MATH 457 Honours Algebra 4[*]

Notes by

Marcel K. Goh

23 April 2020

Note. These notes are quite rough and skip over a lot of details. Most proofs are either omitted or distilled to their main ideas.

1. Rings

A *ring* R is a set with operations $+$ and $\cdot$ such that

i) $(R, +)$ is an abelian group;
ii) $(R, \cdot)$ is a semigroup;
iii) $\cdot$ distributes over $+$ on both sides:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (a + b) \cdot c = a \cdot c + b \cdot c$$

A *semiring is the same as a ring* except that condition (i) above becomes

i') $(R, +)$ is a monoid with absorbing identity 0.

A ring is *unital* if $(R, \cdot)$ has a unit 1. We always assume that $1 \neq 0$, since if $1 = 0$ then $R = \{0\}$. Observe that in a unital ring, $(R, +)$ is necessarily abelian. A ring is said to be *commutative* if $(R, \cdot)$ is.

Even for commutative rings, there are many possible ring structures for $(R, +) = \mathbf{Z}^2$. For example we can take the *Gaussian integers* $\mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\}$ or the *Eisenstein integers* $\mathbf{Z}[\omega] = \{a + b\omega : a, b \in \mathbf{Z}\}$ where

$$\omega = -\frac{1 + i\sqrt{3}}{2}.$$

In both cases the second binary operation is complex multiplication. Since i and ω are both solutions to equations of the form $x^2 + Bx + C = 0$, they are called *quadratic integers* and $\mathbf{Z}[i]$ and $\mathbf{Z}[\omega]$ are called *quadratic rings*.

The definition of a ring is meant to describe a class of $\mathbf{Z}$-like objects, but many rings have properties different from the integers. For example, the ring $\mathbf{Z}[\sqrt{-5}]$ does not have Euclidean division. There are also many non-commutative rings such as the *Lipschitz quaternions*

$$\{a + bi + cj + dk : a, b, c, d \in \mathbf{Z}\}$$

or the *Hurwitz quaternions*

$$\left\{a + bi + cj + dk : a, b, c, d \in \mathbf{Z} \text{ or } a, b, c, d \in \mathbf{Z} + \frac{1}{2}\right\}.$$

If R is a ring, then a subgroup of $(R, +)$ that is closed under multiplication is called a *subring*. If a ring is unital, then any unital subring will have the same unit. A *homomorphism* between two rings R and S is a map $f : R \to S$ that preserves both operations:

$$f(a + b) = f(a) + f(b) \qquad \text{and} \qquad f(a \cdot b) = f(a) \cdot f(b)$$

A homomorphism that preserves the units is called *unital*.

[*] Course given by Prof. Mikaël Pichot at McGill University

An *ideal* in a ring R is a subgroup $(I, +)$ such that

i) $ab \in I$ for all $a \in R$, $b \in I$;

ii) $ab \in I$ for all $b \in I$, $a \in R$.

If (i) holds, I is called a *left ideal* and if (ii) holds, I is called a right ideal. Let $I \subseteq R$ be an ideal. One defines the *quotient ring* R/I as follows. Since $(I, +)$ is a normal subgroup of $(R, +)$, R/I is an abelian group. We associate $r \sim r'$ if $r - r' \in I$. Then we can define multiplication in R/I as $(a+I)(b+I) = ab+I$. This is well-defined because I is an ideal and distributivity holds.

The isomorphism theorems for groups extend to rings as well.

Theorem A (*First isomorphism theorem*). *Let $f : R \twoheadrightarrow S$ be a surjective ring homomorphism. Then f descends to a a ring homomorphism $f' : R/I \to S$ that takes $a + I$ to $f(a)$, where I is the kernel of f.* ▮

Theorem B (*Second isomorphism theorem*). *Let S be a subring and I and ideal in a ring R. Then $S + I$ is a subring of R, I is an ideal in $S + I$, and the map $S \twoheadrightarrow (S + I)/I$ is a surjective ring homomorphism with kernel $S \cap I$.* ▮

Theorem C (*Third isomorphism theorem*). *Let R be a ring and $I \subseteq J \subseteq R$ be ideals. Then $R/I \twoheadrightarrow R/J$ is a surjective ring homomorphism with kernel J/I.* ▮

Theorem D (*Fourth isomorphism theorem*). *Let $f : R \twoheadrightarrow S$ be a surjective ring homomorphism. There is a bijection between the ideals in R containing $\ker f$ and the set of all ideals in S.* ▮

Note that the correspondence in Theorem D works with subrings as well, not just ideals.

An element r in a unital ring R is said to be *invertible* if there exists $s \in R$ such that $rs = sr = 1$. The set of invertible elements is denoted $R^{\times}$ and this is a group under ×, called the *group of units*. A *field* is a ring in which every nonzero element is a unit. Non-commutative fields are called *division rings* or *skew fields* (the quaternions are an example of a skew field).

Let K be a field. The set $K[x]$ of polynomials with coefficients in K is a ring. Then the set

$$K(x) = \{f/g : f, g \in K[x], g \neq 0\}$$

is a field, called the *field of rational functions*. The set $K[[x]]$ is called the *ring of formal series*: possibly infinite sums $\sum_{n \geq 0} a_n x^n$. Addition is done pointwise and multiplication is convolution of power series. The map $K[x] \to K[[x]]$ is a homomorphism and some elements become invertible. For example, $1 - x$ becomes invertible, since $1/(1-x) = \sum_{n \geq 0} x^n$. Not every element in $K[[x]]$ is invertible, but one can invert the elements to get a new field $K((x))$: the set of sequences $K^{\mathbf{Z}}$ that are eventually zero when going to the left.

A *zero-divisor* is an element $r \in R$, $r \neq 0$ for which there exists $s \in R$ such that $rs = 0$. A ring is *cancellative* if $rs = rs'$ implies that $s = s'$. Then we define an *integral domain* to be a unital, commutative, cancellative ring. Every integral domain embeds into a field, called the *field of fractions*. The construction is analogous to building the rational numbers from the integers.

Proposition Z. *If R is a ring with unity, there exists a unique unital homomorphism $f : \mathbf{Z} \to R$.* ▮

Proof. Since $f(1) = 1$, we have $f(n) = 1 + 1 + \cdots + 1 \in R$. ▮

The nonnegative integer n which generates $\ker f$ is called the *characteristic* of R. The image of f is called the *characteristic subring*. For example $\mathbf{Z}/n\mathbf{Z}$ has characteristic n.

Proposition P. *The characteristic of an integral domain R is either 0 or a prime number.* ▮

An *algebra* over a commutative ring R is a ring A with a homomorphism $\eta : \mathbf{R} \to A$ whose image lies in the *centre* of A. Examples of algebras include rings of functions and matrices $M_n(R)$.

For a group G and a ring R, we can define the *group ring* $G[R]$ as the set of all finitely supported functions from G to R. This forms a ring with addition $(f+g)(s) = f(s) = g(s)$ and multiplication $(fg)(s) = \sum_{uv=s} f(u)g(u)$.

2. Ideals

Every element r in a unital ring R generates a *principal* ideal (r). More generally any subset $S \subseteq R$ does. The ideal (S) is the intersection of all ideals that contain S. If R is commutative, then $(r) = rR = Rr$. In $\mathbf{Z}$, the ideals are the of the form $(n) = n\mathbf{Z}$. Then $(n) \subseteq (m)$ if and only if $m \setminus n$ (this is true in any commutative ring). A ring R in which every ideal is principal is called a *principal ring* and if R is also an integral domain, we call it a *principal ideal domain* or PID.

Principal ideals determine their generators up to unit. If $(r) = (s)$, then $s = ar$ and $r = bs$ together imply that both a and b are units. Elements r and s of a ring R are called *associate* if there exists a unit a such that $r = as$.

We can define three operations on ideals. Let $I, J \subseteq R$ be ideals.

i) $I \cap J$ is an ideal.

ii) $I + J = \{a + b : a \in I, b \in J\} = (I \cup J)$ is an ideal.

iii) $IJ = \{ab : a \in I, b \in J\}$ is an ideal.

Lemma P. *Let R be a commutative ring. Let $I = (S)$ and $J = (T)$ be two ideals. Then $IJ = (ST)$.* ▮

In the ring of integers $\mathbf{Z}$, we have $(m)(n) = (mn)$, $(m) \cap (n) = \big(\operatorname{lcm}(m, n)\big)$, and $(m)+(n) = \big(\gcd(m, n)\big)$. When $I \subseteq J$ is an inclusion of ideals, one may think of it as a kind of divisibility $J \setminus I$. For example, $\gcd(m, n) \setminus \operatorname{lcm}(m, n) \setminus mn$.

Lemma D. *If $I, J \subseteq R$ are ideals, then*

$$IJ \subseteq I \cap J \subseteq I + J. \quad ▮$$

The set of ideals forms a semiring where the two operations are $I + J$ and IJ. The semiring in $\mathbf{Z}$ is $\mathbf{N}$ with the addition $m + n = \gcd(m, n)$ and ordinary multiplication.

For an ideal $I \subseteq R$, we define the *radical* of I to be the set

$$\sqrt{I} = \{a \in R : a^n \in I \text{ for some } n \in \mathbf{N}\}.$$

This is an ideal and it has the property that $\sqrt{\sqrt{I}} = \sqrt{I}$. Furthermore, if $I \subseteq J$, then $\sqrt{I} \subseteq \sqrt{J}$.

An ideal $I \subseteq R$ is called *maximal* if it is proper and whenever $I \subseteq J \subseteq R$, then either $J = I$ or $J = R$.

Lemma M. *Let R be a unital ring. Then every proper ideal is included in a maximal ideal.*

Proof. This is an application of Zorn's Lemma. Let I be a proper ideal and let X be the set of all proper ideals containing I, ordered by inclusion. Then this set is inductive (increasing union of ideals is an ideal) so there is a maximal element M. ▮

Lemma F. *Let R be unital and commutative. Then an ideal $I \subseteq R$ is maximal if and only if R/I is a field.*

Proof. This follows from the fourth isomorphism theorem. ▮

Let R be a unital ring. An ideal I of R is *prime* if it is proper and for any ideals A, B of R, $AB \subseteq I$ implies that $A \subseteq I$ or $B \subseteq I$. The *spectrum* of R is the set of all prime ideals and it is denoted $\operatorname{Spec}(R)$. The *maximal spectrum* of R, denoted $\operatorname{Spec}_{\max}(R)$, is the set of all maximal ideals of R.

Maximal ideals are always prime (so $\operatorname{Spec}_{\max}(R) \subseteq \operatorname{Spec}(R)$), but not all prime ideals are maximal. For example, (0) is prime in $\mathbf{Z}$ but certainly not maximal. A ring is called *local* if it has a unique maximal ideal. A ring R is local if and only if $R \setminus R^\times$ is an ideal.

Lemma C. *Let R be a unital commutative ring. Let $I \subseteq R$ be a proper ideal. Then I is prime if and only if $ab \in I$ implies that $a \in I$ or $b \in I$.* ▮

Lemma I. *Let R be a unital commutative ring. Then $I \subseteq R$ is a prime ideal if and only if R/I is an integral domain.* ▮

Since all fields are integral domains, this proves that all maximal ideals are prime. We also have that a commutative ring R is an integral domain if and only if (0) is a prime ideal in R (if R is not commutative, then we say it is a *prime ring*). If R is a PID, then every nonzero prime ideal is maximal.

We can view elements in a commutative unital ring R as "functions" on the set $\operatorname{Spec}(R)$ of prime ideals. To $r \in R$ we identify a function f_r such that $f_r(P) = r \bmod P \in R/P$. We have a bundle at every $P \in \operatorname{Spec}(R)$ and a fibre R/P which is an integral domain. The *total space* $B(R)$ is the union of R/P over all prime ideals P. A *section* is a map $s : \operatorname{Spec}(R) \to B(R)$ such that $s(P) \in R/P$. $\Gamma(R)$ is the set of all sections and $\Gamma_{\max}(R)$ is its restriction to $\operatorname{Spec}_{\max}(R)$. Let $\pi : R \to \Gamma(R)$ map $r \mapsto f_r$ and $\pi_{\max} : R \to \Gamma_{\max}(R)$ take r to f_r, restricted to $\operatorname{Spec}_{\max}(R)$. We want to know when π and $\pi_{\max}$ are faithful.

Proposition K. *The kernel of π is the intersection of all prime ideals and the kernel of $\pi_{\max}$ is the intersection of all maximal ideals.* ▌

For a unital commutative ring R, we define the *nilradical* of R to be the intersection $\operatorname{Nil}(R) = \bigcap P$ of all prime ideals P. The *Jacobean radical* is the intersection $\operatorname{Jac}(R) = \bigcap M$ of all maximal ideals M. Since $\operatorname{Spec}_{\max}(R) \subseteq \operatorname{Spec}(R)$, $\operatorname{Jac}(R) \supseteq \operatorname{Nil}(R)$. An element $r \neq 0$ in a ring R is called *nilpotent* if $r^n = 0$ for some n. It turns out that there is a connection between nilpotency and prime ideals.

Proposition N. *Let R be unital and commutative. Then* $\operatorname{Nil}(R)$ *is the set of all nilpotent elements, i.e.*

$$\sqrt{(0)} = \{r \in R : r^n = 0 \text{ for some } n \in \mathbf{N}\} = \bigcap_{P \in \operatorname{Spec}(R)} P.$$

Proof. To show that a nilpotent element r belongs to every prime ideal P, note that $r^n \in P$, so $r \cdot r^{n-1} \in P$ and we can iterate this until we get that $r \in P$. Conversely, if r is not nilpotent, we can let X be the set of ideals I such that r^n is not in I for any n. X is nonempty and inductive, so by Zorn's Lemma there is a maximal element and it can be shown that this ideal is prime. ▌

Let R be a commutative ring and let $p \in R$ be a nonzero non-unit. Then p is said to be

i) *prime* if $p \setminus ab$ implies that $p \setminus a$ or $p \setminus b$;
ii) *irreducible* if $p = ab$ implies a is a unit or b is a unit.

To find irreducible elements in a ring, may attempt the "bisection process". Let $r \in R$. If r is irreducible, we stop. If r is not irreducible, then $r = r_1 r_2$. If neither is irreducible, we continue by splitting r_1 and r_2 in the same way. This process may not terminate.

Proposition I. *Let R be an integral domain. If an element $p \in R$ is prime, then it is irreducible.*

Proof. . Let $p \in R$ be a prime element. Assume that $p = ab$. This implies that $p \setminus a$ or $p \setminus b$. Say $a = pc$ for some $c \in R$. Then $p = ab = pcb$ and $cb = 1$. So b is a unit. ▌

Note that the converse does not hold. For example, in the ring $\mathbf{Z}[\sqrt{-3}]$, we have $4 = (1+\sqrt{-3})(1-\sqrt{-3})$. The element 2 is irreducible, but it is not prime because 2 divides 4 but does not divide either of $(1+\sqrt{-3})$ and $(1-\sqrt{-3})$.

Proposition A. *Let R be an integral domain. Let p be a nonzero element in R. Then p is prime if and only if (p) is prime and p is irreducible if and only if (p) is maximal among principal ideals.* ▌

This proposition implies that in a PID, irreducible elements are prime.

A ring R is a *unique factorisation domain* if every $r \in R$ can be expressed as a product $r = p_1 \cdots p_n$ of irreducible elements, which is unique up to the order of the p_i. The rings $\mathbf{Z}$, $K[x]$, and $K[x, y]$ are all examples of UFDs. Every PID is a UFD and in a UFD, all irreducible elements are prime.

Lemma S. *In a PID, every chain of ideals stabilises.*

Proof. $I = \bigcup_{n \geq 1} I_n$ is an ideal. Since R is a PID, $I = (x)$ for some x and $x \in I_n$ for some n. This implies that $I = I_n$. ▌

Lemma N. *Let R be a unital ring. Then every increasing chain of ideals stabilises if and only if every ideal is finitely generated.*

Proof. If $I = (x_1, x_2, \ldots)$ is not finitely generated, then $I_n = (x_1, \ldots, x_n)$ is an increasing chain of ideals that does not stabilise. Conversely, if every ideal is finitely generated, then let $I_1 \subseteq I_2 \subseteq \cdots$ be a chain of ideals and let $I = \bigcup_{n \geq 1} I_n$. There exist $(x_1, \ldots, x_n)$ that generate I, so there exists a k such $x_i \in I_k$ for all i and we find that $I = I_k$. ▌

A ring is called *Noetherian* if it the equivalent conditions from Lemma N hold.

For elements r and s of a ring, a *greatest common divisor* or gcd is an element d dividing both r and s such that if any d' divides both r and s, then d' divides d. An integral domain R is called a *Bézout domain* if $(r) + (s)$ is principal for every $r, s \in R$ (of course, every PID is a Bézout domain) and it is called a *GCD domain* if any two $r, s \in R$ have a gcd. Every UFD is a GCD domain.

Lemma B. *The following statements regarding Bézout domains are true.*

i) A ring R is Bézout if and only if every finitely generated ideal is principal.

ii) A Bézout domain is a GCD.

iii) If a ring is both Noetherian and a Bézout domain, then it is a PID. ▮

3. Gaussian Integers

Recall from Section 1 that the Gaussian integers are the ring

$$\mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\}.$$

We write N for the complex modulus, squared. So $N(z) = z\overline{z} = a^2 + b^2$. This is called the *norm* and it is a group homomorphism $\mathbf{C}^\times \to \mathbf{R}^\times$, since $N(zz') = N(z)N(z')$. $N(z) = 0$ implies that $z = 0$. The norm n takes $\mathbf{Z}[i]$ to $\mathbf{N}$. The kernel of N on $\mathbf{C}^\times$ is the unit circle $\{z \in \mathbf{C} : |z| = 1\}$. Let $\ker N$ denote the kernel of N restricted to $\mathbf{Z}[i]$, i.e. $\{\pm 1, \pm i\}$. These are the units of $\mathbf{Z}[i]$.

The image of N is

$$\mathrm{Im}(N) = \{n \in \mathbf{N} : n = a^2 + b^2 \text{ for some } a, b \in \mathbf{Z}\}.$$

This set is stable under product, since if $n = N(z)$ and $n' = N(z')$, then $nn' = N(zz')$. Gauss was interested in studying the number of integer numbers less than a given n that can be expressed as a sum of two squares. We will return to this point later.

We say that a prime number *splits* if it is no longer prime in $\mathbf{Z}[i]$ and we say that it is *inert* otherwise.

Lemma S. *Let p be a prime. Then p is a sum of two squares if and only if it splits in $\mathbf{Z}[i]$.*

Proof. If $p = a^2 + b^2$ then $p = (a + ib)(a - ib)$ and $N(a + ib)N(a - ib) = p^2$ implies that neither of these factors are units. So p is not prime in $\mathbf{Z}[i]$. Conversely, if $p = \alpha\beta$ in $\mathbf{Z}[i]$, then $N(\alpha) = N(\beta) = p$ means that p is the sum of two squares. ▮

Lemma I. *A prime p splits if and only if $p \equiv 1 \pmod 4$.*

Proof. If p splits, then by the previous lemma, $p = a^2 + b^2$ and the sum of two squares is never 3 modulo 4. So if p is an odd prime it is congruent to 1 modulo 4. Conversely, assume that $p \equiv 1 \pmod 4$. Then $p = 1 + 4n$ for some n and there exists $x \in \mathbf{Z}$ such that $x^2 \equiv 1 \pmod p$. (In fact, $x = (2n)!$ works.) Then p divides $x^2 + 1 = (x + i)(x - i)$. So p divides $(x + 1)$ or $(x - i)$, so p divides i and is not inert. ▮

All this talk of divisibility leads nicely into a discussion of Euclidean division. In $\mathbf{Z}$, the goal of Euclidean division for integers a and b is to find a $q \in \mathbf{Z}$ such that $a - bq$ is small, in some sense. The following proves a similar result in $\mathbf{Z}[i]$.

Proposition E. *There is a Euclidean division in $\mathbf{Z}[i]$.*

Proof. . Let $a, b \in \mathbf{Z}[i]$, $b \neq 0$. We can divide them in $\mathbf{C}$ to get $z = a/b$. Then there is a (not necessarily unique) $q \in \mathbf{Z}[i]$ that is of minimal distance to z. We have $|z - q| < 1$; in fact $|z - q| \leq \sqrt{2}/2 < 1$. So $|a - bq| < |b|$. ▮

Let us now define this generally. An integral domain R is a *Euclidean domain* if there exists a function $N : R \to \mathbf{N}$ called the *norm* such that $N(0) = 0$ and for all $a, b \in R$, $b \neq 0$, either b divides a or there exists $q \in R$ such that $N(a - bq) < N(b)$. Proposition E showed that $Z[i]$ is a Euclidean domain with the complex norm, and other familiar examples include $\mathbf{Z}$ with the absolute value function and $K[x]$ with the degree of a polynomial as its norm. In general, the Euclidean division algorithm does not give a unique answer. Even in $\mathbf{Z}$, we can end up with q or $-q$ as a quotient.

Proposition T. $\mathbf{Z}[\sqrt{-2}]$ *is a Euclidean domain.*

Proof. We repeat the same proof as for $\mathbf{Z}[i]$ except for the computation of $|z - q|$, which is now $\leq \sqrt{3}/2$. ▮

Recall that $\mathbf{Z}[\sqrt{-3}]$ is not a Euclidean domain. It is not even a UFD, since $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$. But $\mathbf{Z}[\sqrt{-3}] \subseteq \mathbf{Z}[\omega]$ and this is a Euclidean domain, with norm $N(a + b\omega) = a^2 - ab + b^2$. The units in $\mathbf{Z}[\omega]$ are the elements of norm 1: $\{\pm 1, \pm\omega, \pm\omega^2\}$ and we have unique factorisation up to units.

Proposition P. *Every Euclidean domain is a PID (and consequently a UFD).*

Proof. Let R be a Euclidean domain and $I \subseteq R$ an ideal. Let $b \neq 0$ be an element of I of minimal norm. If $a \in I$ then b divides a. Otherwise, there exists $q \in R$ such that $N(a - bq) < N(b)$, contradicting the minimality of b's norm. So I is principal. ▮

A corollary of this fact is that every ideal in $\mathbf{Z}[i]$ is principal.

4. Modules

For any set X, the set of symmetries $\mathrm{Sym}(X)$ is a group and an action of a group G on X is a group homomorphism $G \to \mathrm{Sym}(X)$. If X is a group, we can define the *ring of endomorphisms* $\mathrm{End}(X)$ as the set of group homomorphisms from X to X.

Lemma M. *Let M be an abelian group. Then* $\mathrm{End}(M)$ *is a ring.*

Proof. Addition is pointwise addition from M and multiplication is composition of maps. ▮

Let R be a a unital commutative ring. A *module* M over R is a ring homomorphism $R \to \mathrm{End}(M)$. Explicitly, the list of axioms of a module are very similar to those of a vector space (in fact, if R is a field, then a module is a vector space). For $r, s \in R$ and $m, n \in M$, we have

i) $r(m + n) = rm + rn$;

ii) $(r + s)m) = rm + sm$;

iii) $(rs)m = r(sm)$;

iv) $1m = m$.

These axioms also work if R is not commutative; in this case, we call M a *left R-module.* The kernel of $R \to \mathrm{End}(M)$ is called the *annihilator* of M:

$$\mathrm{Ann}(M) = \{r \in R : rm = 0 \text{ for all } m \in M\}$$

A module is said to be *faithful* if $\mathrm{Ann}(M)$ is trivial. If M is an R-module, then M is a faithful S-module where $S = R/\mathrm{Ann}(M)$.

Proposition I. *Any ideal I in a ring R is a module over R.*

Proof. For $a \in I$ and $r \in R$, we have $ra \in I$. The rest of the axioms follow. ▮

Quotients R/I are also modules. When $R = \mathbf{Z}$, the action is determined by the group structure in M. For example,

$$2m = (1 + 1)m = 1m + 1m = m + m.$$

When $R = K[x]$ for some field K, we have the following interesting lemma.

Lemma V. *$K[x]$-modules are operators on vector spaces and vice versa.*

Proof. Let M be a $K[x]$-module. The restriction of the $K[x]$ action to K gives a K-module structure on M. This is a vector space. Furthermore, the indeterminate x also acts on M by taking $m \mapsto xm$. This gives a map $x : M \to M$ such that $x(m + n) = x(m)$ and $x(rm) = (xr)m = (rx)m = r \cdot x(m)$. So x is a linear map.

Conversely, if V is a K-vector space, and $T : V \to V$ is a linear map, then V is a $K[x]$-module, because for any $p \in K[x]$, $p(T)$ is a linear map on V. ▮

Note that the module is not faithful, because $K[x]$ has infinite dimension but $\mathrm{End}(V)$ has finite dimension when V has finite dimension. If G is a group, $K[G]$ is the group ring and a $K[G]$-module is a linear representation of G.

A *submodule* M' of M is a subgroup that is stable under the action of the ring, i.e. for all $m, n \in M'$ and $r \in R$, $m + rn \in M'$. For example, ideals are submodules of R and if M' is a submodule, we can define the *quotient module* M/M' with the action of R:

$$r(m + M') = rm + M'$$

If M and M' are modules, then $M \times M'$ is a module. If a module has no proper nontrivial submodules, then it is called *simple*.

An R-module map is a group homomorphism $f : M \to M'$ such that $f(rm) = rf(m)$ for all $r \in R$ and $m \in M$. The kernel $\ker f$ is a submodule of M and the image of f is a submodule of M'. The isomorphism theorems for modules are exactly analogous to the ones given for rings in Section 1.

Lemma S (*Schur's lemma*). *Let M be a simple module. Then $\mathrm{End}_R(M)$ is a skew field.*

Proof. Let $f : M \to M'$ be a module map that is not identically zero. The kernel of f is a submodule of M, so since $f \neq 0$, $\ker f = \{0\}$. Then the image of f is a submodule of M' since $f \neq 0$, $\mathrm{Im}\, f = M'$. Hence f is an isomorphism. ▌

If M is an R-module and $I \subseteq R$ is an ideal, then

$$IM = \left\{ \sum r_i m_i : r_i \in I, m_i \in M \right\} \subseteq M$$

is a submodule.

Theorem C (*Chinese remainder theorem*). *Let I, J be ideals in a ring R. Let M be an R-module. Then the map*

$$M \to M/IM \times M/JM$$

has kernel $IM \cap JM$. ▌

If $I + J = R$ then the map is surjective and $(I \cap J)M = IJM$. With n ideals such that $I_k + I_l = R$ for $k \neq l$, we have

$$M/(I_1 \cdots I_n)M \cong M/I_1 M \times \cdots \times M/I_n M.$$

Let M be an R-module. If $A \subseteq M$, then

$$(A) = \left\{ \sum r_i a_i : r_i \in R, a_i \in A \right\}$$

is the submodule of M *generated* by A. A module is *finitely generated* if it admits a finite generating set and *cyclic* (or *singly generated*) if it is generated by one element. If $M = (a)$ is cyclic, then the map $R \to M$ that sends $r \mapsto ra$ is surjective with kernel $\mathrm{Ann}(M)$.

Lemma P. *Let R be an integral domain. Then the nonzero principal ideals are isomorphic to R.*

Proof. Let $I = (a)$ be an ideal (so it is an R-module). If $r \in \mathrm{Ann}(I)$ then r is a zero divisor. So $R \to I$ is an isomorphism. ▌

A finitely generated R-module M is called *free* if it is isomorphic to R^n for some n. For example, if R is a field, every module (finite-dimensional vector space) is free. Equivalently, an R-module is free if there exists a basis, that is, a generating set A such that any $m \in M$ can be written in a unique way as a finite sum

$$m = \sum_{a \in A} r_a a.$$

The set A is called a *free generating set* and the cardinality of A is called the *rank* of M.

In a PID, every ideal is a free module (isomorphic to the ring itself). For any set A and ring R, we can let F_A be the set of all functions from A to R with finite support. This is a group under pointwise addition and r acts on F_A: $(rf)(a) = r \cdot f(a)$. A basis for F_A is the set $(\delta_a)_{a \in A}$ of delta functions, where $\delta_a(b) = 1$ if $b = a$ and 0 otherwise.

Proposition U (*Universal property of free modules*). *Let ϕ be a map from a set A to an R-module M. Then there is a unique extension of ϕ to a module map $\overline{\phi} : F_A \to M$.*

Proof. Take any element $f \in F_A$ and express it as

$$f = \sum_{a \in A} r_a \delta_a$$

for some $r_a \in R$. Then let $\overline{\phi}$ be given by

$$\overline{\phi}(f) = \sum_{a \in A} r_a \phi(a). \quad ▮$$

Proposition S. *Let $N \hookrightarrow M \twoheadrightarrow F$ be a short exact sequence of modules (so $F \cong N/M$), where F is a free module. Then the sequence splits, i.e. $M \cong N \oplus F$.*

Proof. We need to construct the section s of $\pi : M \twoheadrightarrow F$. Let A be a basis of F. Since π is surjective, for any $a \in A$ we can find $m_a \in M$ such that $\pi(m_a) = m$. This gives a map $s_* : A \to M$ and by the universal property there is a unique extension $s : F_A \to M$. We have $\pi \circ s = \mathrm{Id}$ on the basis and therefore everywhere on F. So s is a section of π. Let $F' = \mathrm{Im}(s) \subseteq M$. So $F' \cong F$ as R-modules. We claim that $M = N \oplus F'$ (viewing N as a submodule of M).

Firstly, $N \cap F' = \{0\}$, since if $m \in N \cap F'$, then $\pi(m) = 0$ and there exists $f \in F$ such that $s(f) = m$. But this implies that $f = \pi\big(s(f)\big) = \pi(m) = 0$, so $m = 0$. And $M = N + F'$ because any $m \in M$ can be expressed as the sum of $\big(m - s \circ \pi(m)\big) + s \circ \pi(m)$. ▮

The following theorem shows that the rank of a free module is well-defined.

Theorem R. *If $R^n \cong R^m$ as R-modules, then $n = m$.*

Proof. Since R is unital and commutative, it contains a maximal ideal M. Let $K = R/M$ and consider the submodule $MR^n = \big\{s(x_1, \cdots, x_n) \in R^n : s \in M, x_i \in R\big\}$. The quotient module is $K^n = (R/M)^n$ and a module isomorphism $R^n \cong R^m$ descends to a R-module isomorphism $K^n \cong K^m$. This map has kernel M and is a K-vector space isomorphism. So the dimension of the two vector spaces are the same and thus $n = m$. ▮

Let M be a module over an integral domain R. The set of *torsion elements*

$$\mathrm{Tor}(M) = \{m \in M : rm = 0 \text{ for some } r \neq 0\}$$

is a submodule of M. A module is called *torsion* if $\mathrm{Tor}(M) = M$ and *torsion-free* if $\mathrm{Tor}(M) = \{0\}$. Note that R^n is torsion-free, since it has a basis $\{e_n\}$ and if $am = ra_1e_1 + \cdots + ra_ne_n = 0$, then $ra_i = 0$ for all i and $m = 0$.

Proposition T. *For any module M over an integral domain R, $M/Tor(M)$ is torsion-free.*

Proof. Let $N = M/\mathrm{Tor}(M)$ and let $\overline{m} \in N$. Suppose there exists $r \neq 0$ such that $r\overline{m} = 0$. So $\overline{rm} = 0$ and $rm \in \mathrm{Tor}(M)$. Thus there exists $s \neq 0$ such that $(rs)\overline{m} = 0$. But $\overline{rs} \neq 0$ so m must be 0. Hence $\mathrm{Tor}(N) = \{0\}$. ▮

Lemma G. *A module M over an integral domain R is torsion if and only if it is generated by torsion elements.*

Proof. The forward direction is clear. Conversely, suppose $M = (A)$ and every element in A is torsion. Let $m = s_1a_1 + \cdots + s_na_n \in M$ for some $s_i \in R$ and $a_i \in A$. Each a_i is a torsion element so there is r_i such that $r_ia_i = 0$. Let $r = r_1 \cdots r_n$. Then $rm = 0$. ▮

Proposition F. *Let M be a finitely generated module over an integral domain R. There exists a free module $F \subseteq M$ such that M/F is torsion.*

Proof. Let $M = (A)$ where A is finite. Let $B \subseteq A$ be a maximal basis which generates a free module F of rank $n = |B|$. Let N be the quotient M/F. For every $a \in A \setminus B$, the module $(B \cup \{a\})$ is not free. So there exists $r \in R, r_b \in R$, not all zero, such that

$$ra + \sum_{b \in B} r_b b = 0.$$

Note that $r \neq 0$, otherwise B would not be a basis. But $ra = 0 \bmod F$, so N is generated by torsion elements and by the previous lemma, N is torsion. ▮

5. Modules over PIDs

An R-module has properties very much like a vector space when R is a PID.

Proposition F. *Let R be a PID. Then every submodule of a free module R^n is free of rank $k \leq n$.*

Proof. We proceed by induction. When $n = 1$, every ideal $I \subseteq R$ is free, isomorphic to R. Now assume the proposition is true for R^n. Let M be a submodule of R^{n+1}. Let $\pi : R^{n+1} \twoheadrightarrow R^n$ be the projection map on to the first n coordinates. So we have a short exact sequence

$$\ker(\pi_{|M}) \hookrightarrow M \twoheadrightarrow \pi(M).$$

But $\pi(M)$ is a submodule of R^n so, by the induction hypothesis, it is free and the sequence splits. Thus $M \cong \ker(\pi_{|M}) \oplus \pi(M)$ is free. ▮

A module M over a unital ring R is called a *Noetherian module* if every submodule is finitely generated.

Propostion N. *Let M be a left R-module. The following are equivalent:*

i) M is Noetherian.

ii) M satisfies the ascending chain condition on left modules.

iii) If $\mathfrak{F}$ is a nonempty family of submodules, there exists a maximal element in $\mathfrak{F}$ with respect to inclusion.

Proof. To show that (i) implies (ii), we let $N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$ be an increasing sequence of modules. We need to know there is an upper bound. Let $N = \bigcup_{i \geq 1} N_i$. Since N is finitely generated, there will be a first index i such that all the generators of N belong to N_i. Thus $N = N_i$ for some i.

We show that (ii) implies (iii) by contraposition. If (iii) fails, then there exists a family $\mathfrak{F}$ of submodules for which there is no maximal element. Pick $N_1 \in \mathfrak{F}$. We can find N_2 such that N_1 is properly contained in N_2. Continuing in this way, we are left with an increasing chain that does not stabilise.

Lastly, assume that (i) does not hold; i.e. there is a submodule N that is not finitely generated. Let $\{n_1, n_2, \ldots\}$ be an infinite countable subset of N such that, for every k, $N_k = (n_1, \ldots, n_k)$ is properly contained in $N_{k+1} = (n_1, \ldots, n_{k+1})$. Now $\mathfrak{F} = \{N_k\}$ is a family of submodules without a maximal element, so (iii) fails. ▮

Proposition S. *Let $N \hookrightarrow P \twoheadrightarrow Q$ be an exact sequence of modules. Then N and Q are Noetherian if and only if P is Noetherian.*

Proof. Clearly N is Noetherian if P is. To show that Q is Noetherian, let $M \subseteq Q$ be a submodule. Then, by the fourth isomorphism theorem, M is the image of a submodule M' of P. Since M' is finitely generated, M is as well.

Conversely, assume that N and Q are Noetherian and let $M \subseteq P$ be a submodule. Let $\pi : P \twoheadrightarrow Q$ be the quotient map and consider the exact sequence $\ker(\pi_{|M}) \hookrightarrow M \twoheadrightarrow \pi(M)$. Let X be a finite generating set for $\ker(\pi_{|M})$ and Y be a finite set in M such that $\overline{Y} = \pi(Y)$ is a finite generating set of $\pi(M)$. Then for any $m \in M$, then there exist some r_x and r_y in R such that

$$m = \sum_{x \in X} r_x x + \sum_{y \in Y} r_y y$$

and $X \cup Y$ generates M. ▮

Theorem R. *The following are equivalent:*

i) R is a Noetherian ring.

ii) The free module R^n is Noetherian for every n.

iii) Every finitely generated R-module is Noetherian. ▮

A corollary of Theorem R is that every finitely generated module over a PID is Noetherian. For example, $R = K[x_1, \ldots, x_n]$ is Noetherian.

Lemma N. *If R is a PID and M a torsion-free R-module, then M is free.*

Proof. In general, we showed that there exists F free such that $F \hookrightarrow M \twoheadrightarrow T$, where T is torsion. Since M is Noetherian, we can choose a maximal F satisfying this property. We claim that $M = F$. Let $\pi : M \twoheadrightarrow T$ denote the quotient map and let $m \in M$. Since $\pi(m) \in T$ is a torsion element, there exists $r \in R$ such that $r\pi(m) = 0$. So $rm \in \ker \pi$ and $rm \in F$. Let $f_r : M \to M$ be the map that sends $m \mapsto rm$. This map is injective because M is torsion-free. Since $f_r(F) \subseteq F$ and $f_r(M) \subseteq F$, so the submodule $f_r(F, M)$ is contained in F. By Proposition F, $f_r(F, M)$ is free, so M is free. ▮

Theorem T. *Let M be a finitely generated module over a PID R. Then $M \cong R^n \oplus \mathrm{Tor}(M)$.*

Proof. Consider the exact sequence $\mathrm{Tor}(M) \hookrightarrow M \twoheadrightarrow N$ where N is torsion-free. Since R is a PID, N is free and the sequence splits, giving us the desired direct sum decomposition. ▮

The integer n given by Theorem T is called the *free rank* of a module. If two modules M and N are isomorphic, then their free ranks are equal and $\mathrm{Tor}(M) \cong \mathrm{Tor}(N)$. The following theorem is called the structure theorem for finitely generated modules over a PID.

Theorem S. *Let R be a PID and let $F \cong R^n$ be a finitely generated free module. Let M be a finitely generated submodule of F. Then there exists a basis $(e_1, \ldots, e_n)$ of F and elements $r_1, \ldots, r_m \in R$ such that $(r_1 e_1, \ldots, r_m e_m)$ forms a basis of M:*

$$F/M \cong R^{n-m} \oplus R/(r_1) \oplus \cdots \oplus R/(r_m)$$

The elements r_i are unique up to multiplication by a unit if we assume that r_i divides r_{i+1}. ▮

The elements r_i in Theorem S are called the *invariant factors* of the module.