Algebra III

Kexing Ying

July 24, 2021

N.B. this course has large overlap with the second year course *Groups and Rings* in particular, the ring subsection. Thus, most revisited proofs are simply omitted or replaced with a hint.

Contents

1 Rings

We will in this section recall some fundamental definitions about rings which we will study throughout the course.

Definition 1.1 (Ring)**.** A ring R is a set together with two distinct elements $0_R, 1_R$, and two binary operations $+_R, \times_R : R^2 \to R$ such that

- $(R, +_R)$ is an additive abelian group with identity 0_R;
- $(R, \times_R)$ is a multiplicative abelian monoid with identity 1_R;
- $\times_R$ distributes over $+_R$, i.e. for all $r, s, t \in R$,

$$(r +_R s) \times_R t = r \times_R t +_R s \times_R t,$$

and

$$r \times_R (s +_R t) = r \times_R s +_R r \times_R t.$$

We note that there is some ambiguity in the literature in the definition of a ring, and in particular, some might call the definition above as a commutative unital ring. We will in this course mostly consider ourselves with this definition, though we might later consider non-commutative rings.

Definition 1.2 (Field)**.** A field F is a ring is for all $f \in F \setminus \{0_F\}$, there exists some $f^{-1} \in F$ such that $f \times_F f^{-1} = 1_F$.

We will simply drop the subscript from the operations and the elements from these definitions whenever there is no confusion.

Recall that one method of constructing a ring from another is the polynomial ring. Let R be ring, then a polynomial on X is a sum

$$\sum_{n=0}^{\infty} a_n X^n$$

for some $(a_n)_{n \in \mathbb{N}} \subseteq R$ where all but finitely many a_i are zero. We say $P(X) = \sum_{n=0}^{\infty} a_n X^n$ has degree d if d is the largest number such that $a_d \neq 0$.

Definition 1.3 (Polynomial Ring)**.** Given a ring R, the polynomial ring $R[X]$ is the set of polynomials equipped with the operations $+_{R[X]}$ and $\times_{R[X]}$ such that

$$\sum_{n=0}^{\infty} a_n X^n +_{R[X]} \sum_{n=0}^{\infty} b_n X^n = \sum_{n=0}^{\infty} (a_n + b_n) X^n,$$

and,

$$\sum_{n=0}^{\infty} a_n X^n \times_{R[X]} \sum_{n=0}^{\infty} b_n X^n = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} a_i b_{n-i} \right) X^n.$$

It is not difficult to see that the ring axioms are satisfied and in fact, it is possible to construct polynomial rings with infinite degrees, though this shall not be considered in this course. An equivalent way of considering elements of polynomial rings is to see them as sequences with finite non-zero elements.

One may adjoin a polynomial ring with another variable, that is $R[X][Y]$ and by writing out the elements, we see that $R[X][Y] \cong R[Y][X]$ and we may instead write $R[X, Y]$ with no ambiguity.

1.1 Subrings and Extensions

Definition 1.4 (Subring)**.** A subring of the ring R is a subset of R containing $0, 1$ and is closed under $+$ and $\times$.

It is clear that a subring of a ring is a ring itself with the inherited operations.

Proposition 1.1. If S, T are subrings of the ring R, then so is $S \cap T$.

Definition 1.5. Given a subring S of R, $S[\alpha]$ for some $\alpha \in R$ is the subset of R consisting of all elements of R that can be expressed as $r_0 + r_1\alpha + \cdots + r_n\alpha^n$ for $r_i \in S$ and $n \in \mathbb{N}$. We call this process the adjoining of S with α.

Clearly $S[\alpha]$ contains 0 and 1 (as $S \subseteq S[\alpha]$) and is closed under $+$ and $\times$, and thus, is a subring of R.

An important example of the above construction is the following. Consider $\mathbb{Z} \subseteq \mathbb{C}$, we have $\mathbb{Z}[i]$ constructed through the definition above is known as the Gaussian integers is a subring of $\mathbb{C}$ consisting of all elements of the form $a+bi$ for $a, b \in \mathbb{Z}$. To see this, consider if $X^2 - rX - s$ is a polynomial of integer coefficients with complex root $\alpha \notin \mathbb{Z}$, then, we may consider $\mathbb{Z}[\alpha]$. As $\alpha^2 - r\alpha - s = 0$, we obtain $\alpha^2 = r\alpha + s$ and thus, for all $r_0 + r_1\alpha + \cdots + r_n\alpha^n \in \mathbb{Z}[\alpha]$,

$$\begin{aligned} r_0 + r_1\alpha + r_2\alpha^2 + \cdots + r_n\alpha^n &= r_0 + r_1\alpha + r_2(r\alpha + s) + \cdots \\ &= (r_0 + r_2 s + \cdots) + (r_1 + r_2 r + \cdots)\alpha. \end{aligned}$$

Hence, all elements of $\mathbb{Z}[\alpha]$ are of the form $a + b\alpha$ for $a, b \in \mathbb{Z}$.

On the other hand, if we consider $\mathbb{Z}[\pi] \subseteq \mathbb{C}$, as π is not an algebraic number, for all $P(X) \in \mathbb{Z}[X] \setminus \{0\}$, $P(\pi) \neq 0$. Thus, if $P(X), Q(X)$ are polynomials such that $P(\pi) = r_0 + r_1\pi + \cdots + r_n\pi^n = s_0 + s_1\pi + \cdots + s_m\pi^m = Q(\pi)$, WLOG. $n \leq m$ we have $0 = (s_0 - r_0) + (s_1 - r_1)\pi + \cdots + (s_n - r_n)\pi^n + s_{n+1}\pi^{n+1} + \cdots + s_m\pi^{m+1}$, implying $s_i = r_i$ for all $i = 1, \cdots, n$ and $s_i = 0$ for $i > n$, we have $P = Q$. Hence, $\mathbb{Z}[\pi] \cong \mathbb{Z}[X]$.

Proposition 1.2. If R is a subring of S, then $R[\alpha]$ for some $\alpha \in S$ is the intersection of all subrings of S containing $R \cup \{\alpha\}$.

Proof. Since $R[\alpha]$ contains both R and α, we have

$$\bigcap \{U \mid R \cup \{\alpha\} \subseteq U \leq S\} \subseteq R[\alpha].$$

On the other hand, for all subrings U containing $R \cup \{\alpha\}$, $R[\alpha] \subseteq U$ as U is closed under $+$ and $\times$. Thus,

$$\bigcap \{U \mid R \cup \{\alpha\} \subseteq U \leq S\} = R[\alpha].$$

□

Definition 1.6 (Integral Domain)**.** A ring R is an integral domain if for all $r, s \in R$, $rs = 0$ implies $r = 0$ or $s = 0$.

In particular, we say $r \in R$ is a zero divisor if there exists a $s \in R \setminus \{0\}$ such that $rs = 0$. Thus, an integral domain is simply a ring with no zero divisors.

Definition 1.7 (Field of Fractions)**.** For R an integral domain, then the field of fractions of R denoted $\mathrm{Frac}(R)$, is $R \times R \setminus \{0\}$ quotiented by the equivalence class

$$(a, b) \sim (r, s) \iff as = br.$$

We write a/b as a representative of the equivalence class $[a, b]$.

We may equip the field of fractions of R with addition and multiplication such that for $a/b, r/s \in \mathrm{Frac}(R)$

$$\frac{a}{b} + \frac{r}{s} = \frac{ad + bc}{bd} \text{ and } \frac{a}{b} \times \frac{r}{s} = \frac{ar}{bs}.$$

It is routine to check these operations are well-defined and that the ring axioms are satisfied. Furthermore, as the name suggests, $\mathrm{Frac}(R)$ is a field and for all $a/b \neq 0$, $(a/b) \times (b/a) = 1$.

Definition 1.8 (Multiplicative System)**.** A set $S \subseteq R$ is a multiplicative system if $1 \in S, 0 \notin S$ and is closed under multiplication.

Definition 1.9. Let R be a ring and $S \subseteq R$ be a multiplicative system. Then $S^{-1}R$ is $R \times S$ quotiented by the equivalence class

$$(a, b) \sim (r, s) \iff as = br$$

for $a, r \in R, b, s \in S$.

Similarly, we may equip $S^{-1}R$ with addition and multiplication such that $S^{-1}R$ is a subring of $\mathrm{Frac}(R)$.

It is possible to use this construction on rings which are not integral domains, though in that case, the equivalence class is more subtle as division by a zero divisor will introduces other elements into the subring. This will be explored later in this course.

1.2 Homomorphisms and Ideals

We recall the definition of ring homomorphism and some related results (whose proofs omitted or shortened).

Definition 1.10 (Ring Homomorphism)**.** Given R, S rings, a ring homomorphism from R to S is a map $f : R \to S$ such that for all $a, b \in R$,

- $f(1_R) = 1_S$;
- $f(a +_R b) = f(a) +_S f(b)$;
- $f(a \cdot_R b) = f(a) \cdot_S f(b)$.

If f is a bijection then we say f is an isomorphism.

Automatically, it is not difficult to see that condition 2 implies $f(0_R) = 0_S$ and from this we can deduece properties such as $f(-x) = -f(x)$.

Proposition 1.3. The image of a ring homomorphism $f : R \to S$ is a subring of S.

As we have seen in other contexts, the notion of an isomorphism is often defined to be a invertible structure preserving map. Though in some contexts, such as topological spaces, bijection is often not enough and we will require the inverse to be structure preserving. The following proposition shows that these two cases are equivalent for rings.

Proposition 1.4. If $f : R \to S$ is an isomorphism, then $f^{-1} : S \to R$ is a ring homomorphism.

Proof. For all $a, b \in S$, we have $f^{-1}(a+b) = f^{-1}(f(f^{-1}(a)) + f(f^{-1}(b))) = f^{-1}(f(f^{-1}(a) + f^{-1}(b))) = f^{-1}(a) + f^{-1}(b)$. Similar argument for the other conditions. □

Proposition 1.5. There exist a unique homomorphism from $\mathbb{Z}$ to R for all ring R.

Proof. Clear by considering if $f : \mathbb{Z} \to R$ is a homomorphism, $f(n_{\mathbb{Z}}) = n_{\mathbb{Z}} \cdot 1_R$. □

Proposition 1.6. Given a ring R and $\alpha \in R$, there exists a unique homomorphism $f : R[X] \to R$ such that $f(X) = \alpha$ and $f\mid_R = \mathrm{id}_R$. This homomorphism is called the evaluation map at α and we denote it as ev_α.

Proof. Clear and as the name suggests, the unique map is

$$\mathrm{ev}_\alpha(P(X)) = P(\alpha),$$

for all $P \in R[X]$. □

More generally, if $f : R \to S$ is a homomorphism and $\alpha \in S$, there exists a unique $\mathrm{ev}_{f,\alpha} : R[X] \to S$ such that $\mathrm{ev}_{f,\alpha}\mid_R = f$ and $\mathrm{ev}_{f,\alpha}(X) = \alpha$. Furthermore, if f is simply the inclusion map from $R \to S$, image of $\mathrm{ev}_{f,\alpha}(X) = \alpha$ is $R[\alpha]$.

Definition 1.11 (Kernel)**.** Let R, S be rings and $f : R \to S$ a ring homomorphism. Then the kernel of f is

$$\ker f := \{r \in R \mid f(r) = 0_S\}.$$

Proposition 1.7. A ring homomorphism $f : R \to S$ is injective if and only if $\ker f = \{0\}$.

Definition 1.12 (Ideal)**.** Given a subset I of a ring R, then I is said to be an ideal if

- $0_R \in I$;
- for all $a, b \in I$ then $a + b \in I$;
- for all $a \in I$, $r \in R$, $ra \in I$.

Definition 1.13. The following ideals are important enough to warrant a definition.

- $\{0_R\} \subseteq R$ is the zero ideal;
- $R \subset R$ is the unit idea;
- for all $r \in R$, $\langle r \rangle := \{rs \mid s \in R\}$ is the principal ideal generated by r.

Proposition 1.8. Every ideal of $\mathbb{Z}$ is principle.

Proposition 1.9. In intersection of ideals is an ideal. Similarly, the sum of two ideals, i.e. if I, J are ideals, then $\{i + j \mid i \in I, j \in J\}$ is an ideal.

Definition 1.14. Let R be a ring and $r_1, \cdots, r_n \in R$. Then the ideal generated by $r_1, \cdots, r_n$ is

$$\langle r_1, \cdots, r_n \rangle := \{r_1 s_1 + \cdots r_n s_n \mid s_i \in R\}.$$

It is clear that the ideal generated by $r_1, \cdots, r_n$ is the smallest ideal containing $r_1, \cdots, r_n$.

Definition 1.15. The produce of ideals I and J is the ideal which elements are of the form $i_1 j_1 + \cdots + i_n j_n$ for all $i_1, \cdots i_n \in I$, $j_1, \cdots, j_n \in J$.

For ideals I, J, we see that $IJ \subseteq I \cap J$ though they are not necessary equal (consider $\langle 2 \rangle \langle 2 \rangle = \langle 4 \rangle$ thought $\langle 2 \rangle \cap \langle 2 \rangle = \langle 2 \rangle$).

Proposition 1.10. If ideals I, J satisfy $I + J = \langle 1 \rangle$, then $I \cap J = IJ$.

As with other mathematical objects, we would like to construct a quotient object for the rings. The equivalence relation we shall quotient on it the following. Let $I \subseteq R$ be an ideal and we define say $r \equiv s \mod I$ for $r, s \in R$ if $r - s \in I$. It is not difficult to check that $\equiv_I$ is a equivalence relation and thus, we may take a quotient of R with respect to this equivalence relation and we denote the equivalence classes with $r + I$.

Definition 1.16 (Quotient Ring)**.** Given R a ring and I an ideal of R, then the quotient ring of R by I is the ring with the underlying set

$$R/I := R/\equiv_I = \{r + I \mid r \in R\},$$

where $0_{R/I} = 0_R + I$, $1_{R/I} = 1_R + I$, and for all $r + I, s + I \in R/I$, $(r + I) + (s + I) = (r + s) + I$ and $(r + I) \cdot (s + I) = rs + I$.

Definition 1.17 (Quotient Map)**.** Given R a ring and I an ideal of R, the quotient map is then the surjective ring homomorphism $q : R \to R/I : r \mapsto r + I$.

It is clear that $\ker q = I$.

A more modern interpretation of the quotient ring is by defining it as an object satisfying its universal property. In particular, the ring R/I, taken together with a ring homomorphism $q : R \to R/I$, has the following universal property.

Proposition 1.11. If $f : R \to S$ is a ring homomorphism such that $I \subseteq \ker f$, then there exists a unique ring homomorphism $\tilde{f} : R/I \to S$ such that for all $r \in R$, $\tilde{f}(r + I) = f(r)$.

Essentially, the universal property states that there exists a unique $\tilde{f}$ such that the following diagram commutes.

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[d, "q"'] & S \\
R/I \arrow[ur, dashed, "\tilde{f}"'] &
\end{tikzcd}$$

Proof. Uniqueness is clear and thus we will show $\tilde{f}$ is well-defined and is a ring homomorphism. Let $r \equiv s \mod I$, and will show $f(r) = f(s)$. Indeed, since $r - s \in I$, we have $r - s \in \ker f$ and so, $f(r) - f(s) = f(r - s) = 0$, hence $f(r) = f(s)$ and $\tilde{f}$ is well-defined. Now, let $r + I, s + I \in R/I$, we have

$$\tilde{f}((r + I) + (s + I)) = \tilde{f}((r + s) + I) = f(r + s) = f(r) + f(s) = \tilde{f}(r + s) + \tilde{f}(s + I),$$

hence by similar argument for multiplication, we have $\tilde{f}$ is a ring homomorphism. □

As an example consider the surjective map $\mathbb{R}[X] \to \mathbb{C}$ which is id on $\mathbb{R}$ and sends X to i. Then this map have kernel $\{P \in \mathbb{R}[X] \mid P(i) = 0\} = \langle X^2 + 1 \rangle$. Thus, we have the diagram

$$\begin{tikzcd}
\mathbb{R}[X] \arrow[r] \arrow[d, "q"'] & \mathbb{C} \\
\mathbb{R}[X]/\langle X^2 + 1 \rangle \arrow[ur, leftrightarrow] &
\end{tikzcd}$$

where the pull-back map is an isomorphism as the map itself is surjective while injectivity follows as we have quotiented out its kernel. As we shall see, whenever we have one field inside another, there is a construction similar this such that we can construct the larger field from the smaller field.

By recalling the evaluation map, if $\alpha \in R$, by the above process, we see that

$$R[X]/I \cong R[\alpha],$$

where I is the kernel of the evaluation map at α.

Definition 1.18. Let R be a ring and I an ideal of R. Then we say I is a prime ideal if R/I is an integral domain. Furthermore, we say I is a maximal ideal if R/I is a field.

Since fields are integral domains, maximal ideals are prime.

Proposition 1.12. *An ideal I of R is prime if and only if for all $rs \in I$, either $r \in I$ or $s \in I$.*

Proposition 1.13. *An ideal I of R is maximal if and only if the only ideal of R containing I is I or the unit ideal R.*

Proof. Follows by considering that a ring is a field if and only if its only ideals are the zero or the unit ideal, and the image of an ideal by a surjective homomorphism is also an ideal. □

1.3 Factorization and PIDs

Definition 1.19 (Unit)**.** Let R be a integral domain, then $R^\times$ is the set of elements r of R such that there exists some $r' \in R$ such that $rr' = 1$. If $r \in R^\times$, then we call r a unit.

Definition 1.20 (Divides)**.** Let $r, s \in R$, we say r divides s if $s \in \langle r \rangle$.

It is clear that a unit divides any element. Indeed, if $u \in R^\times$ and $s \in R$ such that $uu' = 1$, then $s = (su')u$ implying $s \in \langle u \rangle$.

Definition 1.21 (Associate)**.** An associate of $r \in R$ is an element ur of r with $u \in R^\times$.

Definition 1.22 (Irreducible)**.** An element $r \in R$ is irreducible if $r \neq 0$, $r \notin R^\times$ and the only dividors of r are units and associates of r.

Definition 1.23 (Unique Factorization Domain)**.** A ring R is a unique factorization domain (UFD) if it is a integral domain and

- for all non-zero, non-unit element of R is a product of finitely many irreducibles.

- for all $r \in R$ non-zero, non-unit such that

  $$r = p_1 \cdots p_s = q_1 \cdots q_t,$$

  where p_i, q_i are irreducibles, then $s = t$ and after reordering, p_i is an associate of q_i.

Some typical examples of UFDs are $\mathbb{Z}, \mathbb{F}[X], \mathbb{Z}[X], \cdots$ (where $\mathbb{F}$ is a field), though it is more challenging to come up with counter-examples. Consider the ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$, define

$$N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z} : z \mapsto z\bar{z}.$$

It is easy to see that N is multiplicative, and thus, if $u \in \mathbb{Z}[\sqrt{-5}]$ is a unit such that $uu' = 1$, we have

$$N(u)N(u') = N(uu') = N(1) = 1,$$

implying $N(u) = \pm 1$ and so $u = \pm 1$. Then, as ± 1 are the only units of $\mathbb{Z}[\sqrt{-5}]$, we have $3 \cdot 2 = (1 - \sqrt{-5})(1 + \sqrt{-5})$ are products of non-units which are not associate with each other. Hence, to show that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD it suffices to show that the factors are irreducibles. To show this, one again use N by plugging the factors.

Let us construct a ring such that the first condition of UFD fails, i.e. a ring for which a non-zero, non-unit element is not a product of finitely many irreducibles. Define

$$\mathbb{C}[t^{\mathbb{Q}_{\geq 0}}] := \left\{ \sum_{i=0}^{r} c_i t^{a_i} \mid c_i \in \mathbb{C}, a_i \in \mathbb{Q} \right\} = \bigcup_{n=1} \{f^{1/n} \mid f \in \mathbb{C}[X]\}.$$

Then, $\mathbb{C}[t^{\mathbb{Q}_{\geq 0}}]^\times = \mathbb{C}^\times$ and in fact, $\mathbb{C}[t^{\mathbb{Q}_{\geq 0}}]$ does not have any irreducible elements. Let $f \in \mathbb{C}[t^{\mathbb{Q}_{\geq 0}}]^\times$ such that $f = P(t^{1/n})$ and $f^{-1} = Q(t^{1/m})$, then we may write $f = P'(t^{1/(nm)})$ and $f^{-1} = Q'(t^{1/(nm)})$. Hence,

$$1 = P'(t^{1/(nm)})Q'(t^{1/(nm)}) \implies P'Q' = 1 \implies P', Q' \text{ are constants},$$

and so $f \in \mathbb{C}^\times$. On the other hand, if $P(t^{1/n}) \in \mathbb{C}[t^{\mathbb{Q}_{\geq 0}}]$ is irreducible, by the fundamental theorem of algebra, it is a product of linear polynomials implying $P(t^{1/n}) = t^{1/n} - a$ for some $a \in \mathbb{C}$. But, $t^{1/n} - a = (t^{1/(2n)} + \sqrt{a})(t^{1/(2n)} - \sqrt{a})$, a contradiction.

Definition 1.24 (Prime)**.** An element r of a ring R is prime if $\langle r \rangle$ is a prime ideal. Equivalently, r is prime if for all $s, t \in R$, $r \mid st$ implies either $r \mid s$ or $r \mid t$.

Proposition 1.14. Let R be an integral domain in which every element is a finite product of irreducibles. Then every irreducible element of R is prime if and only if for all

$$p_1 \cdots p_s = q_1 \cdots q_t,$$

where p_i, q_i are irreducible, then $s = t$ and after reordering, p_i is an associate of q_i.

Proof. Suppose every irreducible element of R is prime. Then, if

$$p_1 \cdots p_s = q_1 \cdots q_t,$$

where p_i, q_i are irreducible, we have $p_1 \mid q_1, \cdots, q_t$ and so, $p_1 \mid q_i$ for some $i = 1, \cdots, t$, and hence p_i is an associate of q_1. Then, by reordering, we have p_1 and q_1 are associates. Repeating this argument, we may cancel all associates with some terms remaining if $s > t$,

$$p_{t+1} \cdots p_s = 1.$$

But this is a contradiction since then p_{t+1} is a unit and so $s = t$ as required.

Conversely, suppose r is irreducible and $r \mid st$ and so there exists some $rx = st$ for some $x \in R$. Then, we may factor x, s, t into irreducibles such that

$$rp_1 \cdots p_l = q_1 \cdots q_m n_1 \cdots n_k.$$

Then, as such factorizations are unique, r must be an associate of some q_i or n_i which implies that $r \mid s$ or $r \mid t$, so r is prime. □

Proposition 1.15. In an integral domain R, if $r \in R$ is prime, then r is irreducible.

Proof. Suppose otherwise, $r = st$. Then $r \mid st$ but neither $r \mid s$ nor $r \mid t$. □

A counter-example of the reverse is that 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$ but is not a prime.

Definition 1.25 (Principal Ideal Domain)**.** A ring R is a principal ideal domain (PID) if R is an integral domain and every ideal I is principal.

Lemma 1.1. If R is a PID, then any increasing tower of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

is eventually constant, i.e. there exists an $N \in \mathbb{N}$ such that for all $n \geq N$, $I_n = I_N$.

Proof. Let $I = \bigcup_{j=1}^{\infty} I_j$. Since $x, y \in I$, there exists $j, k \in \mathbb{N}$, such that $x \in I_j, y \in I_j$, and so $x, y \in I_{\max\{j,k\}} \implies x + y \in I_{\max\{j,k\}} \subseteq I$. Similarly, by the same argument we have I is closed under multiplication by elements of R. Thus, I is an ideal, and so $I = \langle r \rangle$ is principal. Finally, as $r \in I$, there exists some $N \in \mathbb{N}$ such that $r \in I_N$, and so $I = \langle r \rangle \subseteq I_N$ implying $I = I_N$. □

Lemma 1.2. Let R be a PID, $r \in R$ which is non-zero, non-unit. Then there exists some irreducible $s \in R$ which divides r.

Proof. If r is irreducible, then simply take $s = r$. On the other hand, if r is not irreducible, then there exists r_0, s_0 non-zero, non-associates of r such that $r = r_0 s_0$. If r_0 is irreducible, then we are done while otherwise, we may repeat the process such that $r_0 = r_1 s_1$. This process must terminate since if otherwise, we have

$$\langle r \rangle \subsetneq \langle r_0 \rangle \subsetneq \langle r_1 \rangle \subsetneq \cdots$$

which is non-terminating strictly increasing tower of ideals contradicting our previous lemma. □

Lemma 1.3. Let R be a PID, then any non-zero, non-unit of r factors into irreducibles.

Proof. Similar to before, all factors of r must terminate since otherwise we have produces an non-terminating increasing tower of ideals. □

Theorem 1. Let R be a PID, then R is a UFD.

Proof. We already shown the existence of factorizations and so, it remains to show uniqueness. By proposition 1.14, it suffices to show that every irreducible element of R is prime. Let $r \in R$ be irreducible, $r \mid st$ and $r \nmid s$. Then, since $\langle r, s\rangle$ is principal, there exists some $q \in R$, such that $\langle r, s\rangle = \langle q\rangle$ implying $q \mid r$ and $q \mid s$. But since r is irreducible, either q is an associate of r or a unit. If q is an associate of r, there exists a unit u such that $uq = r$. But $q \mid s$ and so, there exists some $a \in R$, $aq = s$ implying $(au^{-1})r = au^{-1}uq = aq = s$ contradicting $r \nmid s$. Thus, q is a unit and so $\langle r, s\rangle = R$ and there exists some $a, b \in R$ such that $ar + bs = 1$, and so $t = art + bst$. Finally, as $r \mid st$, we have $r \mid art + bst = t$ implying r is prime. □

Corollary 1.1. Let R be a PID, then every non-zero prime ideal of R is maximal.

Proof. Let $I = \langle r\rangle \trianglelefteq R$ be a non-zero prime ideal. Then r is a prime and so, it is irreducible. Now, if $I \leq J = \langle s\rangle$ for some element s, there exists some $t \in R$ such that $st = r$ implying s is a unit or an associate of r. If s is an associate, then there exists some unit u such that $us = r$ and thus, $s = u^{-1}r$ and so $\langle s\rangle \subseteq \langle r\rangle$ implying $\langle s\rangle = \langle r\rangle$. On the other hand if s is a unit, then $s^{-1}s = 1 \in \langle s\rangle$ and so $\langle s\rangle = R$. □

1.4 Euclidean Domains

So far we have developed a nice theory about PIDs though we have yet to have any tools to prove that ring is a PID. We will now develop the notion called Euclidean domains to aid us in this matter.

Definition 1.26 (Euclidean Norm)**.** For integral domain R, a Euclidean norm on R is a function $N : R \to \mathbb{N}$ such that for all $a, b \in R$, $b \neq 0$, there exists $q, r \in R$ such that $a = qb + r$ and either $N(r) < N(b)$ or $r = 0$.

Definition 1.27 (Euclidean Domain)**.** A Euclidean domain is a ring R that admits a Euclidean norm.

Proposition 1.16. Any Euclidean domain R is a PID.

Proof. Let N be the Euclidean norm on R and suppose $I \neq 0$ is an ideal of R. Now since $N(I) \subseteq \mathbb{N}$ is non-empty, $N(I)$ admits some minimal element $k = N(r)$ for some $r \in I$. Suppose $I \neq \langle r\rangle$, then there exists some $s \in I$, $s \notin \langle r\rangle$. Then, by the definition of the Euclidean norm, there exists some $a, b \in R$ such that $s = ar + b$ and either $b = 0$ or $N(b) < N(r)$. But if $b = 0$ then $s = ar$ implying $s \in \langle r\rangle$, so $N(b) < N(r)$. But this contradicts the minimality of $N(r)$ and hence, $I = \langle r\rangle$. □

We see that the notion of an Euclidean norm is very similar to the quotient remainder for the integers, and so it is not very surprising that $\mathbb{Z}$ is a Euclidean domain. In particular, we define $N(n) = |n|$ and for $a, b \in \mathbb{Z}$, $b \neq 0$, we can define

$$q := \left\lfloor \frac{a}{b} \right\rfloor,$$

so $0 \leq \frac{a}{b} - q < 1$, and thus, $0 \leq a - bq < b$ which implies $|a - bq| < |b|$.

A more complicated example is the Gaussian integers $\mathbb{Z}[i]$. Let $N(n + mi) = n^2 + m^2$ and given $x, y \in \mathbb{Z}[i]$, $y \neq 0$, we can define $q' = x/y = a + bi$ for some $a, b \in \mathbb{R}$. Then, defining

$q = a' + b'i$ where $a', b' \in \mathbb{Z}$ such that $|a - a'|, |b - b'| < 1/2$. Finally, by noticing N is multiplicative (as $N(z) = z\overline{z}$), we have

$$N(r) = N(x - qy) = N(y)N\left(\frac{x}{y} - q\right) = N(y)N(q' - q)$$
$$= N(y)(|a - a'|^2 + |b - b'|^2) < \frac{N(y)}{2} < N(y).$$

Thus, $\mathbb{Z}[i]$ is a Euclidean domain.

Given a field $\mathbb{F}$, we can define $N(P) = \deg P$ for $P \in \mathbb{F}[X]$. Then, for $P, S \in \mathbb{F}[X]$, it is not difficult to see that the Euclidean norm conditions hold by long division and induction. A direct corollary of this is that, since $\mathbb{F}[X]$ is a Euclidean domain, it is a PID, and thus, for any irreducible polynomial $P \in \mathbb{F}[X]$, $\langle P \rangle$ is a prime ideal, hence maximal, i.e. by definition $\mathbb{F}[X]/\langle P \rangle$ is a field.

1.5 Chinese Remainder Theorem

Definition 1.28 (Product ring)**.** Let R, S be rings. Then $R \times S$ is the Cartesian product of R and S equipped with the ring structure where addition and multiplication are defined pairwise.

As one might expect, the projection maps from a product ring are ring homomorphisms. On the other hand, the inclusion maps are not ring homomorphisms. In particular, the map

$$i_1 : R \to R \times S : r \mapsto (r, 0), i_2 : S \to R \times S : s \mapsto (0, s),$$

are not ring homomorphisms as they do not map the multiplicative identity to the multiplicative identity of $R \times S$.

We see that the product ring operation is associative, i.e. $(R \times S) \times T \cong R \times (S \times T)$ via the isomorphism $((r, s), t) \mapsto (r, (s, t))$, and we may simply omit the brackets. This argument can be applied analogously to n-fold products.

In general, given a collection of rings $\{R_i\}_{i \in I}$ for some index set I, we may define $\prod_{i \in I} R_i$ to be the set of elements of the form $\{x_i\}_{i \in I}$ such that $x_i \in R_i$. Similarly, we may equip $\prod R_i$ with the ring structure where addition and multiplication are defined pairwise. As before, the projection maps are ring homomorphisms.

This definition of product rings is characterised by the following universal property.

Proposition 1.17. Given a ring S and a collection of rings $\{R_i\}_{i \in I}$. If $f_i : S \to R_1$ is a ring homomorphism for all $i \in I$, then there exists a unique ring homomorphism

$$\prod_{i \in I} f_i : S \to \prod_{i \in I} R_i,$$

such that $f_i = \pi_i \circ (\prod f_i)$ where p_i is the projection map from $\prod R_i$ to R_i.

Proof. Define $\prod_{i \in I} f_i(s) := \{f_i(s)\}_{i \in I} \in \prod_{i \in I} R_i$. It is clear that $\prod_{i \in I} f_i$ is a ring homomorphism and $(\pi_i \circ (\prod_{i \in I} f_i))(s) = \pi_i(\{f_i(s)\}_{i \in I}) = f_i(s)$.

Now, if $g : S \ to \prod_{i \in I} R_i$ is a ring homomorphism such that $\pi_i \circ g = f_i$, then $g(s) = \{f_i(s)\}_{i \in I} = (\prod_{i \in I} f_i)(s)$. Thus, $g = \prod_{i \in I} f_i$. □

The Chinese remainder theorem seeks to solve the question that, if I, J are ideals of the ring R, if $a \in R/I$ and $b \in R/J$, then does there exists some $c \in R$, $c + I = a + I$ and $c + J = b + J$. Furthermore, if such an element exists, how unique is it.

Phrased in a more ring theoretic sense, the existence question asks, if $q_1 : R \to R/I$ and $q_2 : R \to R/J$ are the quotient maps, is (a, b) in the image of $q_1 \times q_2 : R \to R/I \times R/J : r \mapsto (q_1(r), q_2(r))$. On the other hand, the uniqueness question asks if there asks whether or not $q_1 \times q_2$ is injective, and so, it essentially asks what is the kernel of $q_1 \times q_2$.

It is clear that if $q_1 \times q_2(s) = 0$ if and only if $q_1(s) = 0$ and $q_2(s) = 0$ and so, $I \cap J = \ker q_1 \times q_2$. With this in mind, we see that

$$R/I \cap J \hookrightarrow R/I \times R/J$$

is a injection. Sadly, this injection is not a surjection by simply considering the case where $I = J$ and $a \neq b$.

More generally, given $I_1, \cdots, I_r$ is a finite collection of ideals, we have

$$R/\bigcap_{i=1}^{r} I_i \hookrightarrow R/I_1 \times \cdots \times R/I_r,$$

is an injection.

Definition 1.29 (Relatively Prime Ideal)**.** Ideals I, J are relatively prime ideals of R if $I + J = R$.

Theorem 2 (Chinese Remainder Theorem)**.** Let $\{I_i\}_{i=1}^r$ be a finite collection of ideals of R such that $\{I_i\}$ is pairwise relatively prime. Then the map

$$R/\bigcap_{i=1}^{r} I_i \hookrightarrow R/I_1 \times \cdots \times R/I_r,$$

is an isomorphism.

Proof. It suffices to prove surjectivity.

For all i, j, $i \neq j$, as I_i and I_j are pairwise relatively prime, there exists $r_i, \in I_i$ and $r_j, \in I_j$ such that $r_i + r_j = 1$. Thus, $r_i = 1 \mod I_j$ and $r_j = 1 \mod I_i$. Then, for each j, let $f_j = \prod_{k \neq j} r_k$ where r_k is defined as above, we have $f_j = 1 \mod I_j$ since individual $r_k = 1$ mod I_j. On the other hand, for all $k \neq j$, $r_k = 0 \mod I_k$, we have $f_j = 0 \mod I_k$. Finally, for all $s = (s_1, \cdots, s_r) \in R/I_1 \times \cdots \times R/I_r$, choose $\tilde{s}_i$ such that $q_i(\tilde{s}_i) = s_i$. Then, setting $t = f_1\tilde{s}_1 + \cdots + f_r\tilde{s}_r$, we have

$$q_i(t) = q_i(f_1)q_i(\tilde{s}_1) + \cdots + q_i(f_r)q_i(\tilde{s}_r) = 0 + \cdots + 0 + 1 \cdot s_i + 0 + \cdots + 0 = s_i,$$

and so $t \mapsto s$ under the aforementioned map. □

2 Fields

2.1 Field Extensions

Let K be a field. As we have seen before, as fields are rings, there exists a unique ring homomorphism from $f : \mathbb{Z} \to K$. Then the kernel of this map is an ideal of $\mathbb{Z}$, and in particular, as $\mathbb{Z}/\ker f$ is a sub-ring of K, it is an integral domain and so, $\ker f$ is prime. Now, since the prime ideals of $\mathbb{Z}$ are either the zero ideal or the principal ideal of a prime element, we see there are two cases. In the case that $\ker f = \{0\}$, we obtain a injection

$$\iota : \mathbb{Q} \hookrightarrow K : \frac{a}{b} \mapsto f(a)f(b)^{-1}.$$

On the other hand if $\ker f = \langle p \rangle$ for some prime $p \in \mathbb{Z}$, we obtain an injection

$$\iota : \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} \hookrightarrow K.$$

Similar to rings, we refer fields of the first type to have characteristic zero, while fields of the second type to have characteristic p. We call the domain of ι (i.e. $\mathbb{Q}$ or $\mathbb{F}_p$) the prime field of K.

Definition 2.1 (Extension)**.** If K, L are fields such that $K \subset L$, then we say L is an extension of K.

We observe that if L is an extension of K, then L is a K-vector space with the natural operations.

Definition 2.2 (Finite Extension)**.** Let L be an extension of K. Then L is a finite extension of K if the L is a finite dimensional vector space of K. In this case the degree of the extension L/K, denoted $[L : K]$ is the dimension of L as a K-vector space.

Proposition 2.1. Let M, K, L be fields such that $M \subseteq K \subseteq L$, then the following are equivalent:

- L is a finite extension of M;
- L is a finite extension of K and K is a finite extension of M.

In the case that this holds, then $[L : M] = [L : K][K : M]$.

Proof. ($\implies$) Suppose L is a finite extension of M, and let $\{e_1, \cdots, e_r\}$ span L over M. Then, since $M \subseteq K$, $\{e_1, \cdots, e_r\}$ also spans L over K, implying L/K is finite. On the other hand, as K is a M-subspace of L which is finite dimensional, K must also be finite dimensional, implying K/M is finite.

($\impliedby$) Let $\{e_1, \cdots, e_r\}$ be a basis of L over K, and let $\{f_1, \cdots, f_s\}$ be a basis of K over M. Then, for all $l \in L$, $l = \sum \lambda_i e_i$ for some $\lambda_i \in K$. Furthermore, for all i, $\lambda_i = \sum \mu^i_j f_j$ for some $\mu^i_j \in M$, and so

$$l = \sum_i (\sum_j \mu^i_j f_j) e_i = \sum_{i,j} \mu^i_j f_j e_i,$$

implying $\{f_j e_i\}_{i,j}$ spans L over M. This is a finite spanning set and thus L/M is finite.

For the last claim, it suffices to show that $\{f_j e_i\}_{i,j}$ as defined above is linearly independent. Suppose $\sum_{i,j} \lambda_{i,j} f_j e_i = 0$, then $0 = \sum_i (\sum_j \lambda_{i,j} f_j) e_i$ implying $\sum_j \lambda_{i,j} f_j = 0$ as $\{e_i\}$ is linearly independent. Now as $\{f_i\}$ is also linearly independent, this implies $\lambda_{i,j} = 0$ for all i, j implying $\{f_j e_i\}_{i,j}$ is a basis of L over M. Thus, $[L : M] = \dim_M L = |\{f_j e_i\}_{i,j}| = rs = \dim_M K \dim_K L = [L : K][K : M]$ as required. □

2.1.1 One Element Extensions

Definition 2.3. Let L be a field extension of K and let $\alpha \in L$. We denote $K(\alpha)$ denote the smallest subfield of L containing both K and α.

In particular, $K(\alpha)$ consists of all elements of L expressible as $P(\alpha)/Q(\alpha)$ for $P, Q \in K[X]$ and $Q(\alpha) \neq 0$.

Proposition 2.2. Let L be a field extension of K and let $\alpha \in L$. There exists a unique homomorphism $\mathrm{ev}_\alpha : K[X] \to L$ such that $\mathrm{ev}_\alpha |_K = \iota : K \hookrightarrow L$ and $\mathrm{ev}_\alpha(X) = \alpha$.

There are two cases for the kernel of ev_α. In the first case, ev_α is injective and so, for all $P \in K[X] \setminus \{0\}$ $P(\alpha) \neq 0$. If this is the case, we say α is a transcendental number. In this case, the map extends to a map

$$K(X) \hookrightarrow L : \frac{P(X)}{Q(X)} \mapsto \frac{P(\alpha)}{Q(\alpha)}.$$

By inspection, the image of this map is $K(\alpha)$. Hence, this is an isomorphism between $K(X)$ and $K(\alpha)$.

In the case the kernel is non-zero, we have the kernel must be prime as the quotient $K[X]/\ker \mathrm{ev}_\alpha$ is isomorphic to a subring in K which are integral domains. Thus, there exists a unique monic irreducible polynomial $P \in K[X]$ generating $\ker \mathrm{ev}_\alpha$ (recall that $K[X]$ is a PID as it is a Euclidean domain). We call this polynomial P the minimal polynomial of α and we say α is algebraic over K. In this case, we obtain an injective homomorphism

$$K[X]/\langle P(X) \rangle \hookrightarrow L,$$

with its image being a field containing K, α in which every element is expressible as a polynomial in α with coefficients in K. Namely the image is precisely $K(\alpha) = K[\alpha]$ and we have an isomorphism $K[X]/\langle P(X) \rangle \simeq K(\alpha)$.

Note that if P has degree d, any element of $K[X]$ is expressible as $P(X)Q(X) + R(X)$ with $\deg R < d$. So $1, X, \cdots, X^{d-1}$ spans $K[X]/\langle P(X) \rangle$ over K. Furthermore, they are linearly independent since if otherwise, there exists $\lambda_i \in K$ such that $\sum_{i=0}^{d-1} \lambda_i X_i = 0$ implying $P \mid \sum_{i=0}^{d-1} \lambda_i X_i$, a contradiction. Thus, $1, X, \cdots, X^{d-1}$ is a basis of $K[X]/\langle P(X) \rangle$ over K and thus, $1, \alpha, \cdots, \alpha^{d-1}$ is a basis of $K(\alpha)$. With this, we conclude $[K(\alpha) : K] = \deg P$ where P is the minimal polynomial of α.

Proposition 2.3. If L/K is finite and $\alpha \in L$, then α is algebraic over K.

Proof. Let $d = [L : K]$ so $1, \alpha, \cdots, \alpha^d$ is $d + 1$ elements in L. Then, they are linearly dependent and there exists λ_i not all of which are zero such that, $\sum_{i=0}^{d} \lambda_i \alpha^i = 0$ implying α is algebraic. □

Since $K(\alpha) \subseteq L$, we have $[K(\alpha) : K]$ divides $[L : K]$.

In the absence of an ambient field, we write $K(\alpha)$ where α is a root of irreducible $P \in K[X]$ for the quotient $K[X]/\langle P(X)\rangle$.

Proposition 2.4. Let L be a field extension of K and let $\alpha, \beta \in L$ be algebraic over K. Then $\alpha + \beta, \alpha\beta$ and α^{-1} (if $\alpha \neq 0$) are all algebraic over K.

Proof. By the above proposition, it suffices to show that $[K(\alpha)](\beta)$ is finite over K since $\alpha + \beta, \alpha\beta, \alpha^{-1} \in [K(\alpha)](\beta)$. As β is algebraic over K, there exists some $P \in K[X]$ such that $P(\alpha) = 0$. Then, as $P \in K[X] \subseteq K(\alpha)[X]$, we have β is algebraic over $K(\alpha)$ implying $[K(\alpha)](\beta)$ is finite over $K(\alpha)$ and so K by transitivity. □

With the above proposition in mind, we will write $K(\alpha, \beta)$ for $[K(\alpha)](\beta)$.

Corollary 2.1. Let $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ denote the subset of elements of $\mathbb{C}$ algebraic over $\mathbb{Q}$. Then $\overline{\mathbb{Q}}$ is a field.

We have thus far shown the existence of minimal polynomials via an argument using PIDs. This however, does not indicate how to compute such a minimal polynomial. We will now provide some tools for this purpose.

If K is a field and L is an extension of K, we would like to find the minimal polynomial $\alpha \in L$ over K. The main idea is to find a basis L over K and express $1, \alpha, \alpha^2, \cdots$ in term of this basis resulting in some linear dependence. Let us consider the following example.

Suppose we would like to find the minimal polynomial of $\alpha := \sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$. Let $L = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ and so we have the tower

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] \subseteq L.$$

It is clear that $\sqrt{2}$ is a root of the irreducible polynomial $X^2 - 2$ over $\mathbb{Q}$ and so $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$. Furthermore, $[L : \mathbb{Q}[\sqrt{2}]] = 2$ since $X^2 - 3$ is irreducible in $\mathbb{Q}[\sqrt{2}]$. Indeed, if $X^2 - 3$ is reducible in $\mathbb{Q}[\sqrt{2}][X]$, then it factor into linear products, namely $X - \sqrt{3} \in \mathbb{Q}[\sqrt{2}][X]$ and so $\sqrt{3} \in \mathbb{Q}[\sqrt{2}]$. However, if this were the case, there exists some $a, b \in \mathbb{Q}$ such that

$$a^2 + 2b^2 + 2\sqrt{2}ab = (a + \sqrt{2}b)^2 = 3,$$

implying $a^2 + 2b^2 = 3$ and $2ab = 0$. But, as $\mathbb{Q}$ is an integral domain, either $a = 0$ or $b = 0$, and hence, $2b^2 = 3$ or $a^2 = 3$. Clearly, neither is possible and so $X^2 - 3$ is irreducible in $\mathbb{Q}[\sqrt{3}]$. Then, as

$$[L : \mathbb{Q}] = [L : \mathbb{Q}[\sqrt{2}]][\mathbb{Q}[\sqrt{2} : \mathbb{Q}]],$$

we have $[L : \mathbb{Q}] = 2 \cdot 2 = 4$. Now, since $1, \sqrt{2}$ form a basis for $\mathbb{Q}[\sqrt{2}]$ over $\mathbb{Q}$ and $1, \sqrt{3}$ for a basis for L over $\mathbb{Q}[\sqrt{2}]$, we have $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ form a basis of L over $\mathbb{Q}$. Finally, by considering $\alpha^0 = 1, \alpha^1 = \sqrt{2} + \sqrt{3}, \alpha^2 = 5 + 2\sqrt{6}, \alpha^3 = 11\sqrt{2} + 9\sqrt{3}$ and $\alpha^4 = 49 + 20\sqrt{6}$, we see $\alpha^4 = 10\alpha^2 - 1$ and thus, $X^4 - 10X^2 + 1$ is the minimal polynomial of α.

2.2 Finite Fields

Recall that any field contains a $\mathbb{F}_p$ or $\mathbb{Q}$ (the latter of which is impossible for finite fields). If K is a finite field and $\mathbb{F} \subseteq K$ for some prime p such that $[K : \mathbb{F}_p] = r < \infty$, then $|K| = p^r$ since each element of K is expressed uniquely by $a_1e_1 + \cdots + a_re_r$ where $e_1, \cdots, e_r$ is a basis of K over $\mathbb{F}_p$ and $a_i \in \mathbb{F}_p$. Conversely, we asks whether or not there exists a field with p^r elements for any prime p, and if it exists, is it unique up to isomorphism.

Definition 2.4 (Frobenius Endomorphism)**.** Let R be a ring of characteristic p (i.e. the kernel of the unique ring homomorphism $\mathbb{Z} \hookrightarrow R$ is $\langle p \rangle$). Then, observing that $(x+y)^p = x^p + y^p$ by the binomial theorem (all other terms vanishes as their coefficient is divisible by p), we see the map

$$Fr_p : R \to R : r \mapsto r^p$$

is a ring homomorphism and we call it the Frobenius endomorphism.

In the case that K is a field, the Frobenius endomorphism is a ring homomorphism between fields, and thus, as it is not the zero map, it must be surjective. Now, if K is finite, then an injective map from itself to itself must be bijective, and thus, the Frobenius endomorphism is an isomorphism and we refer it as the Frobenius automorphism.

If K is finite, $\text{char}(K) = p$, $|K| := q = p^r$, then $K^\times$ has order $q-1$. Thus, by Lagrange's theorem, $\alpha^{q-1} = 1$ for all $\alpha \in K^\times$, and so $\alpha^q = \alpha$ for all $\alpha \in \mathbb{K}$. Then, $Fr_p^r(\alpha) = \alpha^{p^r} = \alpha^q = \alpha$. This is in fact the least case where this occurs. Indeed, if $Fr_p^s(\alpha) = \alpha^{p^s} = \alpha$, for all $\alpha \in K$, then α is a root of $X^{p^s} - X$ for all α. But $X^{p^s} - X$ can have at most p^s roots in K, $p^s \geq p^r$ and so $s \geq r$.

Proposition 2.5. If K has characteristic p, then

$$K_r := \{x \in K \mid x^{p^r} = x\}$$

is a subfield of K. This field is known as the fixed field of r-th power of the Frobenius map.

Proof. Clearly $0, 1 \in K_r$, and if $a, b \in K_r$, then $(a+b)^{p^r} = a^{p^r} + b^{p^r} = a + b$, $(ab)^{p^r} = a^{p^r} b^{p^r} = ab$ and $(a^{-1})^{p^r} = (a^{p^r})^{-1} = a^{-1}$. □

Lemma 2.1. Let K be a field of characteristic p and $P(X)$ is an irreducible factor of $X^{p^r} - X$, then every element β of $K[X]/\langle P(X) \rangle$ satisfies $\beta^{p^r} - \beta = 0$.

Proof. Let β be a root of $P(X)$ so that $K(\beta) := K[X]/\langle P(X) \rangle$. It is clear that, $K \subseteq K(\beta)_r$ and $\beta \in K(\beta)_r$. Thus, $K(\beta) \subseteq K(\beta)_r$. Hence, $K(\beta) \subseteq K(\beta)_r$ implying that every element is fixed by the r-th power of the Frobenius map. □

Proposition 2.6. There exists a field K of characteristic p such that

- $\alpha^{p^r} = \alpha$ for all $\alpha \in K$,
- $X^{p^r} - X$ factors into linear products in $K[X]$.

Proof. We will construct a tower of fields inductively. Define $K_0 := \mathbb{F}_p$ (it is clear that K_0 satisfy the two properties), and define $K_{i+1} := K[X]/\langle P(X) \rangle$ if there exists some irreducible $P(X)$ that is a factor of $X^{p^r} - X$ in K_i, and if there does not exist such a factor, K_i is the field K we are looking for. This process certainly terminates as $X^{p^r} - X$ can be factored into at most p^r linear factors, and so simply taking K to be the last field in our tower of fields suffices. □

With this proposition in mind, we see that if $X^{p^r} - X$ factor into distinct linear factors, the field constructed above has p^r elements. To show this, we will need additional tools.

Definition 2.5 (Derivative)**.** For K a field, $P(X) \in K[X]$ such that $P(X) = a_0 + a_1X + \cdots + a_nX^n$. Then the derivative of $P(X)$ is defined to be

$$P'(X) := a_1 + a_2X + \cdots + a_nX^{n-1} \in K[X].$$

While this is purely an algebraic definition, the derivative remains to obey some derivative results from analysis, namely $(P(X) + Q(X))' = P'(X) + Q'(X)$ and $(P(X)Q(X))' = P'(X)Q(X) + Q'(X)P(X)$. With this in mind, if $P(X) = Q(X)^2R(X)$ in $K[X]$, we have

$$P'(X) = Q(X)^2P'(X) + 2Q(X)Q'(X)R(X) = Q(X)(Q(X)P'(X) + 2Q'(X)R(X)),$$

implying $Q(X)$ divides both $P(X)$ and $P'(X)$. Then, if $P(X)$ and $P'(X)$ has no common factor in $K[X]$, then $P(X)$ has no repeated roots. Thus, in the case that $P(X) = X^{p^r} - X$ in $K[X]$, we have $P'(X) = p^rX^{p^r-1} - 1 = -1$ implying $P(X)$ has no repeated roots and hence, K has p^r elements.

Corollary 2.2. For all p prime, $r \geq 1$, there exists a field of p^r elements.

2.2.1 Multiplicative Group

Before showing the field as constructed in the previous section is unique up to isomorphism, we will first study the multiplicative group of a field. This will help in the showing of uniqueness and is also interesting by itself.

Let K be a field with p^r elements for some prime p. Then $K^\times$ is a multiplicative group with $p^r - 1$ elements. We note that the order of α divides some d if and only if α is a root of $X^d - 1$. Let $d \mid p^r - 1$, then

$$X^{p^r} - X = X(X^{p^r-1} - 1) = X(X^d - 1)(X^{(p-1)d} + X^{(p-2)d} + \cdots x^d + 1).$$

Now, as $X^{p^r} - X$ factors into distinct linear factors over $K[X]$, so is $X^d - 1$ a product of distinct linear factors. Thus, there are exactly d elements in $K^\times$ of order dividing d.

For $n > 0$, denote $\Phi(n)$ the number of elements of order n in a a cyclic group of order n.

Lemma 2.2. For any d dividing n, there exists a unique subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d.

Proof. Clearly the subgroup of $\mathbb{Z}/n\mathbb{Z}$ generated by n/d is a subgroup of order d, so it remains to show uniqueness. Suppose x is an element of a subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d, then the order of x is divides d. Hence, $dx = 0$ in $\mathbb{Z}/n\mathbb{Z}$ implying dx is divisible by n and thus, $x = k(n/d)$ for some k. This means that x is in the subgroup generated by n/d and we are done. □

Proposition 2.7. For any n, $\sum_{d|n} \Phi(d) = n$.

Proof. We see that the order of elements form an equivalence relation on $\mathbb{Z}/n\mathbb{Z}$ and thus, form a partition. Now, as for all elements x, it has some order d dividing n, each element belongs to exactly to one of the equivalence class which contains the elements of order d, $d \mid n$. Hence, the sum counts all elements of $\mathbb{Z}/n\mathbb{Z}$ which is simply n. □

Proposition 2.8. Let A be an abelian group of order n such that for all $d \mid n$, there exists exactly d elements of A of order dividing d. Then A is cyclic.

Proof. A is cyclic if and only if there exists an element in A of order n which follows if $\Phi(d)$ is the number elements of order d for all d as $\Phi(n) \neq 0$. We will prove this by induction. For $d = 1$, $\Phi(d) = 1$ and the statement holds. Assuming the statement holds for all $d' < d$, as the number of elements with order dividing d is d, the number of elements of order d is,

$$d - \sum_{\substack{d'|d,\\ d'<d}} \Phi(d') = \sum_{d|n} \Phi(d) - \sum_{\substack{d'|d,\\ d'<d}} \Phi(d') = \Phi(d).$$

□

Corollary 2.3. $K^\times$ is cyclic for any finite field K.

Corollary 2.4. For all $r \geq 0$, there exists an irreducible polynomial $P(X) \in \mathbb{F}_p[X]$ of degree r.

Proof. Let K be a field such that $|K| = p^r$. As $K^\times$ is cyclic, there exists some α generating $K^\times$. Then $K = \mathbb{F}_p(\alpha)$ as $0 \in \mathbb{F}_p(\alpha)$ and $\alpha^k \in \mathbb{F}_p(\alpha)$ and so $K = \mathbb{F}_p(\alpha)$. Thus, as the map

$$f : \mathbb{F}_p[X] \to \mathbb{F}_p(\alpha) = K : X \mapsto \alpha$$

is surjective (in particular, $\alpha^{-1} = \alpha^{p^r-2}$),

$$K \cong \frac{\mathbb{F}_p[X]}{\ker f} = \frac{\mathbb{F}_p[X]}{\langle P(X) \rangle}$$

for some irreducible polynomial $P(X) \in \mathbb{F}_p[X]$. Finally, as $[K : \mathbb{F}_p] = r$, $P(X)$ has degree r. □

Theorem 3. Any two finite fields of cardinality p^r are isomorphic.

Proof. Suppose we take $P(X) \in \mathbb{F}_p[X]$ to be an irreducible polynomial of degree $r \geq 0$ (which exists by the above corollary), then we know that for $X + \langle P(X) \rangle \in \mathbb{F}_p[X]/\langle P(X) \rangle$, $X^{p^r} - X = 0$, i.e. $P(X) \mid X^{p^r} - X$. Now, since for any K a field of p^r elements, $X^{p^r} - X$ factors into linear factors, $P(X)$ must also factor into linear factors of which, let us we take a root α of $P(X)$. Thus, as $P(X)$ is irreducible, $P(X)$ is the minimal polynomial of α. Then, the map

$$\frac{\mathbb{F}_p[X]}{\langle P(X) \rangle} \hookrightarrow K$$

induced by $X \mapsto \alpha$ is an isomorphism. Thus, for any K, K' of p^r elements,

$$K \cong \frac{\mathbb{F}_p[X]}{\langle P(X) \rangle} \cong K'.$$

□

As there is only one field of cardinality p^r up to isomorphism, we will denote the field of cardinality p^r as $\mathbb{F}_{p^r}$.

Proposition 2.9. Let $q := p^r$, then $X^{q^s} - X$ factors over $\mathbb{F}_q$ as the product of all irreducible monic polynomials of degree dividing s.

Proof. Since $X^{q^s} - X$ and its derivative $q^s X^{q^s - 1} - 1$ has no common factors, $X^{q^s} - X$ contains no repeated factors. Now if $P(X)$ is a monic irreducible factor of $X^{q^s} - X$ of degree d, by considering the extension of $\mathbb{F}_{q^s}$ over $\mathbb{F}_q$, we have $X^{q^s} - X$ factors over $\mathbb{F}_{q^s}$ as a product of linear factors, and thus, as $P(X) \mid X^{q^s} - X$, it has a root α in $\mathbb{F}_{q^s}$. In particular, we have the injection

$$\mathbb{F}_{q^d} \cong \frac{\mathbb{F}_q[X]}{\langle P(X) \rangle} = \mathbb{F}_q(\alpha) \hookrightarrow \mathbb{F}_{q^s}.$$

Thus, $\mathbb{F}_{q^d}$ is a subfield of $\mathbb{F}_{q^s}$, implying q^s is a power of q^d, and so $d \mid s$.

Finally, if $P(X)$ is a monic irreducible polynomial of degree $d \mid s$, we have $\mathbb{F}_q[X]/\langle P(X) \rangle \cong \mathbb{F}_{q^d}$. Then for all roots α of $P(X)$, $\alpha^{q^d} = \alpha$ and so, as $d \mid s$, $\alpha^{q^s} = \alpha$ and so, α is a root of $X^{q^s} - X$ implying $P(X) \mid X^{q^s} - X$. □

This proposition allows us to count the number of irreducible polynomial of a specific degree over a finite field.

3 Modules

3.1 Definitions

Definition 3.1 (R-Module)**.** A R-module where R is a ring is a set M with two operations $+ : M \times M \to M$, $\cdot : R \times M \to M$ and some $0_M \in M$ such that

- $(M, +)$ form an abelian group with the identity 0_M;
- for all $m \in M$, $1_R \cdot m = m$;
- for all $r, s \in R, m \in M$, $r \cdot (s \cdot m) = rs \cdot m$;
- for all $r, s \in R, m \in M$, $(r + s) \cdot m = r \cdot m + s \cdot m,$;
- for all $r \in R, m, n \in M$, $r \cdot (m + n) = r \cdot m + r \cdot n$.

We note that an R-module over a field is simply a vector space and the theory of modules is the same as the theory of linear algebra.

It is easy to see that a ring is a module over itself with the usual operations, and in fact, if $I \trianglelefteq R$ is an ideal, the I is an R-module with the usual operations inherited from R. This is in contrast with fields which ideals are either the unit ideal or the trivial ideal. In this sense, the only subspace of a field over itself is the zero space or the whole space.

Given rings R, S and a homomorphism $f : R \to S$, we may construct a R-module with S by defining addition as the addition in S and multiplication as $r \cdot s = f(r)s$. By recalling that there is a unique homomorphism between $\mathbb{Z} \to R$, we see that $\mathbb{Z}$ forms a R-module over any ring R.

On the other hand, $\mathbb{Z}$-modules corresponds 1 to 1 with the abelian groups. In particular, for any abelian group A, we define the scalar multiplication by $na = a + \cdots a$, n-times for all a in A, and so A forms a $\mathbb{Z}$-module. Conversely, by inspecting the axioms, these must be the only $\mathbb{Z}$-modules.

Definition 3.2 (R-Submodule)**.** Let M be an R-module. A subset N of M is a R-submodule if $0_M \in N$ and N is closed under addition and scalar multiplication.

By this definition, we see that the ideals of R are precisely the R-submodules of R.

Definition 3.3. Let M be an R-module and suppose $m_1, \cdots, m_r \in M$. Then $\langle m_1, \cdots, m_r \rangle$ is the R-submodule generated by $\{m_1, \cdots, m_r\}$ where

$$\langle m_1, \cdots, m_r \rangle := \{s_1 m_1 + \cdots + s_r m_r \mid s_1, \cdots, s_r \in R\}.$$

As one might expect, this is the smallest R-submodule containing $m_1, \cdots, m_r \in M$, i.e. the intersection of all R-submodules containing $m_1, \cdots, m_r \in M$.

Definition 3.4. Let M be an R-module and let $I \trianglelefteq R$ be an ideal of R. Then, we define

$$IM := \left\{\sum i_j m_j \mid i_j \in I, m_j \in M\right\}.$$

Definition 3.5 (Quotient Module)**.** Let M be an R-module and $N \leq M$ a submodule, then we define $m \equiv_N m' \iff m - m' \in N$. It is clear that $\equiv_N$ is an equivalence relation, and so, we may define the quotient module of M over N by $M/\equiv_N$ and we denote this by M/N.

The quotient module form a module by defining

$$(m+N)+(n+N)=(m+n)+N;\ r\cdot(m+N)=(r\cdot m)+N,$$

where $m+N, n+N \in M/N$ and $r \in R$.

Definition 3.6 (Direct Sum)**.** Given M, N R-modules, the (external) direct sum $M \oplus N$ is the Cartesian product of M and N equipped with pairwise addition and the multiplication defined by $r\cdot(m,n) := (rm, rn)$. It is easy to check that this is an R-module.

Definition 3.7. An element $m \in M$ is R-torsion if there exists some $r \in R \setminus \{0\}$, $rm = 0$. We denote the set of R-torsion elements of M by M^{tors}.

It is easy the check that if R is any integral domain, then the set of R-torsion elements is a submodule. If we quotient a R-module M by M^{tors}, we obtain a torsion free module.

Definition 3.8. Let R be a ring and S a multiplicative system of R and M a R-module, we define

$$S^{-1}M := \left\{\frac{m}{b} \mid m \in M, b \in S\right\} / \sim,$$

where $\sim$ is the equivalence relation defined by

$$\frac{m}{b} \sim \frac{m'}{b'} \iff \exists s \in S, s(b'm - bm') = 0_M.$$

$S^{-1}M$ form a $S^{-1}R$-module with the operations

$$\frac{m}{b} + \frac{m'}{b'} := \frac{b'm + bm'}{bb'},$$

$$\frac{r}{b} \cdot \frac{m'}{b'} := \frac{r \cdot m'}{bb'}.$$

3.2 Homomorphisms and Free Modules

Definition 3.9 (Module Homomorphism)**.** Let R be a ring and M, N be R-modules. Then a map $f : M \to N$ is a R-module homomorphism if

- for all $m, m' \in M$, $f(m+m') = f(m) + f(m')$, and
- for all $m \in M, r \in R$, $f(rm) = rf(m)$.

We say f is an isomorphism if it is also bijective. In this case, the inverse f^{-1} is also a module homomorphism.

It is clear that in the case that R is a field, a module homomorphism is simply a linear map.

Proposition 3.1. The image of a R-module homomorphism $f : M \to N$ is a submodule of N and the kernel is a submodule of M. Furthermore, $\ker f = \{0\}$ if and only if f is injective.

Proof. Clear. □

Proposition 3.2 (Universal Property for Modules)**.** Let L, M, N be R-modules with $N \subseteq M$ and $f : M \to L$ is a module homomorphism such that $N \leq \ker f$. Then there exists a unique module homomorphism $\tilde{f} : M/N \to L$ such that

$$\tilde{f}(m + N) = f(m).$$

In particular, the universal property demonstrates the existence of $\tilde{f}$ such that the following diagram commutes.

$$\begin{tikzcd}
M \arrow[r, "f"] \arrow[d, "q"'] & N \\
M/N \arrow[ru, dashed, "\tilde{f}"'] &
\end{tikzcd}$$

Proof. Uniqueness follows by extensionality, so it suffices to show the map is well defined and is a homomorphism.

$\tilde{f}$ is well defined since if $m + N = m' + N$, then $m - m' \in N \leq \ker f$ implying $0 = f(m - m') = f(m) - f(m')$. Thus, $\tilde{f}(m + N) = f(m) = \tilde{f}(m' + N)$ and so the map is well defined. $\tilde{f}$ is clearly a homomorphism and so we are done. □

We see that $\ker \tilde{f} = q(\ker f) = \{m + N \mid m \in \ker f\}$, and thus, in the case that $N = \ker f$, we have the isomorphism,

$$\tilde{f} : M/\ker f \cong \mathrm{Im}(f).$$

In contrast to vector spaces in linear algebra where every finite dimensional vector space has a basis. On the other hand, in the case of modules, this is in general not true. Nonetheless, we can make the same definition as a basis.

Definition 3.10 (Basis)**.** Let M be a R-module, then a set $B \subseteq M$ is a basis of M if

- B spans M, i.e. every element of M is of the form $r_1 b_1 + \cdots + r_n b_n$ for $r_i \in R$ and $b_i \in B$, and
- B is linearly independent, i.e. if $b_1, \cdots, b_n$ are distinct elements of B such that $r_1 b_1 + \cdots + r_n b_n = 0$ for some $r_1, \cdots, r_n$, then $r_i = 0$ for all i.

An example of a module which does not have a basis is the module of $\mathbb{Z}/3\mathbb{Z}$ over $\mathbb{Z}$. Indeed, any element of $m \in M$ satisfy $3m = 0$ implying any subset of $\mathbb{Z}$ is not linearly independent.

Definition 3.11 (Free Module)**.** An R-module M is a free module if it admits a basis B and we say M is a free module of rank r if B has cardinality r.

Given a set S, we may define a free R-module over S by defining

$$F_S := \{f : S \to R \mid |\mathrm{supp}(f)| < \infty\},$$

i.e. the set of functions from S to R with finite support. Then, F_S is a free module with the basis S (we have here abused the notation by forcing $S \subseteq F_S$ such that for all $s \in S$, we define $s = 1_{\{s\}} \in F_S$ where $1_{\{s\}}$ is taken to be the indicator function). It is clear that S spans F_S and if $\sum r_s s = 0$, then $0 = (\sum r_s s)(s) = r_s$, and so S is also linearly independent.

Proposition 3.3. Let F_1, F_2 be free R-modules, then $F_1 \oplus F_2$ is also free.

Proof. Not difficult to see that, if B_1, B_2 are bases of F_1, F_2 respectively, then $\{(b, 0) \mid b \in B_1\} \cup \{(0, b) \mid b \in B_2\}$ form a basis of $B_1 \oplus B_2$. □

By induction, we see that the finite direct sum of free modules is also free.

Proposition 3.4 (Universal Property for Free Modules)**.** Let S be a set and M be an R-module, then for any $\phi : S \to M$, there exists a unique homomorphism $f_\phi : F_S \to M$ such that $f_\phi(s) = s$ for all $s \in S$.

This is similar to the extension of linear maps where we may define a linear map provided with know where it maps its basis.

Proof. It is clear that $f_\phi : F_S \to M : \sum r_s s \mapsto \sum r_s \phi(s)$ satisfy this property. This map is unique follows by the homomorphism requirement. □

Corollary 3.1. If M, N are free R-modules of the same rank, then they are isomorphic.

Proof. Let B_M, B_N be the bases of M, N respectively. Then, we may take a bijection $\phi : B_M \to B_N$ and so the extension of ϕ is and isomorphism between M and N. □

3.3 Classification of Finitely Presented Modules

Definition 3.12 (Generating Set)**.** A subset S of a module M is a generating set if $\langle S \rangle = M$.

Definition 3.13. Suppose we have a module M and a generating set S of M. Then, we have the natural surjection $F_S \to M$ which maps s to s. Let K be the kernel of this map, we call elements of K relations among S, and for $f \in K \subseteq F_S$, we have $\sum f(s)s = 0$. Then, if K is generated by the set T, we have the isomorphism

$$M \cong F_S/T$$

We call such an description of M a presentation and in the case that T is finite, we say the module is finitely presented.

In other words, a presentation is a description of a module M in terms of a generating set S of M, and a generating set T for the linear relations satisfied by S.

If M is finitely generated with generators $g_1, \cdots, g_n$ and relations $k_1, \cdots, k_m \in F$ such that $k_i = \sum_j r_{ij} g_j$, we define the permutation matrix attached to $\langle g_1, \cdots, g_n \rangle$ and $\langle k_1, \cdots, k_m \rangle$ as the matrix with entries r_{ij}. This matrix give us a map from R^m to R^n and the quotient R^n/AR^m is isomorphic to M.

We would like to ask when two modules are isomorphic and rather or not we can deduce this from their presentations. It is clear that a module can have multiple presentations based on the generating set and so, we introduce the following elementary column operations.

- Exchanging columns (results in reordering the relations while fixing the generators).
- Multiplying a column by a constant unit $u \in R^\times$.
- Adding r times column i to column j (results in replacing the relation $\phi(t_1), \cdots, \phi(t_m)$ by $\phi(t_1), \cdots, \phi(t_{j-1}), \phi(t_j) + r\phi(t_i), \cdots, \phi(t_n)$, which generate the same submodule of F_S.

We see that elementary operations on the columns changes the relations to an equivalent set of relations fixing the generating set.

Similarly, we define the elementary row operations.

- Exchanging rows (results in reordering the generators and rewriting the relations to account for this).
- Multiplying row i by a constant unit $u \in R^\times$ (replaces s_i with $u^{-1}s_i$ and rewrites the relations to account for this).
- Adding r times row i to row j (corresponds to replacing s_i with $s_i - rs_j$ and rewriting the relations to account for this).

We see that these elementary operations corresponds to changes of the choice of the generators, and so, if the presentations of two modules can be transformed into each other with the elementary operations, then the two modules are isomorphic. On the other hand, it unclear whether or not two presentations on the same module can be transformed into each other with the elementary operations. This is true for simple cases such as when R is a field and so M is a vector space though it is unlikely to be true in general.

Definition 3.14 (Smith Normal Form)**.** Let R be an Euclidean domain (definition also work for PID though the proofs will require ED) and M a matrix with entries in R. Then M is in smith normal form (SNF) if the only non-zero entries are the diagonal entries $M_{i,i}$, and moreover, for each i, $M_{i,i} \mid M_{i+1,i+1}$.

Given any matrix over an Euclidean domain, we will always be able to transform it into smith normal form using the elementary operations. In fact, we will provide an constructive algorithm for doing so.

Lemma 3.1. *Given M a matrix over an Euclidean domain R. After finitely many elementary operations, we can ensure M is in the form $[M'_{1,1}] \oplus M'$, where $M'_{1,1}$ divides every entry of M'.*

Proof. Recall that the Euclidean norm $N : R \to \mathbb{N}$ satisfies for all $a, b \in R$, $b \neq 0$, there exists $q, r \in R$ such that $a = qb + r$ and $N(r) < N(b)$ or $r = 0$.

1. Using row and column operations, we can move the non-zero entry of smallest norm to the upper left.
2. Subtract multiples of the first row from the remaining row using the Euclidean norm property so that the first entry of each row is either zero or has norm less than the upper left entry.
3. Do the same with columns, i.e. subtract multiples of the first column from the remaining so that the first entry of each column is either zero or has norm less than the upper left entry.
4. If there exists a non-zero entry in the first row or the first column that is not the upper left, repeat from step 1. This process must terminate in finite steps by the well-ordering principle.
5. Now that every entry in the first row or the first column that is not the upper left is zero, we are done if the upper left entry divides every other entry.

6. If not, let m_{11} be the upper left entry, and there exists some m_{ij} such that $m_{11} \nmid m_{ij}$. Add the first row to the i-th row (which does not change m_{ij}).
7. Now that m_{11} is in the first column, subtract r-multiples of the first column from the j-th column so that $N(m_{ij} - rm_{11}) < N(m_{11})$.
8. As $N(m_{ij} - rm_{11}) < N(m_{11})$, m_{11} is no longer the entry with smallest norm and so, start from step 1. This process eventually terminates as the norm of the upper left entry is decreasing.

Once the algorithm terminates, we see that the resulting matrix is as required. □

Proposition 3.5. Given M a matrix over an Euclidean domain R. After finitely many elementary operations, we can ensure M is in the Smith normal form.

Proof. Recursively apply the above algorithm to the resulting M'. □

In the case where the matrix is a presentation, we see that we may show that two modules are isomorphic by showing they have the same Smith normal form.

Corollary 3.2. Every finitely presented module M of R an Euclidean domain is isomorphic to one of the form

$$M \cong R^s \oplus R/\langle a_1 \rangle \oplus R/\langle a_2 \rangle \oplus \cdots \oplus R/\langle a_t \rangle$$

with $a_1 | a_2 | \cdots | a_t$ in R, $a_i \neq 0$.

We call s the rank of M and $a_1, \cdots, a_n$ are called the invariant factors of M.

Proof. The natural presentation of $R^s \oplus R/\langle a_1 \rangle \oplus \cdots \oplus R/\langle a_t \rangle$ is already in Smith normal form, and so, choosing a_i to be the diagonal entries of the SNF of M suffices. □

The above result is known as the classification of finitely generated modules over Euclidean domain. The statement holds as well for principal ideal domains though we shall not prove it here.

Proposition 3.6. If $M \cong R^s \oplus R/\langle a_1 \rangle \oplus \cdots \oplus R/\langle a_n \rangle \cong R^t \oplus R/\langle b_1 \rangle \oplus \cdots \oplus R/\langle b_m \rangle$ where $a_1 | \cdots | a_n$ and $b_1 | \cdots | b_n$, then $s = t$, $n = m$ and each a_i is an associate of b_i.

Proof. Let $p \in R$, $p \neq 0$ be a prime. Then for any $k \in \mathbb{N}$, $p^{k+1}M \leq p^k M \leq M$ where $p^j M$ is the image of the homomorphism $M \to M : x \mapsto xp^j$. Then, defining

$$M_{p,k} := p^k M / p^{k+1} M,$$

we have for all $x \in M_{p,k}$, $xp = 0$ since for all $x \in p^k M$, $xp \in p^{k+1} M$. Furthermore, $M_{p,k}$ is an $R/\langle p \rangle$-module with the multiplication being

$$(r + \langle p \rangle)(p^k m + p^{k+1} M) = rp^k m + p^{k+1} M.$$

But, as p is prime, $\langle p \rangle$ is a maximal ideal, and so $R/\langle p \rangle$ is a field and $M_{p,k}$ is a $R/\langle p \rangle$-vector space. Now, by considering $M_{p,k} = (R_{p,k})^s \oplus (R/a_1)_{p,k} \oplus \cdots \oplus (R/a_n)_{p,k}$, where the individual summands either contribute 0 or 1 dimension. We see that the map $R/p \to R_{p,k} = p^k R / p^{k+1} R : r + \langle p \rangle \mapsto p^k r + \langle p^{k+1} \rangle$ is an isomorphism and thus, $\dim R_{p,k} = 1$ and so, $\dim(R_{p,k})^s = s$. For the other summands $(R/a_i)_{p,k}$, write $a_i = p^n q$ with p, q relatively prime. Then, by CRT, $R/a_i \cong R/p^n \times R/q$, and so, $p(R/q) = R/q$ implying $(R/q)_{p,k} = 0$. On the other hand, $p^k(R/p^n) = 0$ if $k \geq n$ and if $k < n$, $p^k(R/p^n) = p^k R/p^n R$ and so,

$$(R/p^n)_{p,k} = \frac{p^k R/p^n R}{p^{k+1} R/p^n R} \cong p^k R/p^{k+1} R \cong R/P.$$

Thus, $\dim R/a_i$ is 0 if $k \geq n$ and 1 if $k < n$. Now, taking $d_{p,k} = \dim M_{p,k}$, we have $\dim R/a_i = 0$ for k sufficiently large, implying $s = d_{p,k}$. □

Alternatively, one may formulate the classification by considering the primes which divides a_i. If $p_1, \cdots, p_t$ are the primes dividing a_i so that $a_i = u_i \prod_j p_j^{k_{ij}}$ where u_i is a unit, the Chinese remainder theorem provides the isomorphisms

$$R/\langle a_i \rangle \cong \bigoplus_j R/\langle p_j^{k_{ij}} \rangle,$$

and so,

$$M \cong R^s \oplus \bigoplus_{i,j} R/\langle p_j^{k_{ij}} \rangle.$$

Since abelian groups are $\mathbb{Z}$-modules and $\mathbb{Z}$ is an Euclidean domain, we recover the classification of finitely generated abelian groups.

Corollary 3.3. Let A be a finitely generated abelian group. Then there exists integers $s, a_1, \cdots, a_t$ where $a_1, \cdots, a_t > 1$ and $a_1 | \cdots | a_t$ such that

$$A \cong \mathbb{Z}^s \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_t\mathbb{Z}.$$

3.4 $K[T]$-modules

Given a finite-dimensional K-vector space and $L : V \to V$ a linear map, we can study the map by relating it to a module. As a consequence, we will also obtain a proof for the Jordan decomposition theorem whenever K is algebraically closed.

Definition 3.15. Let V be a finite-dimensional K-vector space and let $L : V \to V$ be a linear map. Then, we define M_L to be the $K[T]$-module where the underlying set of M_L is that of V with the same addition as V. Then, for all $P(T) \in K[T]$, $v \in M_L$, we define $P(T) \cdot v = P(L)(v)$.

M_L has the following presentation. Let $B := \{v_1, \cdots, v_m\}$ be a basis of V and $A := [L]_B = (a_{ij})$. Then, v_i generate M_L as a $K[T]$-module. Moreover, we have for each i, the relation $Tv_i = \sum_{j=1}^m a_{ji} v_j$.

Thus, as $K[T]$ is a Euclidean domain and M_L is finitely generated, there exists polynomials $P_1(T), \cdots, P_n(T) \in K[T]$ such that

$$M_L \cong K[T]^s \oplus \frac{K[T]}{\langle P_1(T) \rangle} \oplus \cdots \oplus \frac{K[T]}{\langle P_n(T) \rangle},$$

and $P_1(T)|P_2(T)|\cdots|P_n(T)$. Furthermore, by taking only monic polynomials, we may ensure this decomposition is unique. We observe that, since $M_L = V$ is finitely generated over K while $K[T]$ is not, $s = 0$ and we must have

$$M_L \cong \frac{K[T]}{\langle P_1(T)\rangle} \oplus \cdots \oplus \frac{K[T]}{\langle P_n(T)\rangle}.$$

With this, we obtain the rational canonical form of L.

Proposition 3.7 (Rational Canonical Form)**.** Let $L : V \to V$ be a linear map and let M_L be the associated $K[T]$-module. Then, there exists polynomial $P_1(T), \cdots, P_n(T) \in K[T]$ such that

$$M_L \cong \frac{K[T]}{\langle P_1(T)\rangle} \oplus \cdots \oplus \frac{K[T]}{\langle P_n(T)\rangle},$$

and $P_1(T)|P_2(T)|\cdots|P_n(T)$. Thus, there exists some basis B of V for which

$$[L]_B = c(P_1(T)) \oplus \cdots \oplus c(P_n(T)),$$

where $c(P(T))$ is the companion matrix of $P(T)$.

From this, we immediately see that the minimal polynomial of L is $P_1(T)$ and the characteristic polynomial is $\prod_i P_i(T)$.

To obtain the Jordan decomposition on the other hand, we will use the prime decomposition as remarked in the previous section. In particular, by the fundamental theorem of algebra, we have that the primes of $\mathbb{C}[X]$ (or with that matter any algebraically closed field) are of the form $X - \lambda$ for all $\lambda \in \mathbb{C}$. Then, for a linear map $L : V \to V$ where V is a vector space over $\mathbb{C}$, we have

$$M_L \cong \frac{\mathbb{C}[X]}{(X-\lambda_1)^{a_1}} \oplus \cdots \oplus \frac{\mathbb{C}[X]}{(X-\lambda_t)^{a_t}}.$$

Now, by considering for $M \cong K[T]/(T-\lambda)^r$, $(T-\lambda)^r$ has the λ-Jordan block of size r as its matrix, we obtain the Jordan normal form of L.

3.5 Noetherian Rings

Definition 3.16 (Noetherian)**.** Let R be a ring and M be a R-module. Then M is called Noetherian if every increasing tower of submodules

$$N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots$$

eventually stabilizes; i.e. there exists some $n \geq 0$ such that $N_i = N_j$ for all $i, j \geq n$.

Proposition 3.8. *M is Noetherian if and only if every submodule N of M is finitely generated.*

Proof. ($\implies$) Suppose otherwise, that there exists some $N \subseteq M$ where N is not finitely generated. Then, we may construct a non-stabilizing tower of submodules by defining $N_0 = \langle n_0 \rangle$ for some $n_0 \in N$ and for $i \in \mathbb{N}$, define $N_{i+1} = \langle N_i, n_{i+1}\rangle$ where $n_{i+1} \in N \backslash N_i$. This tower never terminates since otherwise, N is finitely generated. Thus, M is not Noetherian.

($\Longleftarrow$) Conversely, suppose every submodule of M is finitely generated. Then, given a tower of submodules

$$N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots$$

we may define $N = \bigcup_{i=1}^{\infty} N_i$ which is also a submodule of M and so is finitely generated by some $n_1, \cdots, n_r$. By definition, there exists $i_1, \cdots, i_r$ such that $n_j \in i_j$ for all $j = 1, \cdots, r$. Thus, by taking $k = \max\{i_1, \cdots, i_r\}$, we have N_k contains the generators of N, and so $N = N_k$. This implies $N_l = N_k$ for all $l \geq k$ and hence, the tower terminates and M is Noetherian. □

Definition 3.17 (Noetherian Ring)**.** A ring R is Noetherian if it is Noetherian as a R-module over itself.

We recall that the submodule of a ring R over itself is simply the ideals of R and thus, a ring is Noetherian if and only if every increasing sequence of ideals terminates.

Corollary 3.4. Every PID is Noetherian as every ideal is finitely generated by one element.

Lemma 3.2. Let M be a Noetherian R-module and $N \subseteq M$ be a submodule. Then N and M/N are both Noetherian.

Proof. It is clear that N is Noetherian since any tower of submodules of N is also a tower of submodules of M, and thus, it must terminate.

For M/N on the other hand, a tower of submodules of M/N can be pulled back along the quotient map to be a tower in M which must terminate. Thus, by showing if $q^{-1}(A) = q^{-1}(B)$ then $A = B$ for $A, B \subseteq M/N$ submodules, we have the tower in M/N must terminate. □

Proposition 3.9. Let M be an R-module and let $N \subseteq M$ be a submodule. Then, if N and M/N are both Noetherian, then M is Noetherian.

Proof. Let $K \subseteq M$ be an R-submodule and we will show it is finitely generated. Since $K \cap N$ is a submodule of N, it is finitely generated by some $k_1, \cdots, k_r$. Similarly, as $q_N(K)$ is a submodule of M/N, it is finitely generated by some $\overline{k}_{r+1}, \cdots, \overline{k}_{r+s}$. Then, I claim $k_1, \cdots, k_r, k_{r+1}, \cdots, k_{r+s}$ generates K where $k_{r+i} \in q_N^{-1}(\overline{k}_{r+i})$ for $i = 1, \cdots, s$. Indeed, if $k \in K$, then there exists $a_{r+1}, \cdots, a_{r+s}$ such that $q_N(k) = a_{r+1}\overline{k_{r+1}} + \cdots + a_{r+s}\overline{k_{r+s}}$. Then, $k - (a_{r+1}k_{r+1} + \cdots + a_{r+s}k_{r+s}) \in K \cap N$ since $q_N(k - (a_{r+1}k_{r+1} + \cdots + a_{r+s}k_{r+s})) = 0$ and thus, there exists $a_1, \cdots, a_r$ such that

$$k - (a_{r+1}k_{r+1} + \cdots + a_{r+s}k_{r+s}) = a_1k_1 + \cdots + a_rk_r.$$

Thus, $k = a_1k_1 + \cdots + a_rk_r$ and so K is finitely generated implying M is Noetherian. □

Alternatively, one may show that the direct sum of two Noetherian modules is Noetherian and prove that $M \cong N \oplus M/N$. But then, we may not obtain the following corollary.

Corollary 3.5. If M, N are Noetherian R-moduels, then so is $M \oplus N$ by considering $N \cong (M \oplus N)/M$.

Corollary 3.6. If R is Noetherian, then R^s is Noetherian for all $s \in \mathbb{N}$.

Theorem 4. Let R be a Noetherian ring and M be a finitely generated R-module, then M is Noetherian. In particular, any submodule of an finitely generated module over a Noetherian ring is finitely generated.

Proof. Suppose $g_1, \cdots, g_s$ generate M. Then, we have the surjection

$$f : R^s \to M : (r_1, \cdots, r_s) \mapsto \sum_i r_i s_i,$$

and so, $M \cong R^s / \ker f$. But as we have seen, R^s is Noetherian and the quotient of a Noetherian module is Noetherian, M is Noetherian as required. $\square$

Corollary 4.1. If R is a Noetherian ring, then every finitely generated module is finitely presented.

3.5.1 Hilbert Basis Theorem

As we have seen on the second course work, if $R[X]$ is a Noetherian ring, then so is R Noetherian. The converse is also true and this is known as the Hilbert basis theorem.

Theorem 5 (Hilbert Basis Theorem)**.** If R is a Noetherian ring, then $R[X]$ is also a Noetherian ring.

By induction, we see that this theorem also works for any polynomial ring of finitely many variables.

Proof. We will present a proof by Emmy Noether.

Let $I \subseteq R[X]$ be an ideal and it suffices to show that I is finitely generated. Define $J \subseteq R$ be the set of leading coefficients of some polynomial $P(X) \in I$ including 0. I claim that J is in fact an ideal of R. Indeed, $0 \in J$ and for $r, s \in J$, there exists some $P(X), Q(X) \in I$ such that $P(X)$ has leading coefficient r and $Q(X)$ has leading coefficient s and WLOG. we assume $\deg P \geq \deg Q$. Then $r+s$ is the leading coefficient of $P(X) + X^{\deg P - \deg Q} Q(X) \in I$ and so $r + s \in J$. Lastly, for any $r \in R, s \in J$, where s is the leading coefficient of $P(X) \in I$, we have $rP(X) \in I$ with leading coefficient rs implying $rs \in J$.

Now since R is Noetherian, J is finitely generated and so let us take $j_1, \cdots, j_n$ such that $\langle j_1, \cdots, j_n \rangle = J$. Then, by construction, there exists $P_1(X), \cdots, P_n(X) \in I$ such that $P_i(X)$ has leading coefficient j_i.

Let $d = \max\{\deg P_i \mid i = 1, \cdots, n\}$. Then, for any $P(X) \in I$, there exists $Q_1(X), \cdots, Q_n(X) \in I$ such that

$$\deg(P(X) - Q_1(X)P_1(X) - \cdots - Q_n(X)P_n(X)) < d.$$

Indeed, this is true by inducting on $\deg P$. Clearly, for $\deg P < d$, we may simply take $Q_i = 0$. On the other hand, assuming the inductive hypothesis, such that $\deg P = n + 1$, we write $P(X) = jX^{n+1} + \star$ for some $j \in J$. Then, we can write $j = j_1 r_1 + \cdots j_n r_n$ for some $r_1, \cdots, r_n \in R$. So, we have

$$\begin{aligned} S(X) &:= P(X) - r_1 X^{d - \deg P_1} P_1(X) - \cdots - r_n X^{d - \deg P_n} P_n(X) \\ &= jX^d - (r_1 j_1 + \cdots + r_n j_n) X^d + \star \end{aligned}$$

is a polynomial of degree less equal than n. Thus, by the inductive hypothesis, there exists $Q_1(X), \cdots, Q_n(X) \in I$ such that $S(X) - Q_1(X)P_1(X) - \cdots - Q_n(X)P_n(X)$ has degree less than d. So,

$$\tilde{P}(X) := P(X) - (Q_1(X) + r_1 X^{d - \deg P_1})P_1(X) - \cdots - (Q_n(X) + r_n X^{d - \deg P_n})P_n(X)$$

is a polynomial of degree less than d.

Now, denoting $I_{\le d} \subseteq I$ be the set of polynomials in I with degree less equal than d, we observe that this is an R-submodule of $R[X]_{\le d}$ (note that this is not an ideal as it is not closed under multiplication) where $R[X]_{\le d}$ the polynomials with degree less equal than d. We see that $R[X]_{\le d}$ has a basis $1, \cdots, X^d$ and so it is finitely generated. Now, as R is Noetherian, submodules of finitely generated modules are also finitely generated, and hence, $I_{\le d}$ must also be finitely generated.

With this in mind, taking $T_1(X), \cdots, T_m(X) \in I_{\le d}$ so that $\langle T_1, \cdots, T_m \rangle = I_{\le d}$, there exists $r_1, \cdots, r_m$ such that

$$\tilde{P}(X) = r_1 T_1(X) + \cdots + r_m T_m(X),$$

we have

$$\begin{aligned} P(X) &= (Q_1(X) + r_1 X^{d - \deg P_1})P_1(X) + \cdots + (Q_n(X) + r_n X^{d - \deg P_n})P_n(X) + \tilde{P}(X) \\ &= (Q_1(X) + r_1 X^{d - \deg P_1})P_1(X) + \cdots + (Q_n(X) + r_n X^{d - \deg P_n})P_n(X) \\ &+ r_1 T_1(X) + \cdots + r_m T_m(X) \end{aligned}$$

implying I is generated by $P_1(X), \cdots, P_n(X), T_1(X), \cdots, T_m(X)$ and so is finitely generated. □

Proposition 3.10. If R, S are rings and R is Noetherian, then if there exists a surjective homomorphism $f : R \to S$, then so is S Noetherian.

Proof. Let I be an ideal of S, then $f^{-1}(I)$ is an ideal of R and so is finitely generated, i.e. there exists $r_1, \cdots, r_n \in R$ such that $f^{-1}(I) = \langle r_1, \cdots, r_n \rangle$. Then, as f is surjective, $\langle f(r_1), \cdots, f(r_n) \rangle = I$. Indeed, for all $i \in I$, there exists some $r \in f^{-1}(I)$ and so, $r \in \langle r_1, \cdots, r_n \rangle$ and by linearity, $i = f(r) \in \langle f(r_1), \cdots, f(r_n) \rangle$. On the other hand, for all $i \in \langle f(r_1), \cdots, f(r_n) \rangle$, we may write $i = \sum s_i f(r_i)$ for some $s_1, \cdots, s_n \in S$. Now as f is surjective, for all i there exists some $\tilde{s}_i \in R$ such that $f(\tilde{s}_i) = s_i$ and so,

$$i = \sum_{i=1}^{n} s_i f(r_i) = \sum f(\tilde{s}_i) f(r_i) = f\left(\sum \tilde{s}_i r_i\right)$$

where $\sum \tilde{s}_i r_i \in \langle r_1, \cdots, r_n \rangle = f^{-1}(I)$. Thus, $i = \sum s_i f(r_i) = f(\sum \tilde{s}_i r_i) \in I$. Hence, $\langle f(r_1), \cdots, f(r_n) \rangle = I$ and so, I is finitely generated implying S is Noetherian as required. □

Corollary 5.1. If R is a Noetherian ring an I is an ideal of R, then R/I is also a Noetherian ring.

Corollary 5.2. For any Noetherian ring R and an ideal I of $R[X_1, \cdots, X_n]$, then $R[X_1, \cdots, X_n]/I$ is also a Noetherian ring.

This is a very strong result as most rings we have looked at in this course are constructed by quotienting a polynomial ring by an ideal, often which, the original ring is Noetherian. With this in mind, the only ring which is not Noetherian we have seen in this course is the ring

$$\mathbb{C}[X^{\mathbb{Q}_{\geq 0}}] := \{\text{Polynomials in } \mathbb{C}[t^{1/n}] \text{ for all } n \in \mathbb{Z}_{>0}\}.$$

3.6 Factorization

Now that we have additional tools, we will revisit the topic of factorizations. In particular, we will study factorization in $R[X]$ where R is a UFD. The main idea is that, if F is the field of fraction, we will compare factorizations in $R[X]$ and factorizations in $F[X]$. We note that the two cases are not exactly the same. Consider $\mathbb{Z}$ and its field of fractions $\mathbb{Q}$. We have

$$2X + 6 \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X],$$

where $2X + 6 = 2(X + 3)$ which is reducible in $\mathbb{Z}[X]$. Yet $2X + 6$ is not reducible in $\mathbb{Q}[X]$ since 2 is a unit in $\mathbb{Q}$.

Definition 3.18 (Primitive)**.** $P(X) \in R[X]$ is said to be primitive if its coefficient are relatively prime (recall this means they have GCD 1). Furthermore, if d is the GCD of the coefficients of $P(X)$, then $P(X) = dP'(X)$ where $P'(X) \in R[X]$ is primitive.

Proposition 3.11. If $P(X) \in R[X]$ is primitive and irreducible in $F[X]$, then $P(X)$ is irreducible in $R[X]$.

Proof. Suppose there exists $Q(X), S(X) \in R[X]$ such that $P(X) = Q(X)S(X)$. Then, by the irreducibility of $P(X)$ in $F[X]$, WLOG. $Q(X) = q$ is a unit in $F^\times$. Thus, $Q(X) = q \in R$ and so q divides every coefficients of $P(X)$, implying $q = 1$ and hence $P(X)$ is irreducible. □

The converse of this proposition turns out also to be true.

Lemma 3.3. Let $P(X) \in F[X]$. Then, there exists some $a \in F^\times$ such that $aP(X) \in R[X]$ and $aP(X)$ is primitive. Furthermore, if a' is another element satisfying these properties, then $a' = ua$ where $u \in R^\times$ is a unit.

Proof. Clearly, by multiplying the denominators of the coefficients of $P(X)$, there exists some $b \in R$, $bP(X) \in R[X]$. Then, by our previous remark, there exists some $d \in R$ such that $bP(X) = dP'(X)$ for some primitive $P'(X) \in R[X]$. Hence, $P'(X) = \frac{b}{d}P(X)$ is primitive as required.

Suppose now $aP(X), a'P(X) \in R[X]$ are both primitive for $a, a' \in F^\times$. Then, there exists some $b, b' \in R$ such that $a/a' = b/b'$, and so, $b'aP(X) = ba'P(X)$. Now, as both $aP(X), a'P(X)$ are primitives, b, b' must be the GCD of the coefficients of $b'aP(X), ba'P(X)$ respectively where $b'aP(X) = ba'P(X)$. Thus, b, b' are associates, i.e. there exists some $u \in R^\times$ such that $ub = b'$ and hence $ua = a'$. □

Lemma 3.4 (Gauss's Lemma)**.** If $P(X), Q(X) \in R[X]$ are primitive polynomials, then $P(X)Q(X)$ is also primitive (recall that we require R to be a UFD).

Proof. Suppose otherwise and let d be the GCD of the coefficients of $P(X)Q(X)$. If d is not a unit, then it is divisible by some irreducible $p \in R$. Then $\langle p \rangle$ is a prime ideal of R. Denote $\overline{P(X)}, \overline{Q(X)}$, and $\overline{P(X)Q(X)}$ be the reductions of $P(X)$, $Q(X)$ and $P(X)Q(X)$ in $R/\langle p \rangle[X]$ respectively. Now, since $P(X), Q(X)$ are primitive, they are nonzero in $R/\langle p \rangle[X]$. On the other hand, $\overline{P(X)Q(X)} = 0$ since its coefficients are divisible by p. But, since $R/\langle p \rangle$ is a integral domain, we have $0 \neq \overline{P(X)Q(X)} = \overline{P(X)Q(X)}$, a contradiction! Thus, $P(X)Q(X)$ is primitive as required. □

Corollary 5.3. If $P(X) \in R[X]$ and $Q(X), S(X) \in F[X]$ such that $P(X) = Q(X)S(X)$. Then, there exists some $a \in F^\times$ such that $aQ(X), a^{-1}S(X)$ are in $R[X]$.

Proof. Choose $a, b \in F^\times$ such that $aQ(X), bS(X) \in R[X]$ are primitive. Furthermore, let $d \in R$ such that $P(X) = dP'(X)$ for some primitive $P'(X) \in R[X]$. Then,

$$(aQ(X))(bS(X)) = abP(X) = abdP'(X)$$

is primitive by Gauss's lemma. On the other hand, by construction $P'(X)$ is primitive and so, abd is a unit. Hence,

$$a^{-1}S(X) = (abd)^{-1}(bS(X))d \in R[X]$$

completing the proof. □

Corollary 5.4. Let $P(X) \in R[X]$ be monic and $Q(X) \in F[X]$ be a monic irreducible factor of $P(X)$. Then $Q(X) \in R[X]$.

Proof. By the above corollary, there exists some $a \in F^\times$ such that $aQ(X) \in R[X]$ and divides $P(X)$ in $R[X]$. Since $Q(X)$ is monic, the leading coefficient of $Q(X)$, the leading coefficient of $aQ(X)$ is a implying $a \in R$. Furthermore, the leading coefficient of $aQ(X)$ must divide the leading coefficient of $P(X)$ (which is 1), so $a \mid 1$ implying $a \in R^\times$. Hence, $Q(X) = a^{-1}aQ(X) \in R[X]$. □

This corollary is directly related to the rational root theorem which states that if $P(X) \in R[X]$ is monic and $\alpha \in F$ is a root of $P(X)$. Then, $\alpha \in R$ and divides the constant term $P(0)$.

Proposition 3.12. If $P(X) \in R[X]$ is primitive and irreducible in $R[X]$, then $P(X)$ is irreducible in $F[X]$.

Proof. Let $P(X) = Q(X)S(X)$ for some $Q(X), S(X) \in F[X]$. Then, there exists some $a \in F^\times$ such that $aQ(X), a^{-1}S(X) \in R[X]$ so that $P(X) = aQ(X)a^{-1}S(X)$. If $\deg Q(X), \deg S(X) > 0$, we have found a nontrivial factorization of $P(X)$. □

In summary, we have classified the irreducible elements in $R[X]$ with the irreducible elements of $F[X]$.

Corollary 5.5. Let $P(X) \in R[X]$. Then, if $\deg P(X) = 0$, then $P(X)$ is irreducible in $R[X]$ if and only if it is irreducible in R. On the other hand, if $\deg P(X) > 0$, then $P(X)$ is irreducible in $R[X]$ if and only if $P(X)$ is primitive and irreducible in $F[X]$.

Theorem 6. If R is a UFD, then $R[X]$ is also a UFD.

Proof. We will first prove the existence of factorizations in $R[X]$. Let $P(X) \in R[X]$ and we will induct on $\deg P(X)$. Clearly, for $\deg P(X) = 0$, $P(X) \in R$ and hence, it is factorizable in R.

In general, write $P(X) = dP'(X)$ where $d \in R$ and $P'(X) \in R[X]$ is primitive. As d is factorizable into irreducibles in R, it suffices to show $P'(X)$ factors into irreducibles in $R[X]$. Suppose $P'(X)$ is not irreducible and so (otherwise we are done), we may write $P(X) = Q(X)S(X)$ where neither $Q(X), S(X)$ have degree zero since otherwise $P(X)$ is not primitive. Hence, we are done by applying the inductive hypothesis on $Q(X)$ and $S(X)$.

In order to show the factorization is unique, it suffices for $P(X) \in R[X]$ irreducible, if $P(X) \mid Q(X)S(X)$ in $R[X]$, then either $P(X) \mid Q(X)$ or $S(X)$.

In the case that $\deg P(X) = 0$, write $Q(X) = d_1Q'(X)$ and $S(X) = d_2S'(X)$ where $d_1, d_2 \in R$ and $Q'(X), S'(X) \in R[X]$ are primitives. Then, $P(X) \mid d_1d_2Q'(X)S'(X)$ where $Q'(X)S'(X)$ is also primitive by Gauss's lemma. Thus, $P(X) \mid d_1d_2$ implying $P(X) \mid d_1$ or $P(X) \mid d_2$, and so, $P(X) \mid Q(X)$ or $P(X) \mid S(X)$ as required.

In the case that $\deg P(X) > 0$, we have $P(X)$ is primitive and irreducible in $F[X]$. Then, $P(X) \mid Q(X)S(X)$ in $R[X]$, then $P(X) \mid Q(X)S(X)$ in $F[X]$. As we already know, $F[X]$ is a UFD, and so $P(X) \mid Q(X)$ or $P(X) \mid S(X)$ in $F[X]$. WLOG. let $T(X) \in F[X]$ such that $Q(X) = T(X)P(X)$. Then, by a consequence of Gauss's lemma, there exists some $a \in F^\times$ such that $aP(X), a^{-1}T(X) \in R[X]$. As $P(X)$ is primitive, the GCD of the coefficients of $aP(X)$ must be a and so, $a \in R$. Thus, $T(X) = aa^{-1}T(X) \in R[X]$ and hence $P(X) \mid Q(X)$ in $R[X]$ as required. □

Corollary 6.1. If R is a UFD, then $R[X_1, \cdots, X_n]$ is also a UFD by induction on n.

Unlike the case with Noetherians, the quotient of UFDs is not necessarily a UFD. As example of this is $\mathbb{C}[x, y, z]/\langle xy - z^2\rangle$ (we see that $xy = z^2$ and so provides two factorizations of the same polynomial).

So far we have studied factorizations of polynomial over a ring by considering it factorization on the field of fraction. However, we have yet to fully understand factorizations of polynomials over a field.

In the case that the polynomial has degree between 2 and 3, we have an easy criterion to determine whether a polynomial is irreducible. In particular, $P(X) \in K[X]$ for K a field is irreducible if and only if $P(X)$ has no roots in K. This fails for higher degrees. Nonetheless, for finite fields, there is an algorithmic method to determining whether or not a polynomial is irreducible.

We recall that $X^{q^d} - X \in \mathbb{F}_q[X]$ is the product of the irreducible monic polynomials over $\mathbb{F}_q$ of degree dividing d.

Corollary 6.2. $P(X) \in \mathbb{F}_q[X]$ of degree d is irreducible if and only if $\gcd(P(X), X^{q^r} - X) = 1$ for all $r < d$.

Proof. Clearly, if the gcd is not 1, then $P(X)$ is not irreducible. On the other hand, if $Q(X) \mid P(X)$ and $\deg Q(X) = r$, then $Q(X) \mid X^{q^r} - X$ and so $\gcd(P(X), X^{q^r} - X) \neq 1$. □

In the case that $K = \mathbb{Q}$ the question becomes much harder and in general we do not have a complete method of determining whether or not a polynomial is irreducible over $\mathbb{Q}$. Nonetheless, we have some tricks.

In the case that $P(X) \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X]$ if $P(X)$ is monic, then it is primitive, and so, $P(X)$ is irreducible over $\mathbb{Q}$ if and only if it is irreducible over $\mathbb{Z}$.

In the more general case where $P(X) = \sum_{n=0}^{d} a_n X^n \in K[X]$ is monic (where K is the field of fractions of R), we observer that

$$P_r(X) := r^d P\left(\frac{X}{r}\right) = \sum_{n=0}^{d} r^d a_n \left(\frac{X}{r}\right)^n = \sum_{n=0}^{d} r^{d-n} a_n X^n,$$

which is also monic. Thus, if r is divisible by all denominators in P, then $P_r(X)$ lies in $R[X]$. Furthermore, by observing that if $P(X) = Q(X)S(X)$, we have $P_R(X) = Q_r(X)S_r(X)$. Hence, $P(X)$ is irreducible if and only if $P_r(X)$ is irreducible. So, in order to determine whether or not $P(X)$ is irreducible, it suffices to show $P_r(X)$ is irreducible.

Proposition 3.13. Let R be an integral domain and let $P(X) \in R[X]$ be a monic polynomial and $p \subseteq R$ be a prime ideal. Then $P(X)$ is irreducible if $\overline{P(X)} \in R/p[X]$ is irreducible.

Proof. Suppose $P(X) = Q(X)S(X)$ with Q, S not units. Then, since P is monic, so are both Q and S monic and so, $\deg Q, \deg S < \deg P$. Thus, $\overline{P(X)} = \overline{Q(X)S(X)}$ with $\deg \overline{Q(X)}, \deg \overline{S(X)} < \deg \overline{P(X)}$ implying $\overline{P(X)}$ is reducible. □

In summary, we may determine the irreducibility of a polynomial over a field of fractions by first reducing it to a polynomial over the underlying ring and then, determining its irreducibility by taking the quotient over a prime ideal. However, this method is not always applicable. In particular, there exist irreducible polynomials in $\mathbb{Z}[X]$ that are reducible over $\mathbb{F}_p$ for all p (e.g. $X^4 + 1$).

Proposition 3.14 (Eisenstein's Criterion)**.** Let $P(X) = \sum_{n=0}^{d} a_n X^n \in R[X]$ be monic where R is an integral domain. Then, if there exists a prime ideal $p \subseteq R$ such that $a_i \in p$ for all $0 \le i < d$ and $a_0 \notin p^2$, $P(X)$ is irreducible.

Proof. Suppose $P(X) = Q(X)S(X)$ with Q, S monic in $R[X]$ with positive degree. Then, taking the modulo of p, we have $X^d = \overline{Q(X)S(X)}$.

We note that as R is not necessarily a UFD, we may not directly conclude $\overline{Q(X)} = X^{\deg Q}$ and $\overline{S(X)} = X^{\deg S}$ though nonetheless, this is true. Indeed, if otherwise, we may take aX^r and bX^s be the lowest nonzero terms of $\overline{Q(X)}$ and $\overline{S(X)}$ respectively. WLOG. we may assume $r < \deg Q$, then abX^{r+s} is a nonzero term of lowest degree in $\overline{P(X)} = X^d$. But this implies $ab = 0$ in R/p which cannot happen as p is prime.

Finally, $Q(0), S(0) \in p$ and so $a_0 = P(0) = Q(0)S(0) \in p^2$ which is a contradiction. □

4 Introduction to Category Theory

Definition 4.1 (Category)**.** A category C is a collection of objects $\mathrm{Ob}(C)$ of C and for each $X, Y \in \mathrm{Ob}(C)$, a collection of morphisms $\mathrm{Hom}_C(X, Y)$ from X to Y such that,

- for $X, Y, Z \in \mathrm{Ob}(C)$, there exists a composition rule

$$\mathrm{Hom}_C(X, Y) \times \mathrm{Hom}_C(Y, Z) \to \mathrm{Hom}_C(X, Z) : (f, g) \mapsto g \circ f,$$

- for each $X \in \mathrm{Ob}(C)$, there exists an element $\mathrm{Id}_X \in \mathrm{Hom}_C(X, Y)$,
- for all $X, Y, Z, W \in \mathrm{Ob}(C)$, $f \in \mathrm{Hom}_C(X, Y), g \in \mathrm{Hom}_C(Y, Z), h \in \mathrm{Hom}_C(Z, W)$, we have $(h \circ g) \circ f = h \circ (g \circ f)$,
- for all $X, Y \in \mathrm{Ob}(C)$, $f \in \mathrm{Hom}_C(X, Y)$, $f \circ \mathrm{Id}_X = \mathrm{Id}_X \circ f = f$.

We note that we use the word collection rather than set since we can also construct the category of sets. So, if we simply consider sets then we will introduce Russell-like paradoxes. In proper set theory, the definition is phrased in terms of “classes” though we shall avoid their use here.

An example of a category is the category of groups. Indeed, Grp is a category where $\mathrm{Ob}(\mathrm{Grp}) = \{\text{Groups}\}$ and $\mathrm{Mor}(\mathrm{Grp}) = \{\text{Group homomorphisms}\}$. Similarly, we have the category of rings, topological spaces, sets, R-modules, and so on.

We can also talk about subcategories. An example of this is the category of finitely generated modules is a subcategory of modules and the category of abelian groups is a subcategory of groups.

Definition 4.2 (Isomorphism)**.** Let C be a category and let $X, Y \in \mathrm{Ob}(C)$ and $f \in \mathrm{Hom}_C(X, Y)$, then f is said to be an isomorphism if there exists $g \in \mathrm{Hom}_C(Y, X)$ such that $g \circ f = \mathrm{Id}_X$ and $f \circ g \in \mathrm{Id}_Y$.

Definition 4.3 (Covariant Functor)**.** Let C, D be categories. Then a covariant function $F : C \to D$ is collection of data

- for each $X \in \mathrm{Ob}(C)$, we obtain $F(X) \in \mathrm{Ob}(D)$,
- for each $X, Y \in \mathrm{Ob}(C)$ and $f \in \mathrm{Hom}_C(X, Y)$, we obtain $F(f) \in \mathrm{Hom}_D(F(X), F(Y))$ such that $F(\mathrm{Id}_X) = \mathrm{Id}_{F(X)}$ and $F(f \circ g) = F(f) \circ F(g)$.

Definition 4.4 (Contravariant Functor)**.** Let C, D be categories. Then a contravariant function $F : C \to D$ is collection of data

- for each $X \in \mathrm{Ob}(C)$, we obtain $F(X) \in \mathrm{Ob}(D)$,
- for each $X, Y \in \mathrm{Ob}(C)$ and $f \in \mathrm{Hom}_C(X, Y)$, we obtain $F(f) \in \mathrm{Hom}_D(F(Y), F(X))$ such that $F(\mathrm{Id}_X) = \mathrm{Id}_{F(X)}$ and $F(f \circ g) = F(g) \circ F(f)$.

A class of very useful functions which we have used in this course are the forgetful functors. These are functors which “forgets” parts of the structure of the category. For example, we have the natural forgetful function from the category of rings to the category of abelian groups by forgetting the multiplication operator.

Definition 4.5 (Natural Transformation)**.** Let C, D be categories and $F, G : C \to D$ are functors. A natural transformation ι from F to G is a collection of morphisms $\iota_X \in$

$\mathrm{Hom}_D(F(X), G(X))$ for each $X \in \mathrm{Ob}(C)$ such that for all $X, X' \in \mathrm{Ob}(C)$ and $f \in \mathrm{Hom}_C(X, X')$ the following diagram commutes,

$$\begin{tikzcd}
F(X) \arrow[r, "\iota_X"] \arrow[d, "F(f)"'] & G(X) \arrow[d, "G(f)"'] \\
F(X') \arrow[r, "\iota_{X'}"] & G(X')
\end{tikzcd}$$

i.e. $G(f) \circ \iota_X = \iota_{X'} \circ F(f)$.

We observe that we may compose natural transformations and furthermore, for each category, we can define the identity natural transformation. With this in mind, given two categories C, D, we may define the category of functors from C to D $\mathrm{Fun}(C, D)$ by taking the morphisms to be the natural transformations from C to D.

Definition 4.6 (Natural Equivalence)**.** A natural transformation $\iota : F \to G$ is a natural equivalence if it is an isomorphism in $\mathrm{Fun}(C, D)$, i.e. ι_X is an isomorphism for all $X \in \mathrm{Ob}(C)$.

Definition 4.7. Let C, D be categories and $F : C \to D$ be a functor. We say F is an equivalence of categories if there exists a functor $G : D \to C$ and natural equivalences $FG \sim \mathrm{Id}_D$ and $GF \sim \mathrm{Id}_C$.

Definition 4.8 (Adjoint Functors)**.** Let C, D be categories and $F : C \to D$, $G : D \to C$ be functors. Then (F, G) is an adjoint pair if for all $X \in \mathrm{Ob}(C), Y \in \mathrm{Ob}(D)$, there exists $\iota_{X,Y} : \mathrm{Hom}_C(X, G(Y)) \simeq \mathrm{Hom}_D(F(X), Y)$ such that, for all $f : X \to X'$ and $g : Y \to Y'$, the diagrams

$$\begin{tikzcd}
\mathrm{Hom}_C(X', G(Y)) \arrow[r, leftrightarrow, "\iota_{X',Y}"] \arrow[d, "\circ f"'] & \mathrm{Hom}_D(F(X'), Y) \arrow[d, "\circ F(f)"'] \\
\mathrm{Hom}_C(X, G(Y)) \arrow[r, leftrightarrow, "\iota_{X,Y}"] & \mathrm{Hom}_D(F(X), Y)
\end{tikzcd}$$

and

$$\begin{tikzcd}
\mathrm{Hom}_C(X, G(Y)) \arrow[r, leftrightarrow, "\iota_{X,Y}"] \arrow[d, "G(g)\circ"'] & \mathrm{Hom}_D(F(X), Y) \arrow[d, "g\circ"'] \\
\mathrm{Hom}_C(X, G(Y')) \arrow[r, leftrightarrow, "\iota_{X,Y'}"] & \mathrm{Hom}_D(F(X), Y')
\end{tikzcd}$$

commutes.