Notes from Part III Catch-up Workshop: Rings and Modules

Stacey Law

Michaelmas 2016 swcl2

These notes are based on those of Nigel Burke who gave the same workshop in Michaelmas 2015, and material from the IB Groups, Rings and Modules course. Many of the exercises have been taken from these sources. Any mistakes are entirely the author's. If you have any comments or corrections, please email swcl2@cam.ac.uk.

PAGE

I Useful resources . . . 2
II Introduction . . . 3
1 Rings, subrings and polynomial rings . . . 3
2 Homomorphisms, ideals and quotients . . . 4
III Workshop . . . 7
1 Rings, subrings and polynomial rings . . . 7
2 Homomorphisms, ideals and quotients . . . 7
3 Integral domains and special ideals . . . 8
4 Zorn's Lemma . . . 10
5 Factorisation . . . 12
6 Modules and submodules . . . 15
7 Homomorphisms and quotient modules . . . 18
8 The structure theorem . . . 19

I Useful resources

Texts:

- P. M. Cohn, *Classic Algebra*. Wiley, 2000.
- **P. J. Cameron, *Introduction to Algebra*. OUP**
- J. B. Fraleigh, *A First Course in Abstract Algebra*. Addison Wesley, 2003. [Good for examples and motivation, not many proofs.]
- **B. Hartley, T. O. Hawkes, *Rings, Modules and Linear algebra: a further course in algebra*. Chapman and Hall, 1970.**
- I. Herstein, *Topics in Algebra*. John Wiley and Sons, 1975.
- P. M. Neumann, G. A. Stoy, E. C. Thomson, *Groups and Geometry*. OUP, 1994.
- M. Artin, *Algebra*. Prentice Hall, 1991.

There are also many sets of lecture notes on rings and modules which can be found online.

II Introduction

1 Rings, subrings and polynomial rings

Definition 1.1. *A* ring (commutative ring with 1) *is an abelian group* $(R, +)$ *with identity* 0_R *and an associative binary operation* $\cdot$ *satisfying the following axioms:*

- $x \cdot y = y \cdot x \ \forall \ x, y \in R$ (commutativity)
- $\exists \ 1_R \in R$ *s.t.* $1_R \cdot x = x = x \cdot 1_R \ \forall \ x \in R$ (identity)
- $x \cdot (y + z) = x \cdot y + x \cdot z \ \forall \ x, y, z \in R$ (distributivity)

Examples 1.2.
1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
2. $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$, the integers modulo n ($n \in \mathbb{Z}_{\geq 0}$)
3. The set of all functions from $\mathbb{R}$ to $\mathbb{R}$ with pointwise operations.
4. The trivial ring consisting of one element $0 = 1$.

Exercise 1. Are the Gaussian integers $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$ a ring (with usual $+$ and $\cdot$ in $\mathbb{C}$)?

Polynomial rings $R[X]$ for any ring R are very important examples of rings, especially when R is a field. $R[X]$ consists of *formal expressions* of the form

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n, \qquad \text{for some } n \in \mathbb{N},\ a_i \in R \ \forall i.$$

Each such f in $R[X]$ gives rise to an *induced function*

$$\overline{f} : R \to R \qquad r \mapsto f(r)$$

Warning: *f is not the same thing as $\overline{f}$!* Consider $f(X) = X^2 + X \in \mathbb{Z}_2[X]$. Then f is not the zero polynomial as $\deg(f) = 2$, but $\overline{f}$ is the zero function from $\mathbb{Z}_2$ to $\mathbb{Z}_2$.

In general, we may have polynomial rings in many variables, e.g. $R[X, Y] = (R[X])[Y]$, or $R[X_1, X_2, \dots]$.

Definition 1.3. *An element $x \in R$ is* invertible *or is a* unit *if $\exists \ y \in R$ such that $x \cdot y = 1_R$. A ring R is a* field *if every non-zero element is invertible (and R is non-trivial).*

Examples 1.4.
1. Units in $\mathbb{Z}[i]$: ± 1 and $\pm i$ only, so $\mathbb{Z}[i]$ is not a field.
2. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields.
3. $\mathbb{Z}_n$ is a field if and only if n is prime.

Exercise 2. Let R be a ring. Show that for all $x \in R$,

1. $x \cdot 0_R = 0_R$, and
2. $x \cdot (-1_R) = -x$, where $-x$ is the additive inverse of x (i.e. unique inverse of x in $(R, +)$).

Exercise 3. Characterise all rings R where $1_R = 0_R$.

Definition 1.5. *A* subring $S \subseteq R$ *of a ring* R *is a subgroup of* $(R, +)$ *containing* 1_R *such that* $x \cdot y \in S \ \forall \ x, y \in S$.

Examples 1.6. 1. $\mathbb{Q}$ contains $\mathbb{Z}$ as a subring. In fact, any subring of $\mathbb{Q}$ contains $\mathbb{Z}$, since 1 generates the cyclic group $(\mathbb{Z}, +)$.

2. The intersection of subrings is again a subring.

Definition 1.7. *For any subset* X *of* R*, the* subring of R generated by X *is the smallest subring* $S \subseteq R$ *containing* X*:*

$$S = \bigcap_{\substack{T \text{ subring of } R \\ T \supseteq X}} T.$$

If $S = R$*, we say* X generates R.

Definition 1.8. *If* R *and* S *are rings, then the* ring direct sum $R \oplus S$ *is the ring on the set* $R \times S$ *with operations*

$$(x, y) + (x', y') := (x + x', y + y'), \qquad (x, y) \cdot (x', y') := (xx', yy') \qquad \forall \ x, x' \in R, \ y, y' \in S.$$

Have $0 = (0_R, 0_S)$ *and* $1 = (1_R, 1_S)$.

Warning: if R and S are non-trivial rings, then $R \oplus S$ is never a field (even if R and/or S is a field!), e.g. $(1_R, 0_S)$ is not a unit.

2 Homomorphisms, ideals and quotients

Definition 2.1. *For rings* R *and* S*, a* ring homomorphism $\varphi : R \to S$ *is a map that preserves the ring structure, i.e.*

- φ *is a group homomorphism* (preserves $+$)
- $\varphi(1_R) = 1_S$ (respects the identity)
- $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) \ \forall \ x, y \in R$ (preserves $\cdot$)

If φ *is bijective, we say* φ *is a* ring isomorphism, R *and* S *are* isomorphic*, and write* $R \cong S$.

Remark 2.2. 1. The image $\varphi(R)$ is a subring of S.

2. Any ring hom $\varphi : R \to S$ lifts naturally to a ring hom $\tilde{\varphi} : R[X] \to S[X]$ that only acts on the coefficients.

Example 2.3. 1. For any rings R and S, the zero map $\varphi : R \to S$, $r \mapsto 0$ for all $r \in R$.

2. Evaluation maps: for $r \in R$, the map $\varphi : R[X] \to R,\ f(X) \mapsto f(r)$ is a ring hom.

Definition 2.4. *A subset I of a ring R is an* ideal *if it is a subgroup of $(R, +)$ and $x \cdot r \in I\ \forall\ x \in I$ and $r \in R$.*

Remark 2.5. So clearly, $1_R \in I$ if and only if $I = R$.

Example 2.6. 1. In $\mathbb{Z}$, $n\mathbb{Z} := \{nx \mid x \in \mathbb{Z}\}$ is an ideal.

2. The union of two ideals is not necessarily an ideal: e.g. $2\mathbb{Z}$ and $3\mathbb{Z}$ are ideals in $\mathbb{Z}$. Their union $2\mathbb{Z} \cup 3\mathbb{Z}$ contains both 3 and 2 but not their difference $3 - 2 = 1$ (taking their union fails to make a subgroup).

Exercise 4. Let $\{J_\lambda \mid \lambda \in \Lambda\}$ be some collection of ideals of a ring R, where Λ is an arbitrary indexing set. Suppose further that given any two ideals J_λ and $J_{\lambda'}$, *either* $J_\lambda \subseteq J_{\lambda'}$ or $J_{\lambda'} \subseteq J_\lambda$ (so this is a family of *nested* ideals: we can *totally order* the ideals by inclusion). Show that the union of nested ideals $J := \bigcup_{\lambda \in \Lambda} J_\lambda$ *is* an ideal of R. [In contrast to Example 2.6 (2)!]

Exercise 5. Show that the kernel of any ring homomorphism is an ideal.

Definition 2.7. *For an ideal I of a ring R, the quotient group $R/I = \{x + I \mid x \in R\}$ can be made into a ring via $(x + I) \cdot (y + I) := xy + I$. This gives the quotient ring R/I.*

Exercise 6. Check that the multiplication in R/I is well-defined, i.e. if $x + I = x' + I$ and $y + I = y' + I$ then $xy + I = x'y' + I$.

Exercise 7. 1. What ideals of a ring R are also subrings?

2. What ring homs have kernels that are subrings?

3. What are the ideals in a field k?

4. If I and J are ideals of a ring R, show the following are also ideals of R:

   (a) $I + J = \{i + j \mid i \in I,\ j \in J\}$

   (b) $IJ = \{\sum_{m=1}^{n} i_m j_m \mid i_m \in I,\ j_m \in J,\ n \in \mathbb{N}\}$

   (c) $I \cap J$

Show further that $IJ \subseteq I \cap J$.

Moral: even though kernels of group homs are subgroups, kernels of ring homs are usually not subrings.

Remark 2.8.
1. Every ring R has at least two ideals, namely R itself and $\{0_R\}$.
2. Like for groups, a ring hom $\varphi : R \to S$ is injective if and only if $\ker \varphi = \{0_R\}$.

Definition 2.9. *An ideal I in a ring R is* principal *if it is of the form $I = (x) = Rx = \{rx \mid r \in R\}$ for some $x \in R$. This is the ideal* generated by x*, and is the smallest ideal of R containing x.*

In general, we say an ideal I is finitely generated *if there exists a finite subset $\{x_1, \ldots, x_n\}$ of R such that $I = (x_1, \ldots, x_n) = \{r_1x_1 + \cdots + r_nx_n \mid r_i \in R\}$.*

Exercise 8.
1. Show that every ideal in $\mathbb{Z}$ is principal.
2. Let k be a field. Show that every ideal in $k[X]$ is principal.

Definition 2.10. *A ring R is* Noetherian *if every ideal of R is finitely generated.*

R is Noetherian if and only if it has the *ascending chain condition (ACC)*: if whenever $I_1 \subseteq I_2 \subseteq \cdots$ are ideals of R, then $I_n = I_{n+1} = \cdots$ for some $n \in \mathbb{N}$.

III Workshop

1 Rings, subrings and polynomial rings

For the purposes of most (undergraduate) Cambridge courses, a *ring* will mean a *commutative ring with 1*. You will see some non-commutative rings in Part III courses like the Lent term course 'Algebras' to be given by Dr Brookes, but any relevant concepts in the non-commutative setting will be introduced then.

Intuitively, a ring is a set with both plus and times. (In general, we want to exclude the trivial ring since it does not have interesting structure.) Here is one more example:

Example 1.1. Let S be any set. Then the power set $\mathcal{P}(S)$ is a ring with operations $A + B := A \triangle B$ (symmetric difference) and $A \cdot B := A \cap B$ (intersection). The 0 of this ring is $\emptyset$, while the 1 of this ring is S.

Just as groups have subgroups, rings also have substructures called subrings. A subset of R is a *subring* if it is itself a ring and contains 1_R.

Examples 1.2.

1. $\mathbb{Z}$ has no *proper* subrings, since the element 1 generates all of $\mathbb{Z}$.
2. The dyadic rationals $\{\frac{a}{2^b} \mid a \in \mathbb{Z},\ b \in \mathbb{Z}_{\geq 0}\}$ form a subring of $\mathbb{Q}$. Here, only powers of 2 have multiplicative inverses. This can be generalised by choosing some set of primes and their products to have multiplicative inverses, not just the prime 2. This construction describes all subrings of $\mathbb{Q}$ and is an example of the much more general idea of *localisation*, a useful tool in commutative algebra.
3. Let R be a ring and let S_1 and S_2 be subrings of R. Must the union $S_1 \cup S_2$ be a subring or R? No, e.g. $R = \mathbb{Q}$, $S_1 = \{\frac{a}{2^b} \mid a \in \mathbb{Z},\ b \in \mathbb{Z}_{\geq 0}\}$, $S_2 = \{\frac{a}{3^b} \mid a \in \mathbb{Z},\ b \in \mathbb{Z}_{\geq 0}\}$. Then $\frac{1}{2} + \frac{1}{3} \notin S_1 \cup S_2$ (the union fails to be a subgroup). S_1 and S_2 generate the subring $\{\frac{a}{2^b 3^c} \mid a \in \mathbb{Z},\ b, c \in \mathbb{Z}_{\geq 0}\}$.

2 Homomorphisms, ideals and quotients

Like a group homomorphism preserves group structure, a ring homomorphism preserves ring structure, namely the plus, times, and the multiplicative identity.

In group theory, normal subgroups arise precisely as kernels of group homomorphisms. There is an analogue in ring theory: ideals are precisely the kernels of ring homomorphisms.

In the introductory exercises, you checked that quotient rings R/I are well-defined, and showed that kernels are always ideals. So for the converse, we need to realise any given ideal I as a kernel of some ring homomorphism. This can be done via the *canonical projection map* $\pi : R \to R/I,\ r \to r + I$.

Like for groups, we have a first isomorphism theorem for rings: if $\varphi : R \to S$ is a ring homomorphism, then $R/\ker\varphi \cong \text{Image}(\varphi)$ *as rings*. You can check that the well-defined group isomorphism $r + \ker\varphi \mapsto \varphi(r)$ is in fact a ring isomorphism, since it preserves the times and the 1.

Example 2.1 (Homomorphisms). 1. Consider the 'evaluation at i' homomorphism $\varphi : \mathbb{Z}[X] \to \mathbb{C},\ f \mapsto \overline{f}(i)$. The image is $\mathbb{Z}[i]$, and the kernel is $(1 + X^2)$. Hence $\mathbb{Z}[X]/(1 + X^2) \cong \mathbb{Z}[i]$.

2. For any ring R, there is a unique ring homomorphism $\varphi : \mathbb{Z} \to R$, since $\varphi(1)$ must equal 1_R. This determines the *characteristic* $\mathrm{char}(R)$ of R, which is the smallest positive integer such that $\varphi(n) = 0_R$ if such an n exists, and 0 otherwise. So e.g. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ all have characteristic 0, while $\mathrm{char}(\mathbb{Z}_n) = n$.

Example 2.2 (Ideals). 1. In $\mathbb{Z}[X]$, the ideal $(2, X) = \{\text{polys with even constant term}\}$ is *not* principal. If $(2, X) = (f)$, then X is a multiple of f, so $f = \pm X$ or ± 1. But 2 is also a multiple of f, so $f = \pm 1$ or ± 2. But then $f = \pm 1 \notin (2, X)$, a contradiction.

   Similarly, the ideal (X, Y) in $\mathbb{Q}[X, Y]$ is not principal.

2. In the exercises you showed that $IJ := \{\sum i_m j_m\}$ is an ideal, for any ideals I and J. Why do we need to take the sum? This is because $S := \{ij \mid i \in I,\ j \in J\}$ is not necessarily an ideal. Example: $R = \mathbb{Z}[X]$, $I = (2, X)$, $J = (3, X)$. Then $2 \cdot X, X \cdot 3 \in S$, so if S is an ideal then their difference X must lie in S because ideals are closed under $+$. But X cannot be written as ij for some $i \in I, j \in J$ by considering degree. [In fact, any such example must have neither I nor J being a principal ideal.]

3. In $\mathcal{P}(\mathbb{N})$, the ideal $I = \{A \subset \mathbb{N} \mid A \text{ is finite}\}$ is not finitely generated. If $I = (A_1, \ldots, A_n)$, then for all $A \in I$, we have $A \subseteq A_1 \cup A_2 \cup \cdots \cup A_n$. But $A_1 \cup \cdots \cup A_n \neq \mathbb{N}$, so there exists a finite set $A \not\subset A_1 \cup \cdots \cup A_n$, contradiction.

Remark 2.3. On the topic of finite generation, an important concept is that of Noetherian rings. A ring R is *Noetherian* if every ideal of R is finitely generated. We've just seen that $\mathcal{P}(\mathbb{N})$ is not Noetherian, while by Exercise 8, $\mathbb{Z}$ and $k[X]$ (k any field) are.

A key result that you should know in relation to Noetherian rings is *Hilbert's Basis Theorem:* R Noetherian $\implies$ $R[X]$ Noetherian.

Hence rings like $\mathbb{Z}[X, Y]$ and $\mathbb{C}[X_1, X_2, \ldots, X_n]$ are also Noetherian. If you are familiar with varieties from algebraic geometry, one often looks at vanishing sets of polynomials.

Take polynomials $\{f_i \in \mathbb{C}[X_1, \ldots, X_n] \mid i \in S\}$ where S is some arbitrary indexing set. Let $V := \{p \in \mathbb{C}^n \mid f_i(p) = 0\ \forall\ i \in S\}$. Then $I(V) := \{$ all polys in $\mathbb{C}[X_1, \ldots, x_n]$ which vanish on all points of $V\}$ is an ideal, and it contains all of the f_i.

So $I(V)$ could potentially be large if S is large (e.g. uncountable), but in fact, $\mathbb{C}[X_1, \ldots, X_n]$ being Noetherian means that $I(V)$ has a *finite* generating set.

3 Integral domains and special ideals

Definition 3.1. *A (non-trivial) ring R is an* integral domain *if $ab = 0 \implies a = 0$ or $b = 0$.*

In other words, 'R has no zero-divisors'; a *zero-divisor* is a non-zero element x s.t. $\exists\ y \neq 0,\ xy = 0$. In an integral domain, we have 'cancellation': if $a \neq 0$ and $ab = ac$, then $b = c$ because $a(b - c) = 0$.

Example 3.2. 1. $\mathbb{Z}$, $\mathbb{Z}[X]$, any field k are integral domains.

2. $\mathbb{Z}_n$ is an integral domain if and only if n is prime, e.g. $2 \cdot 3 = 0$ in $\mathbb{Z}_6$.

Remark 3.3. 1. Let R be an integral domain and let $f, g \in R[X]$. Then $\deg(fg) = \deg(f) + \deg(g)$: degrees add as you expect because leading terms don't cancel. But in $\mathbb{Z}_6[X]$ for example, $2X \cdot 3X = 0$ does not have degree 2.

2. A homomorphic image of an integral domain need not be an integral domain, e.g. $\mathbb{Z} \to \mathbb{Z}/(6) \cong \mathbb{Z}_6$, $n \mapsto n \pmod 6$.

A useful result:

Proposition 3.4. *Every finite integral domain R is a field.*

Proof. Given any $0 \neq x \in R$, we seek an inverse: $y \in R$ such that $xy = 1$. Consider $f : R \to R$, $y \mapsto xy$. Then f is injective because R is an integral domain ($xy = xz \implies y = z$), so f is surjective as R is finite. In particular, $\exists\ y \in R$ such that $f(y) = 1$. □

Given a ring R, we can extend it and make it into a field by adding in multiplicative inverses for every non-zero element. We can't do this for any old ring though: R needs to be an integral domain in the first place, because fields cannot have zero-divisors.

To get $\mathbb{Q}$ from $\mathbb{Z}$ for example, we take all expressions a/b ($a \in \mathbb{Z}$, $0 \neq b \in \mathbb{Z}$, up to equivalence relation $a/b = c/d$ iff $ad = bc$ etc.) and this contains a copy of $\mathbb{Z}$ via $n \mapsto n/1$. We can do the same for any integral domain R, constructing the *field of fractions of R,* Frac(R). The field of fractions of a field k is canonically isomorphic to k itself.

Another way to make fields from rings is to quotient out by special ideals. Coming back to a general ring R, not necessarily an integral domain:

Definition 3.5. *A proper ideal I in a ring R is* maximal *if $I \subseteq J \subseteq R \implies I = J$ or $J = R$, i.e. no other ideal J can be 'strictly sandwiched in between'.*

Example 3.6. 1. In $\mathbb{Z}$, what are the maximal ideals? ((n) is maximal iff n is prime.)

2. In $\mathbb{Z}[X]$, is (X) maximal? (No, e.g. $(X) \subsetneqq (2, X) \subsetneqq \mathbb{Z}[X]$.)

3. In $\mathbb{Z}[X]$, $(2, X)$ is maximal. Suppose $(2, X) \subsetneqq J$ and choose some $f \in J \setminus (2, X)$. Then f has odd constant term. But then $f - 1 \in (2, X) \subset J$ since it has even constant term, hence $1 \in J$ so $J = R$.

4. If k is an algebraically closed field (e.g. $k = \mathbb{C}$), then the maximal ideals of $k[X_1, \ldots, X_n]$ are precisely $(X_1 - a_1, \ldots, X_n - a_n)$ for some $a_i \in k$. This is usually known as the *weak Nullstellensatz* (or a corollary thereof). You'll come across Hilbert's Nullstellensatz again if you do algebraic geometry or commutative algebra courses.

We'll see later that every proper ideal is contained in some maximal ideal, using Zorn's Lemma. (You may already be familiar with Zorn if you've taken a logic and set theory course before.) But

first, one way to identify maximal ideals is the following result:

Proposition 3.7. *Let I be a proper ideal of a ring R. Then I is maximal $\Leftrightarrow$ R/I is a field.*

The proof is straightforward from definitions.

Remark 3.8. We can explicitly construct a field of size 27. Consider $\mathbb{Z}_3[X]/(X^3-X+1)$. Elements are of the form $a+bX+cX^2+(X^3-X+1)$ for $a,b,c \in \mathbb{Z}_3$, so there are 27 elements in this quotient ring. We claim (X^3-X+1) is a maximal ideal of $\mathbb{Z}_3[X]$, whence this ring is in fact a field.

So suppose not, i.e. that $(X^3-X+1) \subsetneqq (f) \subsetneqq \mathbb{Z}_3[X]$ for some polynomial f (all ideals in $\mathbb{Z}_3[X]$ are principal since $\mathbb{Z}_3$ is a field). f cannot be a constant as $(f) \neq \mathbb{Z}_3[X]$, and f cannot be cubic as $(f) \neq (X^3-X+1)$, so f has degree 1 or 2. Then X^3-X+1 is a multiple of f so X^3-X+1 factors as a linear $\times$ quadratic. But this is a contradiction as X^3-X+1 has no roots in $\mathbb{Z}_3$.

Definition 3.9. *A proper ideal I in a ring R is* prime *if $ab \in I \implies a \in I$ or $b \in I$ (for $a,b \in R$).*

Example 3.10.
1. In $\mathbb{Z}$, (n) is a prime ideal if and only if n is a prime (in the usual sense).
2. In $\mathbb{Z}[X]$, (X) is prime.
3. 0 is a prime ideal of R if and only if R is an integral domain. 0 is a maximal ideal of R if and only if R is a field.

Similarly to maximal ideals, we can relate primeness to a property of R/I. Again, the proof is straightforward from the definitions.

Proposition 3.11. *Let I be a proper ideal of a ring R. Then I is prime $\Leftrightarrow$ R/I is an integral domain.*

Corollary 3.12. *Let I be an ideal in a ring R. Then I maximal $\implies$ I prime, since R/I field $\implies$ R/I integral domain.*

Exercise 9. In $\mathbb{Z}[X]$, let $p \in \mathbb{Z}$ be a prime and consider the ideals (p), (X) and (p,X).
1. Check these are all prime ideals of $\mathbb{Z}[X]$. Are any maximal?
2. What about the same ideals in $\mathbb{Q}[X]$: which are still prime? Which are maximal?

Exercise 10. Show that if every ideal of an integral domain R is principal, then every non-zero prime ideal is maximal.

4 Zorn's Lemma

Zorn's Lemma is a very useful tool for constructing prime or maximal ideals of a ring that have a certain property. It is equivalent to the axiom of choice, but that shouldn't put you off using it in

algebra courses.

Lemma 4.1 (Zorn's Lemma)**.** *Let $\mathcal{P}$ be a non-empty poset. If every chain of $\mathcal{P}$ has an upper bound in $\mathcal{P}$, then $\mathcal{P}$ has a maximal element.*

Unpacking the terminology:

- A partially ordered set (poset) $(\mathcal{P}, \leq)$ is a set $\mathcal{P}$ with an order relation $\leq$ (i.e. reflexive, antisymmetric and transitive), where some pairs of elements may be *incomparable* (hence the name partial).
- A *chain* is a subset S of $\mathcal{P}$ where every pair *is* comparable, i.e. this subset is *totally ordered* under $\leq$.
- An *upper bound* of a subset S is an element $x \in \mathcal{P}$ such that $s \leq x$ for all $s \in S$. [So x is comparable to (and bigger than) every element of S. Note that x doesn't need to belong to S itself (but must live inside $\mathcal{P}$).]
- Finally, a *maximal element of $\mathcal{P}$* is an element $m \in \mathcal{P}$ such that $m \leq x \implies m = x$. [So any $x \in \mathcal{P}$ either satisfies $x \leq m$ or is incomparable to m. Hence m is *not* necessarily an upper bound of the whole poset $\mathcal{P}$.]

An application:

Corollary 4.2. *Let I be a proper ideal of a ring R. Then there exists a maximal ideal of R containing I.*

Proof. Let $\mathcal{P}$ be the set of all proper ideals of R containing I. $\mathcal{P} \neq \emptyset$ as $I \in \mathcal{P}$. Partially order $\mathcal{P}$ by inclusion.

Let $\{J_\lambda\}_{\lambda \in \Lambda}$ be a chain in $\mathcal{P}$. The union $J = \bigcup_{\lambda \in \Lambda} J_\lambda$ lies in $\mathcal{P}$ and is an upper bound for the chain.

By Zorn, we have some maximal element M of $\mathcal{P}$, so M contains I. It remains to show that M is a maximal ideal. Suppose $M \leq M' \lneq R$. Then $M' \in \mathcal{P}$, so $M = M'$ by maximality of M. □

Let's motivate the steps of the above proof:

- In order to use Zorn, we want a poset $\mathcal{P}$ describing ideals with the property that we're interested in, namely 'containing I'. So let $\mathcal{P}$ be the set of all proper ideals of R containing I. We need $\mathcal{P}$ to be non-empty, which is satisfied because I itself lies in $\mathcal{P}$. Partially order $\mathcal{P}$ by inclusion.
- Next, we must show that all chains in $\mathcal{P}$ have an upper bound in $\mathcal{P}$. So take an arbitrary chain of ideals $\{J_\lambda\}_{\lambda \in \Lambda}$. Under the inclusion ordering, something that's bigger than all of the J_λ is clearly the union of the J_λ, which I've called J. We just need to check that J is an element of $\mathcal{P}$. J clearly contains I since each of the J_λ do. J is an ideal from Exercise 4: a union of **nested** ideals is again an ideal. And J is indeed proper because if it contained the element 1, so would one of the J_λ, but they are all themselves proper.
- So by Zorn, we have some maximal element M of our poset $\mathcal{P}$. Clearly M is a proper ideal containing I, so it remains to show that M is a maximal ideal of our ring. So suppose M is

contained inside M' and M' is not all of R. Then M' contains I, so M' belongs to $\mathcal{P}$. But M was a maximal element in $\mathcal{P}$, so $M = M'$, hence M is a maximal ideal as required.

In applications to rings, ideals and modules, the partial order you want to take is almost always going to be ordering by inclusion, and the upper bound is almost always the union construction.

Remark 4.3. The existence of ideals maximal with respect to missing a multiplicatively closed set is an important fact in commutative ring theory, because such ideals turn out to be prime. I ask you to prove this in Exercise 11.

This again relates to the concept of *localisation*. Often one takes a prime ideal P and sets $S = R \setminus P$. 'Throw in' multiplicative inverses for elements of S to get a new ring, denoted $S^{-1}R$ or R_P, where elements of S are now invertible (they may have already been invertible in R originally). This process is called *localising at the prime ideal* P.

Localisation is a useful tool because R_P is a *local* ring, i.e. it has a unique maximal ideal. (In fact, the maximal ideal is the set of those elements of the form $\frac{p}{s}$ with $p \in P$, $s \in S$). The construction allows us to control certain properties and structure of R_P so that we may deduce useful things about the original ring.

Exercise 11.

1. Let S be a (multiplicatively closed) subset of a ring R such that $0 \notin S$. Show that there is an ideal P maximal with respect to the condition $P \cap S = \emptyset$.
2. Show further that any such ideal is a prime ideal of R.
3. Show that the intersection of all prime ideals in a ring R is the set of nilpotent elements in R. (Recall $r \in R$ is *nilpotent* if there exists $n \geq 1$ such that $r^n = 0$.)

   [Show any nilpotent element lies in every prime ideal. For the converse, show that any non-nilpotent element does not lie in some prime ideal (this is the contrapositive). Hint: $S = \{r^n : n \geq 1\}$ is a multiplicatively closed set, for any element $r \in R$.]

5 Factorisation

The idea of this section is the following picture:

$$\text{rings} \supset \underbrace{\text{integral domains}}_{\text{have cancellation}} \supset \underbrace{\overbrace{\text{UFDs}}^{\text{Gauss' Lemma } \exists \mathbb{Z}[X]}}_{\text{can factorise into products of irreducibles}} \supset \underbrace{\text{PIDs}}_{\text{all ideals principal}} \supset \underbrace{\text{EDs}}_{\text{have division algorithm}} \supset \text{fields}$$

In an integral domain, thanks to cancellation, we can talk about *factorising* elements. In $\mathbb{Z}$, any integer can be expressed uniquely (up to reordering) as a product of primes and possibly -1, which is a unit. The equivalent 'atomic' elements in an integral domain which cannot be factored further in a non-trivial way are called *irreducible*.

An integral domain where we can factorise every non-zero, non-unit element into a product of irreducibles, and where this factorisation is unique up to reordering and maybe multiplying those irreducibles by units, is called a *unique factorisation domain (UFD)*. We'll later show that $\mathbb{Z}[X]$ is a UFD using Gauss' Lemma, which lets us factorise polynomials in $\mathbb{Z}[X]$ by factorising them in $\mathbb{Q}[X]$.

We still have the notion of a *prime* element in an integral domain, which is slightly different to that of an irreducible, but the two properties coincide in $\mathbb{Z}$. $\mathbb{Z}$ is an example of a *principal ideal domain (PID)*. The name says it all: a PID is an integral domain in which every ideal is principal, and you should have proved in Exercise 8 that $\mathbb{Z}$ and $k[X]$ for any field k are PIDs.

As the picture suggests, every PID is a UFD. Nicer still, we have what is called a *Euclidean domain (ED)*, and every ED is a PID. The distinguishing feature of an ED is a *Euclidean function* which essentially gives us a division algorithm (more on that shortly).

We will not prove these inclusions; they are in lecture notes for the Part IB Rings and Modules course or easily found online. The technical definitions are as follows:

Definition 5.1. *Let R be an integral domain.*

- *A non-zero, non-unit element $r \in R$ is* irreducible *if $r = xy \implies x$ or y is a unit.*
- *A non-zero, non-unit element $r \in R$ is* prime *if $r|ab \implies r|a$ or $r|b$. (Notation: we say $r|a$ if $\exists\ c \in R$ such that $a = cr$.)*
- *Elements $s, t \in R$ are* associates *if $s = ut$ for some unit u. Equivalently, $s|t$ and $t|s$, or $(s) = (t)$.*

Remark 5.2.

1. r prime $\Leftrightarrow (r)$ prime:

$$\underbrace{ab \in (r)}_{r|ab} \implies \underbrace{a \in (r)}_{r|a} \text{ or } \underbrace{b \in (r)}_{r|b}$$

   and r is a non-unit $\Leftrightarrow (r)$ is proper.

2. r prime $\implies r$ irreducible. Straightforward from definitions.

3. The converse is false: e.g. in $\mathbb{Z}[\sqrt{-3}]$, 2 is irreducible but not prime.

   Why is 2 irreducible? Suppose $2 = ab$ where a and b are non-units. [In general, looking at norms is very useful when dealing with subrings of $\mathbb{C}$!] Then $4 = N(2) = N(a)N(b)$, where $N(z) = |z|^2$ is the norm squared function on $\mathbb{C}$. But $N(a)$ and $N(b)$ are integers, since $N(x+y\sqrt{-3}) = x^2+3y^2$ $(x, y \in \mathbb{Z})$. From this it's also clear that the only units in $\mathbb{Z}[\sqrt{-3}]$ are ± 1. So a, b non-units implies $N(a) = N(b) = 2$, which is impossible. Hence 2 is irreducible.

   Similarly, $1 \pm \sqrt{-3}$ also have norm 4 and so are irreducibles in $\mathbb{Z}[\sqrt{-3}]$. From this we can see that 2 is not a prime element: $2|(1 + \sqrt{-3})(1 - \sqrt{-3})$ but $2 \nmid 1 \pm \sqrt{-3}$.

Definition 5.3. *An integral domain R is a* unique factorisation domain (UFD) *if it satisfies*

(UFD1) Every non-zero, non-unit element $r \in R$ can be written as a product of irreducibles; and

(UFD2) This is unique up to reordering and multiplying by units, i.e. if $r = p_1 \cdots p_m = q_1 \cdots q_n$ for irreducibles p_i, q_j, then $m = n$ and after possibly reordering, p_i and q_i are associates for all i.

Equivalently, R is a UFD if it satisfies (UFD1) and (UFD2'):

(UFD2') All irreducibles are primes.

Definition 5.4. *An integral domain R is a* principal ideal domain (PID) *if every ideal of R is principal.*

Definition 5.5. *An integral domain R is a* Euclidean domain (ED) *if there exists a function $\phi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that*

- *$\phi(a) \leq \phi(b)$ if $a|b$, and*
- *$\forall\ a \in R,\ 0 \neq b \in R$, we can write $a = qb + r$ for some $q, r \in R$ with $\phi(r) < \phi(b)$ or $r = 0$.*

We say ϕ is a Euclidean function *on R.*

Example 5.6.

1. EDs: $\mathbb{Z}$ with $\phi(n) = |n|$ and $k[X]$ with $\phi(f) = \deg(f)$.
2. You can check that the squared norm function $\phi(z) = N(z) = |z|^2$ makes $\mathbb{Z}[i]$ a Euclidean domain, but that this function doesn't work for $\mathbb{Z}[\sqrt{-3}]$. But is there some other 'exotic' function ϕ that is a Euclidean function for $\mathbb{Z}[\sqrt{-3}]$? No: $2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ are different factorisations of 4, so $\mathbb{Z}[\sqrt{-3}]$ is not even a unique factorisation domain, let alone Euclidean domain.
3. Examples of PIDs but not EDs are hard, but exist in the literature.
4. $\mathbb{Z}[X]$ is an important example of a UFD that is not a PID. We've already seen that $(2, X)$ is not principal. To show that $\mathbb{Z}[X]$ is a UFD, we use the fact that $\mathbb{Z}$ is a UFD + Gauss' Lemma:

   Lemma 5.7 (Gauss' Lemma). *Let $f \in \mathbb{Z}[X]$ be such that the highest common factor of the coefficients of f is 1 (i.e. no non-unit divides all of its coefficients). Then f is irreducible in $\mathbb{Z}[X]$ if and only if f is irreducible in $\mathbb{Q}[X]$.*

   Why do we need the HCF condition? For example, $7(X^2 + X + 1)$ is irreducible in $\mathbb{Q}[X]$ (no linear factors), but clearly reducible in $\mathbb{Z}[X]$ as $7 \cdot (X^2 + X + 1)$. This is because 7 is a unit in $\mathbb{Q}[X]$, but not in $\mathbb{Z}[X]$.

   Now $\mathbb{Q}[X]$ is a Euclidean domain, hence a UFD. So as long as factorisations exist in $\mathbb{Z}[X]$, their uniqueness follows from the uniqueness of factorisations in $\mathbb{Q}[X]$.

   More generally, there is a version of Gauss' Lemma for any UFD R and its field of fractions $\mathrm{Frac}(R)$, not just $\mathbb{Z}$ and $\mathbb{Q}$. So in general, R is a UFD $\implies$ $R[X]$ is a UFD.
5. Finally, we've already seen an example of an integral domain that is not a UFD: $\mathbb{Z}[\sqrt{-3}]$. (It is an integral domain since it is a subring of $\mathbb{C}$.)

Exercise 12. Determine whether or not the following rings are fields, PIDs, UFDs, integral domains:

1. $\mathbb{Z}_{17}[X]$
2. $\mathbb{Z}_{18}[X]$
3. $\mathbb{Z}[X]/(X^2+1)$
4. $\mathbb{Z}_2[X]/(X^2+1)$
5. $\mathbb{Z}_2[X]/(X^2+X+1)$
6. $\mathbb{Z}_3[X]/(X^2+X+1)$

6 Modules and submodules

A module is like a vector space, but over a ring R rather than a field. For intuition, you should often consider the cases $R =$ field and also $R = \mathbb{Z}$.

Definition 6.1. *A* module *over a ring R is a set M together with operations $+ : M \times M \to M$ and $\cdot : R \times M \to M$ such that*

- *$(M, +)$ is an abelian group (with identity 0_M say)*
- *$r(x+y) = rx + ry \ \forall \ r \in R, x, y \in M$*
- *$(r+s)x = rx + sx \ \forall \ r, s \in R, x \in M$*
- *$(rs)x = r(sx) \ \forall \ r, s \in R, x \in M$*
- *$1_R x = x \ \forall \ x \in M$*

These are really the same axioms for a vector space, except instead of having the set of scalars lie in a field, they lie in a ring R. In the following examples, M is always an R-module.

Example 6.2.

1. R field, M: a vector space over R
2. R any ring, $M = R^n$, the set of n-tuples with entries in R. Addition is done coordinate-wise, and multiplication is given by $r \cdot (x_1, \ldots, x_n) = (rx_1, \ldots, rx_n)$.
3. $\mathbb{Z}$-modules are precisely abelian groups. Any abelian group G can be made into a $\mathbb{Z}$-module as follows: for $n \geq 0$, define $nx = \underbrace{x + \cdots + x}_{n \text{ times}}$ (and as a sum of $-x$'s if n is negative). But this is the *unique* way to make G into a $\mathbb{Z}$-module, because the axioms tell us for example that $2x$ must equal $x + x$, $3x = 2x + x = x + x + x$, and so on. Conversely, we already know that any $\mathbb{Z}$-module G is an abelian group by the first axiom, and the rest become trivial when we take $R = \mathbb{Z}$.
4. $R[X]$ is an R-module: we can add elements of $R[X]$ together and we can multiply by elements of R.

5. R any ring, M = any ideal I of R. Again, we can add elements of I together since it is a subgroup, and we can multiply by elements of R (and stay inside I). This is a good place to look for examples of modules for the later exercises.

6. Let S be a subring of R. Then R is an S-module: we can add elements of R together, and we can multiply by scalars, which are now taken from the subring S.

7. Quotient rings R/I are also R-modules. Addition is given by adding the cosets together: $(r+I)+(s+I) = r+s+I$, and scalar multiplication is given by $r \cdot (s+I) := rs+I$.

8. We've made the quotient ring R/I into a module over R. But R/I is ring in its own right, so what do modules over R/I look like?

   A neat characterisation to help you think about them is: R/I-modules M are precisely R-modules M such that $IM = 0$.

   [If M is an R/I-module, there is a natural way to make M an R-module: the abelian group structure of M isn't affected by the ring of scalars, and to define scalar multiplication by elements of R, take $rm := (r+I)m$. This implies $i \cdot m = 0 \ \forall \ i \in I, m \in M$. Conversely, if M is an R-module such that $IM = 0$, then to define scalar multiplication by elements of the quotient ring, take $(r+I)m := rm$. The condition $IM = 0$ makes this well-defined.]

Definition 6.3. *An* algebra over a ring R *is an R-module A with an associative binary operation $\cdot : A \times A \to A$ ('multiplication') satisfying:*

- $(a+b)\cdot c = a\cdot c + b\cdot c$ *and* $a\cdot(b+c) = a\cdot b + a\cdot c \ \forall \ a,b,c \in A$ *(distributivity)*
- $(ra)\cdot(sb) = (rs)(a\cdot b) \ \forall \ r,s \in R, a,b \in A$ *(compatibility with scalars)*

So an R-algebra A is an R-module with an extra *associative multiplication operation* that distributes and is compatible with the scalar multiplication. Usually, we deal with algebras over a field, say $R = k$, which means we care about k-algebras: these are simply k-vector spaces that are also rings.

Example 6.4.

1. What about Euclidean space $\mathbb{R}^3$ with the vector cross product? Is this an algebra over the reals? It is clearly a real vector space, and now we have a way of multiplying vectors together. Unfortunately it's not (according to our working definitions of 'ring' and 'algebra'), because cross product is *not* associative: $a \times (b \times c) \neq (a \times b) \times c$ in general. In fact, the cross product doesn't even make $\mathbb{R}^3$ into a commutative ring, because $a \times b = -(b \times a)$ (anti-commutativity).

2. The space of all functions from $\mathbb{R}$ to $\mathbb{R}$ *is* an algebra over $\mathbb{R}$: we can add functions together and multiply them by real constants, so it is a real vector space (in fact an infinite-dimensional one). But we can also multiply functions together by doing it pointwise: $(fg)(x) := f(x)g(x)$, so in fact this space is also a ring, and hence it is a real algebra.

3. Group algebras: let G be a group and let $\mathbb{C}G$ be the $\mathbb{C}$-vector space with basis indexed by the group elements $\{e_g \mid g \in G\}$. We define multiplication of the vector space elements as $e_g \cdot e_h = e_{gh}$ and extend it linearly, so

$$\sum_{g\in G} \alpha_g e_g \cdot \sum_{h\in G} \beta_h e_h = \sum_{g,h\in G} \alpha_g \beta_h e_{gh}$$

for complex numbers α_g, β_h. This turns $\mathbb{C}G$ into an algebra over $\mathbb{C}$.

Representation theory deals with objects called *representations* (unsurprisingly), often of a group G over $\mathbb{C}$ or some other field. These turn out to be precisely modules over the ring $\mathbb{C}G$. More generally, one can consider representations of algebras A, not just groups G, and these are precisely just A-modules.

Having vector spaces in mind is a good example of nice modules, but some modules can also look nothing like vector spaces. Recall the definitions of linear combinations, linear independence, spanning set and basis from your linear algebra courses. The definitions are the same in the context of modules:

Definition 6.5. *Let M be an R-module and let $x_1, \dots, x_n \in M$.*

- *A* linear combination *(or* R-linear combination*) of the $x_1, \dots, x_n$ is an element of the form $r_1x_1 + \cdots + r_nx_n \in M$.*
- *$x_1, \dots, x_n$ are a* spanning set *for M if every element of M is a linear combination of the x_i.*
- *$x_1, \dots, x_n$ are* linearly independent *(or* R-linearly independent*) if $r_1x_1 + \cdots + r_nx_n = 0_M$ for some $r_i \in R$ implies $r_i = 0$ $\forall i$.*
- *$x_1, \dots, x_n$ form a* basis *(or* R-basis*) of M if they are both linearly independent and span M.*

But these don't always behave nicely anymore. Here are some warnings and examples:

Example 6.6.
1. $R[X]$ has $\{1, X, X^2, \dots, \}$ as a basis.
2. $R = \mathbb{Z}$, $M = \mathbb{Z}$: $\{2, 3\}$ is a spanning set, but does not contain a basis. Also, $\{2\}$ is a linearly independent set, but does not extend to a basis. $\mathbb{Z}$ has a basis of size 1, namely $\{1\}$, but the proper submodule $2\mathbb{Z}$ also has a basis of size 1, namely $\{2\}$. So proper submodules don't have strictly smaller bases, in contrast to the case of finite-dimensional vector spaces and subspaces.
3. The $\mathbb{Z}$-module $\mathbb{Z}_5$ doesn't have a basis at all. Any one element x is already linearly dependent, because $5 \cdot x = x + x + x + x + x = 0$.

We have just hinted at the next concept: *submodules*. Like for any other object and sub-object that you have seen so far, a submodule is a module in its own right and is closed under scalar multiplication by R.

Definition 6.7. *Let M be an R-module. A subset N of M is a* submodule (R-submodule of M) *if it is a module under the induced operations, i.e. N is a subgroup of $(M, +)$ and $rx \in N$ $\forall$ $r \in R, x \in N$. This is often written $N \leq M$ or $N \subseteq M$.*

Example 6.8.
1. From above, $R = \mathbb{Z}$, $M = \mathbb{Z}$, $N = 2\mathbb{Z}$.
2. $0_R \cdot x = 0_M$ for all $x \in M$. So $\{0_M\}$ is a submodule of M, called the *zero submodule* of M.
3. $R = k$ field, M a k-vector space. What are the submodules of M? (Vector subspaces)
4. $R = \mathbb{Z}$, $M =$ an abelian group. What are the submodules of M? (Subgroups)

5. R any ring, $M = R$. What are the submodules of M? (Ideals of R)

Definition 6.9. *Let M be an R-module.*

- *For $x_1, \ldots, x_n \in M$, the submodule* generated *by $x_1, \ldots, x_n$ is $(x_1, \ldots, x_n) = Rx_1 + \cdots + Rx_n = \{r_1x_1 + \cdots + r_nx_n \mid r_i \in R\}$.*
- *M is* finitely generated *if $M = (x_1, \ldots, x_n)$ for some $x_i \in M$, i.e. M has a finite spanning set.*
- *M is* cyclic *if it can be generated by a single element, i.e. $M = (x)$ for some $x \in M$.*

Warning: submodules of finitely generated module need not be finitely generated themselves. E.g. $R = \mathcal{P}(\mathbb{N})$, $M = R$. Then M is finitely generated (by the single element $1_R = \mathbb{N}$ in fact), but the submodule (ideal) $I = \{A \subseteq \mathbb{N} \mid A \text{ finite}\}$ is not finitely generated.

7 Homomorphisms and quotient modules

Definition 7.1. *Let M, N be R-modules. A function $\varphi : M \to N$ is a* homomorphism (R-homomorphism, R-module map) *if it preserves module structure, i.e. φ is a group homomorphism and $\varphi(rx) = r\varphi(x)$ $\forall$ $x \in M, r \in R$.*

The image $\varphi(M)$ is a submodule of N, and $\ker\varphi$ is a submodule of M.

Example 7.2.
1. $R = k$ field, R-hom $= k$-linear maps.
2. $R = \mathbb{Z}$, R-hom $=$ group hom (between abelian groups).
3. An $R[X]$-module M is precisely an R-module equipped with an R-hom $\overline{X} : M \to M$ given by $m \mapsto Xm$. So in the case R is a field k, a $k[X]$-module is just a k-vector space equipped with a k-linear map from the space to itself, and in the case $R = \mathbb{Z}$, a $\mathbb{Z}[X]$-module is an abelian group equipped with a group hom from the group to itself.

We say a module is *free* if it has a basis, and *free of rank n* if it has a basis of size n. For example, R, R^2, R^3, $R[X]$ are free. If M is free of rank n, then $M \cong R^n$.

Remark 7.3.
1. So far, it is not obvious that $R^n \ncong R^m$ for $n \neq m$. (This turns out to be true whenever R is a Euclidean domain though for example.)
2. If M is finitely generated, say $M = (x_1, \ldots, x_n)$, then M is a homomorphic image of R^n: take the map $\varphi : R^n \to M$ with $(r_1, \ldots, r_n) \mapsto r_1x_1 + \cdots r_nx_n$. This is surjective so $R^n / \ker\varphi \cong M$.
3. Recall that the R-submodules of R itself are just the ideals I of R. So the quotient modules of R are precisely R/I for some ideal I. Moreover, M is a cyclic R-module iff M is an image of $R^1 = R$, so M is cyclic iff $M \cong R/I$ for some ideal I of R.

We've made quotient groups and quotient rings. Naturally, we can also make quotient modules.

Definition 7.4. *Given an R-module M and submodule N, the quotient group M/N can be made into an R-module by defining scalar multiplication by $r(x+N) := rx+N$ for all $r \in R, x \in M$. This is the* quotient module *M/N.*

As usual, given any submodule N, we can realise it as the kernel of an R-homomorphism via the *projection map* $\pi : M \to M/N$, $x \mapsto x+N$. So we have a correspondence

kernels of group homs	kernels of ring homs	kernels of module homs
$\updownarrow$	$\updownarrow$	$\updownarrow$
normal subgroups	ideals	submodules

Like for groups and rings, we also have the first isomorphism theorem for modules: $M/\ker\varphi \cong \varphi(M)$ are isomorphic *as modules*.

Exercise 13. An R-module M always has at least two submodules, 0 and M itself. M is *simple (irreducible)* if it has only these submodules. Show that a non-trivial (non-zero) R-module is simple if and only if it is isomorphic *as an R-module* to R/I for some maximal ideal $I \leq R$.

(Hint: to show that a simple module $0 \neq M$ is isomorphic to R/I for some I, consider the ideal $\mathrm{Ann}(m) := \{r \in R \mid r \cdot m = 0_M\}$ for some $0 \neq m \in M$. This is the *annihilator* of m.)

8 The structure theorem

Definition 8.1. *If M and N are R-modules, then the* module direct sum *$M \oplus N$ is the abelian group $M \oplus N$ endowed with scalar multiplication $r(x,y) := (rx, ry)$ $\forall$ $r \in R, x \in M, y \in N$.*

Theorem 8.2. *A finitely generated module over a PID is a (finite) direct sum of cyclic modules.*

The structure theorem is not true for UFDs, e.g. $R = \mathbb{Z}[X]$, $M = (2, X)$. M is finitely generated, but it is not a cyclic module since it is not a principal ideal. You can also show that it is not the direct sum of at least 2 cyclic modules.

Let's apply the structure theorem to $\mathbb{Z}$ which *is* a PID. We already know that $\mathbb{Z}$-modules are precisely abelian groups. The cyclic abelian groups are $\mathbb{Z}_n$ *and* $\mathbb{Z}$ (remember, the infinite group $\mathbb{Z}$ is still a cyclic group since it has the generator 1). This gives:

Corollary 8.3. *Any finitely generated abelian group is of the form $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k} \oplus \mathbb{Z}^m$ for some $n_i, m \in \mathbb{N}$. In particular, any finite abelian group has this form with $m = 0$.*

But we can do even better than this: for example, we know by the Chinese Remainder Theorem that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$ when m and n are coprime. This means we can refine the structure theorem to say

$$\mathbb{Z}_{p_1^{a_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{a_t}} \oplus \mathbb{Z}^m$$

for not necessarily distinct primes $p_1, \ldots, p_t$ and $a_i \geq 1$. This is basically as far as we can go, since we have groups like $\mathbb{Z}_4 \oplus \mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2$ and $\mathbb{Z}_{32}$ which are all non-isomorphic but have the same size.

What about for general PIDs R?

Proposition 8.4 (Chinese Remainder Theorem for PIDs)**.** *Let R be a PID. Let $r, s \in R$ be coprime (i.e. no non-unit divides both r and s). Then $R/(rs) \cong R/(r) \oplus R/(s)$ as R-modules (and also as rings).*

Definition 8.5. *For a PID R, a cyclic R-module R/I is* primary *if $I = (p^a)$ for some prime element $p \in R$ and $a \geq 0$, or $I = 0$.*

More generally, a proper ideal I of a ring R is *primary* if whenever $xy \in I$, then $x \in I$ or $y^n \in I$ for some $n > 0$. Any prime ideal is primary, but the converse is not true (e.g. $(X, Y^2) \subset k[X, Y]$ for k a field). With this terminology, we can now combine the structure theorem together with the Chinese Remainder Theorem to get the following:

Corollary 8.6 (Primary decomposition theorem)**.** *Every finitely generated module over a PID is a (finite) direct sum of primary modules.*

A useful corollary of the primary decomposition theorem is Jordan Normal Form. Let $R = \mathbb{C}[X]$. Let V be a finite-dimensional $\mathbb{C}$-vector space and let $\alpha : V \to V$ be a linear map. Then V is a $\mathbb{C}[X]$-module by letting $f \cdot x := f(\alpha)(x)$. We know that V is a direct sum of primary submodules, but what do primary submodules W of V look like?

The prime elements of $\mathbb{C}[X]$ are precisely the irreducibles, since $\mathbb{C}[X]$ is a PID. By the fundamental theorem of algebra, the irreducible polynomials are precisely the linear ones, $X - \lambda$ for some $\lambda \in \mathbb{C}$. So primary $\mathbb{C}[X]$-submodules W are isomorphic to $\mathbb{C}[X]/((X - \lambda)^a)$. [We can only have R/I with I of the form (p^a), $a > 0$: if $I = (1) = R$ then R/I is zero, and we can omit zero summands in the structure theorem. We can't have the case $I = 0$ here because then $W \cong \mathbb{C}[X]$ is infinite-dimensional, whereas V is finite-dim.]

Hence the elements of W are all of the form $f(\alpha)(x)$ where $\deg(f) < a$. One can check that $x, (\alpha - \lambda)(x), (\alpha - \lambda)^2(x), \ldots, (\alpha - \lambda)^{a-1}(x)$ forms a basis for W (span and linearly independent), w.r.t which the linear map $\alpha - \lambda$ has matrix

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

So α has matrix equal to a 'λ-block':

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

Corollary 8.7 (Jordan Normal Form)**.** *Let α be a linear map on a finite-dimensional $\mathbb{C}$-vector space V. Then there exists a basis of V w.r.t. which α has matrix equal to a diagonal sum of blocks (of various sizes, for various values of $\lambda \in \mathbb{C}$).*