HT 2022

A3: Rings and Modules

Jiaming (George) Yu
jiaming.yu@jesus.ox.ac.uk

June 22, 2023

Contents

Part I

Rings

1 Rings

1.1 Units

First recall the definition of a ring.

Definition 1.1 (Rings)

A set R, together with two binary operations $+$ (addition) and $\times$ (multiplication), is a *ring* if $(R,+)$ is an Abelian group, $(R,\times)$ is a monoid[1], and that $\times$ distributes over $+$. Denote the additive identity as 0 and the multiplicative identity as 1.[2]
For any such ring, $(R,+)$ is its *additive group*, and we say R is a *commutative ring* if $\times$ is commutative.

[1] a group without invertibility

[2] It is not necessarily the case that $1 \neq 0$

Definition 1.2

Let R, S be rings and $\phi : R \to S$ be a map. We say ϕ is *additive* if it is a homomorphism of the additive groups of R, S, and *multiplicative* if it is a homomorphism of the multiplicative monoids of R, S.
If ϕ is both additive and multiplicative, and it preserves the identity, i.e. $\phi(1_R) = 1_S$, then we call it a *ring homomorphism*.

Now we introduce units.

Definition 1.3 (Units)

Let R be a ring, and let $x \in R$. We say x is a *unit* if there is some $x^{-1} \in R$ s.t. $xx^{-1} = x^{-1}x = 1$; in other words, if x is invertible w.r.t. multiplication. We write $U(R)$ for the set of all units in R.[3]

[3] Contrast this with R^*, the set of all non-zero elements of R.

It is easy to show that $U(R)$ forms a group — the group of units — under $\times$ restricted to $U(R)$.

Definition 1.4 (Trivial Ring)

Let $R = \{0\}$, with $1 = 0$, and $0 + 0 = 0 \times 0 = 0$. R is the (unique) *trivial ring* or *zero ring*. A ring with $1 \neq 0$ is a *non-trivial ring*.

Example 1.1

The integers $\mathbb{Z}$ form a non-trivial commutative ring with $U(\mathbb{Z}) = \{-1, 1\}$.

Theorem 1.1

Let R be a ring. There exists a unique ring homomorphism $\chi_R : \mathbb{Z} \to R$, where

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

Definition 1.5 (Characteristic of Ring)

Let R be a ring. If there is some $n \in \mathbb{N}^*$ with $\chi_R(n) = 0_R$, then we call the smallest such n the *characteristic* of R. If there are no such n, then R has a characteristic of 0.

1.2 Ring Isomorphisms and Subrings

Definition 1.6 (Ring Isomorphisms)

A *ring isomorphism* is a ring homomorphism $\phi : R \to S$ with an inverse $\phi^{-1} : S \to R$ that is also a ring homomorphism.

Definition 1.7 (Subrings)

Let R be a ring. A subset $S \subseteq R$ is a *subring* of R if S is a ring with $+_R, \times_R$ restricted to S (this implies that $0, 1 \in S$).

Remark that since 0 and 1 are preserved in subrings, this implies that:

- subrings of a non-trivial ring are non-trivial
- the trivial ring is not a subring of any non-trivial ring
- characteristic of a ring remains unchanged for subrings

Proposition 1.2 (Subring Test)

Let R be a ring and $S \subseteq R$. If $1 \in S$ and $\forall x, y \in S : x - y, xy \in S$, then S is a subring of R.

Definition 1.8

Let $d \in \mathbb{N}^*$. Define $\mathbb{Z}[\sqrt{-d}] := \left\{ z + w\sqrt{-d} : z, w \in \mathbb{Z} \right\}$. For the special case of $d = 1$, the set $\mathbb{Z}[i]$ is the *Gaussian integers*. Each $\mathbb{Z}[\sqrt{-d}]$ is a subring of $\mathbb{C}$.

1.3 Integral Domains

Definition 1.9 (Zero Divisors)

Let R be a ring and $x \in R$. We say x is a *left* (resp. *right*) *zero divisor* if there is some $y \in R^*$ such that $xy = 0$ (resp. $yx = 0$). In other words, if the left (resp. right) multiplication by x map has a non-trivial kernel.

One can show that a unit is never a zero divisor.

Definition 1.10 (Integral Domains)

A non-trivial and commutative ring R is an *integral domain* (ID) if it has no non-zero zero divisors (i.e. the only zero divisor is 0).

The prototypical example for an integral domain is $\mathbb{Z}$. Other important examples include $\mathbb{Z}[\sqrt{-d}]$ and the set of algebraic integers.

Definition 1.11 (Algebraic Integers)

Define $\overline{\mathbb{Z}} \subset \mathbb{C}$ to be the set of all *algebraic integers*, where each $\alpha \in \overline{\mathbb{Z}}$ is a (complex) root of some monic[4] polynomial with integer coefficients. In other words, there exists some $d \in \mathbb{N}^*$ and $a_0, \ldots, a_{d-1} \in \mathbb{Z}$ such that $\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_1\alpha + a_0 = 0$.

[4] leading coefficient is 1

1.4 Polynomial Rings

Definition 1.12

Let R be a non-trivial ring. Define $R[X]$, the *polynomial ring* over R with variable X, as

$$R[X] := \{a_0 + a_1X + \cdots + a_nX^n : n \in \mathbb{N}, a_0, \ldots, a_n \in R\}$$

where $X \in R$ is a distinguished element which commutes with every element of $R[X]$. We also require that if $a_0 + a_1X + \cdots + a_nX^n = 0_R$, then $a_0 = \cdots = a_n = 0_R$.
For multiple variables $X_1, \ldots, X_k$, we define recursively:

$$R[X_1, \ldots, X_k] := R[X_1, \ldots, X_{k-1}][X_k]$$

Note that R is a subring of $R[X]$.

2 Ideals and Quotients

Definition 2.1 (Ideals)

Let R be a ring. An *ideal* in R is a subgroup I of the additive group of R that is closed under multiplication by all elements of R. In other words, $\forall x \in I, r \in R : rx, xr \in I$. For non-commutative rings, we distinguish between *left ideals* and *right ideals*.

Definition 2.2 (Ideal Generation)

Let R be a ring and $x \in R$. Define the ideal *generated by* x as

$$\langle x \rangle := \{r_1 x s_1 + \cdots + r_n x s_n : n \in \mathbb{N}, r_1, \ldots, r_n, s_1, \ldots, s_n \in R\}$$

and for $x_1, \ldots, x_n \in R$, define the ideal[5] *generated by* $x_1, \ldots, x_n$ as

$$\langle x_1, \ldots, x_n \rangle := \langle x_1 \rangle + \cdots + \langle x_n \rangle$$

For an ideal I in R, we say I is *principal* if $\exists x \in R : I = \langle x \rangle$, and we say I is *finitely generated* if $\exists x_1, \ldots, x_n \in R : I = \langle x_1, \ldots, x_n \rangle$.

[5] We will later show why these are indeed ideals.

For any ring R, we have that $\{0\}$ and R are ideals, and we name them the *zero ideal* and *unit ideal* respectively.[6] Since any non-zero element of a field is a unit, a field only has two ideals.

[6] Since they are generated by zero and a unit respectively — observe: $r = rx^{-1}x = xx^{-1}r$.

Example 2.1

Let R be a ring and $x \in R$. Rx is a left ideal, xR is a right ideal, and $\langle x \rangle$ is an ideal.
TODO: why this is not equal to RxR and is that an ideal or not.

Example 2.2

Let R be a ring and $I_1, \ldots, I_n$ be (resp. left, right) ideals in R. Then $I_1 + \cdots + I_n$ and $\cap_{j=1}^{n} I_j$ are both (resp. left, right) ideals in R.

Definition 2.3

An ideal I is *proper* if $1 \notin I$, or equivalently, $I \neq R$.
An ideal I is *prime* if it is proper and whenever $ab \in I$ we have either $a \in I$ or $b \in I$.
An ideal I is *maximal* if it is proper and whenever $I \subseteq J \subseteq R$ for some ideal J, we have $I = J$ or $J = R$.

2.1 Quotient Rings

Theorem 2.1

Let R be a ring and $I \subseteq R$ be an ideal. Then the commutative group R/I, endowed with a multiplication

Proposition 2.2

Let R be a commutative ring and I an ideal in R. Then I is prime iff R/I is an integral domain. In particular, R is an integral domain iff $\{0_R\}$ is prime.

Proposition 2.3

Let R be a commutative ring and I an ideal in R. Then I is maximal iff R/I is a field.

2.2 The Chinese Remainder Theorem

2.3 First Isomorphism Theorem

2.4 Field Extensions

Definition 2.4

We say $\mathbb{K}$ is a *field extension* of $\mathbb{F}$ if $\mathbb{K}$ is a field and $\mathbb{F}$ is its subfield.
The *degree* of such a field extension, denoted by $|K : F|$, is the dimension of K/F.

Definition 2.5

Given a field extension $\mathbb{K}$ of $\mathbb{F}$ and let $\alpha \in \mathbb{K}$. We say α is $\mathbb{F}$-*algebraic* if it is the root to some $p \in \mathbb{F}[X]^*$, otherwise we say α is $\mathbb{F}$-*transcendental*.

Theorem 2.4 (Tower law)

Suppose $\mathbb{L}$ is a field extension of $\mathbb{K}$, and $\mathbb{K}$ is a field extension of $\mathbb{F}$. Then $\mathbb{L}$ is a field extension of $\mathbb{F}$, and $|L : F| = |L : K||K : F|$, provided the degrees are finite.

3 Divisibility

Definition 3.1 (Divisor)

For a commutative ring R and some $a, b \in R$, we say a is a *divisor* of b, or a *divides* b, or b is a *multiple* of a, and write $a \mid b$, if any of the following:

(i) $\exists x \in R : b = xa$

(ii) $b \in \langle a \rangle$

(iii) $\langle b \rangle \subseteq \langle a \rangle$

We say a and b are *associates*, and write $a \sim b$, if $a \mid b$ and $b \mid a$.

The relation $\mid$ is a preorder since it is both reflexive and transitive. The relation $\sim$ is an equivalence relation

In a field, every non-zero element divides every other non-zero element (guaranteed by invertibility and closeness of multiplication), so all non-zero elements are associates of each other.

3.1 Factorization

Definition 3.2 (Irreducibles)

Let R be a ring. We say a non-zero element $x \in R$ is *irreducible* if $x \not\sim 1$ and $\forall a \in R : a \mid x \implies (a \sim x) \vee (a \sim 1)$.

Irreducibility is preserved within $\sim$ equivalence classes.

Definition 3.3 (Primes)

Let R be a ring. We say $x \in R$ is *prime* if $x \not\sim 1$ and $\forall a, b \in R : x \mid ab \implies (x \mid a) \vee (x \mid b)$.

Primes are what ensures uniqueness of factorization.

In an integral domain, every prime is an irreducible, but the converse is not true.

3.2 Euclidean Domains

Definition 3.4 (Euclidean Functions)

A *Euclidean function* on an integral domain R is a function $f : R^* \to \mathbb{N}$ such that for any $a, b \in R^*$,

(i) $a \mid b \implies f(a) \leqslant f(b)$

(ii) $\exists q, r \in R : a = bq + r$ and either $r = 0$ or $f(r) < f(b)$

Definition 3.5 (Euclidean Domains)

An integral domain R is a *Euclidean domain* (ED) if R can be equipped with a Euclidean function.

3.3 Unique Factorization Domains

Another property of the integers that ensures factorization into primes is that we cannot divide an integer indefinitely. We will formalize and generalize this intuition.

Definition 3.6

An integral domain R has the *ascending chain condition on principal ideals* (ACCP) if for every sequence $(d_n)_{n=0}^{\infty}$ where $\forall n \in \mathbb{N} : d_{n+1} \mid d_n$, there exists some $N \in \mathbb{N}$ such that $\forall n \geqslant N : d_n \sim d_N$. In other words, every ascending chain is eventually constant.

Proposition 3.1

Let R be a Bézout domain. Then R has the ACCP iff R is a PID.

Proof. ($\Rightarrow$) Suppose R has the ACCP. AFSOC that I is an non-principal ideal in R. Let $d_0 \in I$, we can then construct a chain of elements of I iteratively as follows: suppose we have $d_0, \ldots, d_n \in I$, then there exists $d \in I \setminus \langle d_n \rangle$ since I is not principal. Since R is Bézout, there exists d_{n+1} such that $\langle d_{n+1} \rangle = \langle d, d_n \rangle \subset I$
($\Leftarrow$) Suppose R is a PID. $\square$

Lemma 3.2

Suppose R is an integral domain with the ACCP. Then every $x \in R^*$ has a factorization into irreducibles.

Definition 3.7

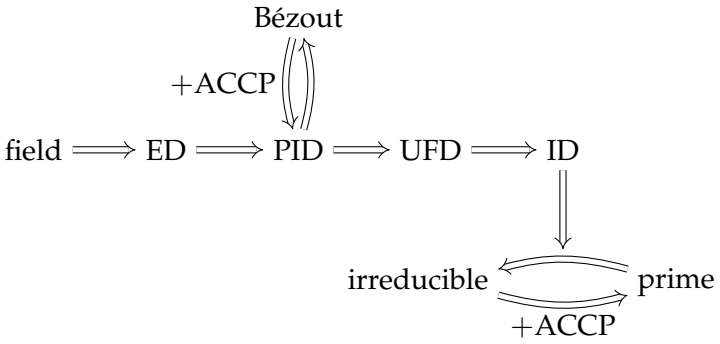
A *unique factorization domain* (UFD) is an integral domain in which every $x \in R^*$ has a unique factorization into irreducibles.

Theorem 3.3

Every PID is a UFD.

Proof. Let R be a PID. Then R has the ACCP, and by Lemma 3.2, we know that every $x \in R^*$ has a factorization into irreducibles. XXXX □

Finally, we summarize the relationships between a few key concepts in the graph below.



Part II

Modules

4 Modules

Modules can be seen as a generalization of vector spaces. Modules are to rings as vector spaces are to fields. Over the course of this part of the note, we will revisit many familiar concepts from vector spaces and apply them to modules.

Definition 4.1 (Modules)

Let R be a ring. An *R-module* is an Abelian group $(M, +)$ with a binary operation $\cdot : R \times M \to M$ called the *scalar multiplication* of R on M, it satisfies the following for any $r, s \in R$ and $x, y \in M$:

(i) $1 \cdot x = x$

(ii) $r \cdot (s \cdot x) = (rs) \cdot x$

(iii) $(r + s) \cdot x = (r \cdot x) + (s \cdot x)$

(iv) $r \cdot (x + y) = (r \cdot x) + (r \cdot y)$

4.1 Linear Maps

Definition 4.2 (Linear Maps)

Let M, N be R-modules. A map $\phi : M \to N$ is an *R-linear map* if it is a group homomorphism[7] with $\forall x \in M, r \in R : \phi(r \cdot x) = r \cdot \phi(x)$.

[7] Recall: $\phi(x + y) = \phi(x) + \phi(y)$. This implies it maps 0_M to 0_N and maps inverses to inverses.

Definition 4.3 (Submodules)

Let M be an R-module. An R-module N is a *submodule* of M, written as $N \leqslant M$, if the inclusion map $\iota : N \to M; x \mapsto x$ is a well-defined R-linear map. Further, if $N \neq M$, we say N is a *proper submodule*.

Proposition 4.1 (Submodule Test)

Let M be an R-module, and let $N \subseteq M$ be non-empty. If for any $x, y \in N$ and $r \in R$ there is $x + y \in N$ and $rx \in N$, then N is a submodule of M (with addition on M and scalar multiplication of R on M restricted to well-defined operations on N).

4.2 Isomorphisms

Definition 4.4 (Linear Isomorphism)

Let M, N be R-modules. A map $\phi : M \to N$ is an *R-linear isomorphism* if it is R-linear and has an R-linear inverse.

Theorem 4.2 (First isomorphism theorem for modules)

Let M, N be R-modules and $\phi : M \to N$ be R-linear. Then $\ker\phi \leqslant M$ and $\operatorname{Im}\phi \leqslant N$, and the map

$$\widetilde{\phi} : M/\ker\phi \to N;\ x + \ker\phi \mapsto \phi(x)$$

is an injective R-linear map. In particular, $\operatorname{Im}\phi \cong M/\ker\phi$.

5 Free Modules

Definition 5.1 (Generated Modules)

For an R-module M and some $\Lambda \subseteq M$, define the *module generated by* Λ as

$$\langle\Lambda\rangle := \{r_1 \cdot x_1 + \cdots + r_n \cdot x_n : n \in \mathbb{N}, x_1, \ldots, x_n \in \Lambda, r_1, \ldots, r_n \in R\}$$

Similarly, for $x_1, \ldots, x_n \in M$, define

$$\langle x_1, \ldots, x_n\rangle = \{r_1 \cdot x_1 + \cdots + r_n \cdot x_n : r_1, \ldots, r_n \in R\} = \langle\{x_1, \ldots, x_n\}\rangle$$

Both $\langle\Lambda\rangle$ and $\langle x_1, \ldots, x_n\rangle$ are submodules of M.

We can again refer to vector spaces for analogy. For any $\mathbb{F}$-module V, the submodule generated by $\Lambda \subseteq V$ is just the subspace spanned by Λ. Note also that any R-module M is generated by M.

Definition 5.2

Let M be an R-module. We say M is *finitely generated* if M can be generated by some finite set Λ. We say M is *cyclic* if M can be generated by a set of size 1.
If $\mathcal{E} \subset M$ generates M and no proper subset of $\mathcal{E}$ generates M, then $\mathcal{E}$ is a *minimal generating set*.

We have that for any ring R, the R-module R is cyclic (generated by 1), and for any submodule $K \leqslant R$, the quotient module R/K is also cyclic (generated by $1 + K$). In fact, every cyclic R-module is isomorphic to R/K for some submodule K.[8]

[8] To see this, consider the map $\phi : R \to M;\ r \mapsto rx$, it is surjective and R-linear, hence by the first isomorphism theorem, such a submodule K exists.

Proposition 5.1

A commutative group M is cyclic if and only if the $\mathbb{Z}$-module M is cyclic.

Definition 5.3

For an R-module M, a set $\mathcal{E} \subseteq M$ is a *minimal generating set* if $\mathcal{E}$ generates M and no proper subsets of $\mathcal{E}$ generates M.

Importantly, minimal generating sets need not exist, but a finitely generated module must contain a minimal generating set. An example is the

$\mathbb{Z}$-module $\mathbb{Q}$, which is not finitely generated and does not have a minimal generating set. Additionally, minimal generating sets need not be the **smallest** generating sets. For example, both $\{1\}$ and $\{2,3\}$ are minimal generating sets for the $\mathbb{Z}$-module $\mathbb{Z}$, but $\{2,3\}$ is larger in size.

5.1 Linear Independence

Definition 5.4

For an R-module M and $r_1 \ldots, r_n \in R$, we say $x_1, \ldots, x_n \in M$ are *R-linearly independent* if $r_1 \cdot x_1 + \cdots + r_n \cdot x_n = 0_M$ implies $r_1 = \cdots = r_n = 0_R$.

Definition 5.5

Let M be an R-module, then $\mathcal{E}$ is a *basis* of M if it is a linearly independent generating set for M. A module with a basis is *free*. In particular, all bases are minimal generating sets.[9]

[9] The converse is not true! $\{2,3\}$ is minimal generating, but not a basis for the $\mathbb{Z}$-module $\mathbb{Z}$.

6 Presentations

Note that for a finitely generated module, its quotient is also finitely generated, but it is not true for submodules. As an example, $\overline{Z}$ is finitely generated (by ???) but

Definition 6.1

An R-module M has a *finite presentation* with *presentation matrix* $A \in M_{m,n}(R)$ if there is an R-linear isomorphism $\Phi : R^n / R^n A \to M$.

7 Smith Normal Form

7.1 Elementary Operations

There are 3 kinds of elementary operations that can be applied to matrices in $M_{n,m}(R)$, they are transvections, dilations, and interchanges.

Note we write I_n for the identity matrix of size n, and write $E_n(i,j)$ for the $n \times n$ matrix with all 0's except $e_{i,j} = 1$. Additionally, for $A \in M_{n,m}(R)$, we write $c_1, \ldots c_m$ for its columns and $r_1, \ldots, r_n$ for its rows.

Definition 7.1 (Transvections)

Let $\lambda \in R$ and $1 \leqslant i, j \leqslant m$ with $i \neq j$. Define

$$T_m(i, j; \lambda) := I_m + \lambda \cdot E_m(i, j)$$

Given $A \in M_{n,m}(R)$, the effect of $AT_m(i, j; \lambda)$ is λ times the i^{th} column added to the j^{th} column, written as

$$A \xrightarrow{c_j \mapsto c_j + c_i\lambda} AT_m(i, j; \lambda)$$

and the effect of $T_n(i, j; \lambda)A$ is λ times the j^{th} row added to the i^{th} row, written as

$$A \xrightarrow{r_i \mapsto r_i + \lambda r_j} T_n(i, j; \lambda)A$$

Definition 7.2 (Dilations)

Let $u \in U(R)$ and $1 \leqslant i \leqslant m$. Define

$$D_m(i; u) := I_m + (u - 1) \cdot E_m(i, i)$$

Definition 7.3 (Interchanges)

Let $1 \leqslant i, j \leqslant m$. Define

$$S_m(i, j) := I_m - E_m(i, i) - E_m(j, j) + E_m(i, j) + E_m(j, i)$$

Definition 7.4

Let $A, B \in M_{n,m}(R)$. We say A and B are *equivalent by elementary operations* and write $A \sim_{\mathcal{E}} B$ if there exists some $A = A_0 \to \cdots \to A_k = B$ generated by subsequently applying only elementary row or column operations.
We say A and B are *equivalent* and write $A \sim B$ if there exists matrices $S \in \mathrm{GL}_n(R), T \in \mathrm{GL}_m(R)$ such that $A = SBT$.
In a field $\mathbb{F}$, we say $A, B \in M_n(\mathbb{F})$ are *similar* if there exists $P \in \mathrm{GL}_n(\mathbb{F})$ such that $A = P^{-1}BP$.

We have that $\sim_{\mathcal{E}}$ implies $\sim$, and similar also implies $\sim$. In general, the group generated by elementary operations is a proper subgroup of the general linear group.

Example 7.1

Let $A, B \in M_{n,m}(R)$. TODO similar matrices

Theorem 7.1

Let R be a Euclidean domain. Then every $A \in M_{n,m}(R)$ is equivalent by elementary operations to a diagonal matrix.

7.2 Smith Normal Form

Definition 7.5

We say that $A \in M_{n,m}(R)$ is in *Smith normal form* over R if it is diagonal and for all $1 \leqslant i < \min(n, m)$ we have $A_{i,i} \mid A_{i+1,i+1}$.

Lemma 7.2

Let R be a Bézout domain. Then every diagonal matrix $A \in M_{n,m}(R)$ is equivalent by elementary operations to a matrix in Smith normal form.

Theorem 7.3

Let R be a Euclidean domain. Then every matrix $A \in M_{n,m}(R)$ is equivalent by elementary operations to a matrix in Smith normal form.

Proof. This follows directly from Theorem 7.1 and Lemma 7.2. □

7.3 Applications

Theorem 7.4

Let R be an Euclidean domain and suppose M is generated by $x_1, \ldots, x_n$. Then there exists $a_1 \mid \ldots \mid a_n \in R$ and matrix $Q \in \mathrm{GL}_n(R)$ such that

$$\begin{aligned} \frac{R}{\langle a_1 \rangle} \oplus \cdots \oplus \frac{R}{\langle a_n \rangle} &\to M \\ (r_1 + \langle a_1 \rangle, \ldots, r_n + \langle a_n \rangle) &\mapsto (rQ).x_1 + \cdots + (rQ).x_n \end{aligned}$$

gives a well-defined R-linear isomorphism.