cdot e_j = \sum_{i=1}^n a_{ij} e_i$, hence

$$(XI - A) \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = 0$$

By multiplying both sides by the adjugate of $XI - A$, we know that for any i,

$$\chi_A(X) \cdot e_i = \det(XI - A) \cdot e_i = 0 \implies \chi_A(A)e_i = 0$$

But this can only happen when $\chi_A(A) = 0$. □

Recall that we have mentioned Theorem 6.1, which is yet another way of classifying the finite abelian groups by writing it as a product of cyclic p-groups. Indeed, we can achieve this by generalising our structure theorem one step further.

Lemma 16.9. *Let R be a PID and $a, b \in R$ has $\gcd(a, b) = 1$ (up to associates), then there is an isomorphism of R-modules*

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

Proof. Since R is a PID, $(a, b) = (d)$ for some $d \in R$, so $d = \gcd(a, b)$ by certain questions in example sheet. Hence $(a, b) = R$ since d must be a unit by hypothesis, so there is $r, s \in R$ with $ra + sb = 1$. Define an R-module homomorphism $\phi : R \to R/(a) \oplus R/(b)$ by $x \mapsto (x + (a), x + (b))$. To see it is surjective, $\phi(sb) = (1 + (a), 0 + (b)), \phi(ra) = (0 + (a), 1 + (b))$, hence $\phi(sbx+ray) = (x+(a), y+(b))$. Now if $\phi(x) = (0+(a), 0+(b))$, then $x \in (a)\cap(b)$, so $x = x(ra + sb) = rax + sxb \in (ab)$. It is obvious that anything in (ab) is mapped to zero, hence $\ker \phi = (ab)$, so we deduce the theorem from isomorphism theorem. □

This reduced to Chinese Remainder Theorem when we set $R = \mathbb{Z}$.

Theorem 16.10 (Prime Decomposition Theorem)**.** *Let R be a ED and let M be a finitely generated R-module. Then*

$$M \cong R/(p_1^{n_1}) \oplus \cdots \oplus R/(p_k^{n_k}) \oplus R^m$$

where $p_1, \ldots, p_k$ are prime in R.

Note that $p_1, \ldots, p_k$ need not to be distinct.

Proof. By the structure theorem, we have

$$M \cong R/(d_1) \oplus \cdots \oplus R/(d_t) \oplus R^m$$

So it suffices to write each $R/(d_i)$ in the desired form. Choose i and write $d_i = up_1^{\alpha_1} \cdots p_r^{\alpha_r}$ where p_i are pairwise non-associates and u is a unit. So by the preceding lemma, we have

$$R/(d_i) \cong R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_r^{\alpha_r})$$

which establishes the theorem. □

Note that Theorem 6.1 is a direct consequence of this.
Let V be a vector space over a field F and let $\alpha : V \to V$ be an endomorphism, then we can make V an $F[X]$-module (written as V_α) by $f(X) \cdot v = f(\alpha)v$.

Lemma 16.11. *If V is finite-dimensional, then V_α is finitely generated as an $F[X]$-module.*

Proof. If $v_1, \dots, v_n$ generates V as a vector space, then they also generate V_α as an $F[X]$-module since $F \leq F[X]$. □

The lemma itself is trivial, but the thing to take from here is that V_α, being also an F-vector space, is isomorphic to V. This is very useful if we want to analyze the behaviour of α in V: If we know that V_α is isomorphic to some $F[X]$-modules (via e.g. Theorem 16.10) that are easier to study, then they are also automatically isomorphic as F-vector spaces. So by choosing a nice basis for this $F[X]$-module (as a vector space), we can obtain a nice matrix of α.

Example 16.3. 1. Suppose $V_\alpha \cong F[X]/(X^n)$ as $F[X]$-module, then we can choose the basis $1, X, \dots, X^{n-1}$ for it to be an F-vector space in which the matrix of α would be

$$(\star) = \begin{pmatrix} 0 & & & \\ 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{pmatrix}$$

Since α acts as multiplication by X.
2. Suppose $V_\alpha \cong F[X]/(X-\lambda)^n$ as an $F[X]$-module, then wrt the basis $1, X - \lambda, \dots, (X-\lambda)^{n-1}$, $\alpha - \lambda \operatorname{id}$ has matrix $(\star)$, so α exists as a Jordan block.
3. Suppose $V_\alpha \cong F[X]/(f)$ where $f \in F[X]$ is in the form $f(X) = a_0 + a_1 X + \dots + a_{n-1}X^{n-1} + X^n$, then with respect to $1, X, \dots, X^{n-1}$, α has the matrix

$$C(f) = \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & -a_1 \\ & \ddots & 0 & \vdots \\ & & 1 & -a_{n-1} \end{pmatrix}$$

which is called the companion matrix of f.

Theorem 16.12 (Rational Canonical Form)**.** *Let $\alpha : V \to V$ be an endomorphism of a finite dimensional vector space V over a field F, then*

$$V_\alpha \cong F[X]/(f_1) \oplus \dots \oplus F[X]/(f_t)$$

where $f_i \in F[X]$ are monic and $f_1 | f_2 | \dots | f_t$. Moreover, with respect to a suitably chosen basis for V, α has matrix of the form

$$\begin{pmatrix} C(f_1) & & & \\ & C(f_2) & & \\ & & \ddots & \\ & & & C(f_t) \end{pmatrix}$$

Proof. V_α is finitely generated as an $F[X]$-module and since $F[X]$ is a ED, we can apply the structure theorem to get

$$V_\alpha \cong F[X]/(f_1) \oplus \dots \oplus F[X]/(f_t) \oplus F[X]^m$$

where $f_i \in F[X]$ are monic and $f_1 | f_2 | \dots | f_t$. $m = 0$ since V is finite dimensional over F. The result is immediate. □

Remark. 1. If we start by an $n \times n$ matrix of α, then this matrix must be similar to the above form.
2. The minimal polynomial of α is f_t.
3. The characteristic polynomial of α is $f_1 \cdots f_t$ (up to associates). Hence the minimal polynomial divides the characteristic polynomial, so we immediately have Cayley-Hamilton.

Example 16.4. When V is 2-dimensional vector space over F, then one of the following cases happen

$$V_\alpha \cong F[X]/(X-\lambda_1) \oplus F[X]/(X-\lambda_2), V_\alpha \cong F[X]/(f)$$

where $(X-\lambda_1)(X-\lambda_2)$ or f is the characteristic polynomial of α.

Corollary 16.13. *Let $A, B \in \mathrm{GL}_2(F)$ that are not scalar matrices, then A, B are conjugate iff they have the same characteristic polynomial.*

Proof. Immediate. □

Lemma 16.14. *Primes in $\mathbb{C}[X]$ are polynomials $X - \lambda$ where λ is any complex number (up to associates).*

Proof. FTA. □

Theorem 16.15 (Jordan Normal Form)**.** *Let $\alpha : V \to V$ be an endomorphism of a finite dimensional vector space over $\mathbb{C}$. Let V_α be V as the $\mathbb{C}[X]$-module with X acting as α. Then there is an isomorphism of $\mathbb{C}[X]$-modules*

$$V_\alpha \cong \mathbb{C}[X]/(X-\lambda_1)^{n_1} \oplus \cdots \oplus \mathbb{C}[X]/(X-\lambda_t)^{n_t}$$

where $\lambda_i \in \mathbb{C}$ are not necessarily distinct and $n_i \in \mathbb{N}$. In particular, there is a basis for V such that α has the matrix

$$\begin{pmatrix} J_{n_1}(\lambda_1) & & \\ & \ddots & \\ & & J_{n_t}(\lambda_t) \end{pmatrix}, J_n(\lambda) = \begin{pmatrix} \lambda & & & \\ 1 & \lambda & & \\ & \ddots & \ddots & \\ & & 1 & \lambda \end{pmatrix}$$

Proof. We know that $\mathbb{C}[X]$ is a ED and V_α is finitely generated as V is finite dimensional. By Prime Decomposition Theorem, noting that primes in $\mathbb{C}[X]$ are linear factors, and we cannot have any copy of $\mathbb{C}[X]$ as the dimension is finite. Then we already have the isomorphism. Now $J_n(\lambda)$ represents the multiplication by X on $\mathbb{C}[X]/(X-\lambda)^n$ wrt the basis $1, X-\lambda, \ldots, (X-\lambda)^{n-1}$. This shows the theorem. □

Remark. 1. The theorem implies that any matrix with entries in $\mathbb{C}$ is similar to a matrix in the said form.
2. The Jordan blocks are unique up to reordering.
3. The minimal polynomial of α is $\prod_i (X-\lambda_i)^{c_i}$ where c_i is the size of the largest block with eigenvalue λ_i.
4. The characteristic polynomial of α is $\prod_i (X-\lambda_i)^{a_i}$ where a_i is the sum of the sizes of the blocks with eigenvalue λ_i.
5. The eigenspace of λ_i has dimension equal to the number of blocks with eigenvalue λ.
6. The uniqueness statement may be proved by considering the dimension of the generalized eigenspaces $\ker((\alpha - \lambda_i I)^n)$, $n = 1, 2, \ldots$.

Theorem 16.16. *The structure theorem is true for any PIDs.*

We will not prove this in the course, but we will illustrate the trick that is used for this extension.

Theorem 16.17. *Let R be a PID, then any finitely generated torsion-free R-module is free.*

Note that for R a ED, this is a corollary of the structure theorem.

Lemma 16.18. *Let R be a PID and M an R-module. Let $r_1, r_2 \in R$ that are not both 0. Let $d = \gcd(r_1, r_2)$.*
1. There is a matrix $A \in \mathrm{SL}_2(R)$ such that

$$A \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$$

2. If $x_1, x_2 \in M$, then there is $x_1', x_2' \in M$ such that $Rx_1 + Rx_2 = Rx_1' + Rx_2'$ and $r_1x_1 + r_2x_2 = dx_1' + 0x_2'$.

Proof. We know that $(r_1, r_2) = (d)$, so there is $\alpha, \beta \in R$ such that $\alpha r_1 + \beta r_2 = d$. Write $r_1 = s_1 d, r_2 = s_2 d$ with $s_1, s_2 \in R$. We simply take the matrix

$$A = \begin{pmatrix} \alpha & \beta \\ -s_2 & s_1 \end{pmatrix} \in \mathrm{SL}_2(R)$$

and it works for the first part. For the second part, we can take $x_1' = s_1x_1 + s_2x_2, x_2' = -\beta x_1 + \alpha x_2$. □

Proof of Theorem 16.17. Say $M = Rx_1 + \cdots + Rx_n$ with n minimal. If $x_1, \ldots, x_n$ are independent, then the module is free. Otherwise, there is $r_1, \ldots, r_n \in R$ such that $r_1x_1 + \cdots + r_nx_n = 0$ where WLOG $r_1 \neq 0$. By the preceding lemma, we can choose x_1', x_2' such that $Rx_1 + Rx_2 = Rx_1' + Rx_2'$, so $M = Rx_1' + Rx_2' + Rx_3 + \cdots + Rx_n$ and $dx_1' + r_3x_3 + \cdots + r_nx_n = 0$ for $d = \gcd(r_1, r_2) \neq 0$. Continue the process to $3, \ldots, n$ to reduce the case to $rx_1 = 0$ for some $r \neq 0$, but R is torsion-free, so $x_1 = 0$, contradicting the minimality of n. □