ALGEBRA - 3

SIDDHANT CHAUDHARY

These are my course notes for the **ALGEBRA-3** course which I took in my third semester. The two books used in the course were *Algebra* by *Michael Artin*, and *Abstract Algebra: The Basic Graduate Year* by *Robert Ash*. Throughout the document, the symbol ■ will stand for QED.

Contents

Date: September 2020.

1. Introduction to Rings

Definition 1.1. A *ring* R is a set with two binary operations $+$ and $\cdot$, containing *distinct* elements 0 and 1 such that the following properties hold.

(1) $(R, +, 0)$ is an abelian group.
(2) $(R, \cdot, 1)$ is a monoid.
(3) For any $a, b, c \in R$ the two distributive laws

$$a(b+c) = ab + ac$$
$$(b+c)a = ba + ca$$

hold.

Unless stated otherwise, we will assume that all our rings will be *commutative* , i.e $ab = ba$ for all $a, b \in R$.

Example 1.1. $\mathbb{Z}$ is one of the most common rings, which has a lot of special properties. $\mathbb{Z}$ is also the most important ring to study in number theory.

Example 1.2. $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are *fields*, i.e each non-zero element in these rings has a multiplicative inverse.

Example 1.3. The ring $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ is called the ring of *Gaussian Integers*.

Example 1.4. The ring $\mathbb{Z}/n\mathbb{Z}$, the usual integers modulo n which is obtained by quotienting $\mathbb{Z}$ by $n\mathbb{Z}$. Moreover, $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime number, which is one of the basic facts in number theory.

Example 1.5. The ring $\mathbb{R}[x]$, of polynomials with real coefficients in one variable, is also very important.

Example 1.6. A *non-commutative* ring which will be of interest to us will be the ring of $n \times n$ matrices with real entries.

1.1. **Initial properties.**

Let us prove some basic properties of rings.

Proposition 1.1. *Let R be an arbitrary ring. Let r, a, b, c be elements of R. Then, the following hold.*

(1) *R has a unique multiplicative identity.*
(2) $0 \cdot r = 0 = r \cdot 0$.
(3) $(-a)b = -(ab) = a(-b)$.
(4) $a(b - c) = ab - ac$.

Proof. These are naturally proved as follows.

(1) If 1 and $1'$ are two multiplicative identities for R, then we have $1 = 1 \cdot 1' = 1'$.
(2) We have the following chain of equalities.

$$0r = (0+0)r = 0r + 0r$$

and by adding the additive inverse of $0r$ to both sides, we get the result.
(3) We see that

$$0 = 0b = (a + (-a))b = ab + (-a)b$$

and the result follows. The other equality can be proven the same way.

(4) We have

$$a(b-c) = a(b+(-c)) = ab + a(-c) = ab + (-(ac)) = ab - ac$$

■

Exercise 1.1. Show that if we allow $0 = 1$ in a ring, then the ring only has one element.

Solution. This is easy to see by property (2) above, because for all $r \in R$

$$r = r \cdot 1 = r \cdot 0 = 0$$

Proposition 1.2. *Let R be a commutative ring. Then, for any $a, b \in R$ and $n \in \mathbb{N}$, we have*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

where for any $c \in \mathbb{Z}$ and $x \in R$,

$$cx := x + x + ... + x \ (n \textit{ times})$$

Proof. This is immediate by expanding the left hand side and using induction. ■

1.2. **More Definitions.** We will now see some fundamental notions in ring theory.

Definition 1.2. Let R be a ring. Any subset $S \subset R$ that is a ring with the same operations as those in R *and* and the identity is called a *subring* of R.

Example 1.7. Let $R = \mathbb{Z}/6\mathbb{Z}$ and let $S = \{0, 2, 4\}$. Notice that S is clearly an additive subgroup. Moreover, S is also closed under multiplication. However, by our definition, S is *not* a subring of R, because it does not have the same identity as that of R. It can be checked however that 4 acts as an identity for S.

Definition 1.3. Let R be a ring. An element $a \in R$ is called a *unit* in R if there is some $b \in R$ such that $ab = 1$.

Example 1.8. In $\mathbb{Z}$, the only units are ± 1. In $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, every non-zero element is a unit, since these rings are fields.

Definition 1.4. A non-zero element $a \in R$ is called a *zero-divisor* if there is some non-zero $b \in R$ such that $ab = 0$. A ring R is an *integral domain* (or just *domain*) if R has no zero divisors.

Exercise 1.2. Show that any field is a domain.

Solution. This is clear from the definition of a field, because every non-zero element is a unit, and hence it cannot be a zero-divisor.

Exercise 1.3. Show that the cancellation law holds in a domain, i.e for non-zero $a \in R$,

$$ab = ac \implies b = c$$

Solution. If $ab = ac$, then we see that $a(b-c) = 0$, and since a is non-zero and R is a domain, it follows that $b = c$. By the same reasoning, once can show that the map $x \to ax$ is injective in a domain.

Exercise 1.4. Show that any finite integral domain is a field.

Solution. Let F be any finite integral domain, and let $a \in F$ such that $a \neq 0$. Consider the map $x \to ax$, which is injective. Since F is finite, this means that there is some $b \in X$ such that $ab = 1$. Hence, F is a field.

1.3. **Homomorphisms.** In this section, we will define and study some properties of homomorphisms.

Definition 1.5. Let R, S be rings. A map $\varphi : R \to S$ is called a *ring homomorphism* if the following conditions are satisifed for $a, b \in R$.

(1) $\varphi(a + b) = \varphi(a) + \varphi(b)$.
(2) $\varphi(ab) = \varphi(a)\varphi(b)$.
(3) $\varphi(1_R) = \varphi(1_S)$.

So a ring homomorphism is a group homomorphism of the underlying abelian group that preserves multiplication and identity.

Remark 1.2.1. Since we will be mostly dealing with commutative rings in this course, we impose condition (3). However, in general, ring homomorphisms are defined without condition (3) above. Even more generally, rings are defined to not necessarily have an identity. But we don't deal with those here.

1.4. **Polynomial Rings.** In this section, we shall formally define the ring of polynomials over a commutative ring.

Definition 1.6. Let R be a (commutative) ring. Define the *ring of polynomials* over R, which will be denoted by $R[x]$, as

$$R[x] := \{(a_0, a_1, a_2, ...) \mid a_i \in R \text{ for each } i \geq 0 \text{ and } a_i \text{ is eventually zero}\}$$

So we have defined polynomials to be infinite sequences in R. A typical sequence is interpretted as the formal sum

$$a_0 + a_1 x + ... + a_n x^n$$

and hence we interpret x as the element $(0, 1, 0, 0, ...)$ of the ring.

Exercise 1.5. Define $+, \cdot$ and verify ring axioms for the ring $R[x]$. Find 1. Find a copy of R inside $R[x]$.

Solution. Let $\{a_i\}_{i\geq 0}$ and $\{b_i\}_{i\geq 0}$ be two infinite sequences in R. We define addition as

$$\{a_i\}_{i\geq 0} + \{b_i\}_{i\geq 0} := \{a_i + b_i\}_{i\geq 0}$$

and multiplication as

$$\{a_i\}_{i\geq 0} \cdot \{b_i\}_{i\geq 0} := \left\{\sum_{k=0}^{i} a_k b_{i-k}\right\}_{i\in\mathbb{N}}$$

and note that the multiplication looks like the convolution of two power series. It is rather tedious to check that these definitions make sense, but it can easily be seen by interpreting these sequences as polynomial addition and multiplication (infact, these definitions are made so that those operations remain valid). For instance, the associativity of multiplication is proven as follows (here we use the power series interpretation):

$$\begin{aligned}\sum_{n=0}^{\infty} a_n x^n \cdot \left(\sum_{n=0}^{\infty} b_n x^n \cdot \sum_{n=0}^{\infty} c_n x^n\right) &= \sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} b_k c_{n-k}\right) x^n \\ &= \sum_{n=0}^{\infty}\left(\sum_{j=0}^{n} a_j \left(\sum_{k=0}^{n-j} b_k c_{n-j-k}\right)\right) x^n \\ &= \sum_{n=0}^{\infty}\left(\sum_{j=0}^{n}\sum_{k=0}^{n-j} a_j b_k c_{n-j-k}\right) x^n\end{aligned}$$

and so in the above sum, the n^{th} coefficient of the resultant power series is the sum of all terms $a_j b_k c_m$ satisfying $j+k+m=n$, and this is clearly symmetric in j,k and m, and hence associativity follows.

It is clear that

$$1_{R[x]} = (1_R, 0, 0, ...)$$

Moreover, if we consider the map $\varphi : R \to R[x]$ given by

$$\varphi(s) = (s, 0, 0, ...)$$

then it is clear that φ is an injective homomorphism.

Remark 1.2.2. Let $p(x) \in R[x]$ be any polynomial. If

$$p(x) = a_0 + a_1 x + ... + a_n x^n$$

then we immediately have

$$p(x) = \sum_{i=0}^{\infty} (a_i, 0, 0, ...) \cdot (0, 0, ..., 1, 0, ...)$$

where the 1 appears at the i^{th} slot on the RHS.

Exercise 1.6. For which R is $\deg(fg) = \deg(f) + \deg(g)$ for non-zero $f, g \in R[x]$?

Solution. The answer is when R is an integral domain. Moreover, for the same equation to make sense when one of f, g is zero, we define the degree of the zero polynomial to be $-\infty$.

Remark 1.2.3. It is easy to see that

$$R \text{ is an integral domain } \iff R[x] \text{ is an integral domain}$$

1.4.1. *Multiple Variables.* Let us now see how to formalize the notion of a polynomial in multiple variables.

Definition 1.7. Let R be a (commutative) ring. Define

$$R[x_1, ..., x_k] = \left\{ \text{finite sums } \sum_{i_j \geq 0} a_{i_1,...,i_k} x_1^{i_1} ... x_k^{i_k} \right\}$$

and the notation

$$\sum_{\underline{i}} a_{\underline{i}} x^{\underline{i}}$$

will be used, where $\underline{i} \in \mathbb{Z}^k_{\geq 0}$. The monomial $x^{\underline{i}} = x_1^{i_1}...x_k^{i_k}$ is said to have *multidegree* $\underline{i} = (i_1, ..., i_k)$ and *total degree* $i_1 + ... + i_k$. A *homogeneous polynomial* is one in which all non-zero terms have the same total degree.

1.5. **The Substitution Principle.** Here we will see two important homomorphisms related to polynomial rings.

Theorem 1.3 (**Substitution Principle, Basic Version**). *Let R be a ring, and let $c \in R$. Then, the map* ev$_c$ *given by*

$$R[x] \xrightarrow{\text{ev}_c} R$$
$$\sum_i a_i x^i \to \sum_i a_i c^i$$

is a ring homomorphism. ev$_c$ *is called the evaluation at c.*

Proof. It is clear that $\text{ev}_c(1_{R[x]}) = 1_R$. So, we only need to check that addition and multiplication are preserved. Let $p = (a_0, a_1, ...)$ and $q = (b_0, b_1, ...)$ be two polynomials in $R[x]$. Then, observe that

$$\begin{aligned} \text{ev}_c(p+q) &= \text{ev}_c((a_0 + b_0, a_1 + b_1, ...)) \\ &= \sum_i (a_i + b_i)c^i \\ &= \sum_i a_i c^i + \sum_i b_i c^i \\ &= \text{ev}_c(p) + \text{ev}_c(q) \end{aligned}$$

and also

$$\begin{aligned} \text{ev}_c(pq) &= \sum_i \left(\sum_{k=0}^{i} a_k b_{i-k} \right) c^i \\ &= \left(\sum_i a_i c^i \right) \left(\sum_i b_i c^i \right) \\ &= \text{ev}_c(p)\text{ev}_c(q) \end{aligned}$$

where the equality on the RHS follows from the distributive law in R. This completes the proof. ■

Theorem 1.4 (**Substitution Principle, General Version**). *Given a ring homomorphism $R \xrightarrow{\varphi_0} R'$ and $c \in R'$, there exists a unique ring homomorphism $R[x] \xrightarrow{\varphi} R'$ extending φ_0 such that $\varphi(x) = c$. The corresponding commutative diagram is given below.*

$$\begin{tikzcd} R \arrow[r, hook] \arrow[d, "\varphi_0"] & R[x] \arrow[dl, "\varphi"] \\ R' & \end{tikzcd}$$

where $R \hookrightarrow R[x]$ is the inclusion map and $\varphi(x) = c$.

Proof. Define the map φ by

$$\sum_i a_i x^i \xrightarrow{\varphi} \sum_i \varphi_0(a_i) c^i \tag{$*$}$$

By similar reasoning as in the proof of **Theorem** 1.3 and using the fact that φ_0 is a homomorphism, it is immediate that φ is a homomorphism as well. Moreover, any such homomorphism φ must satisfy $(*)$, and hence the uniqueness part also follows. ■

Example 1.9. It is easily seen that ev_c as in **Theorem** 1.3 is a special case of **Theorem** 1.4, where $R' = R$ and the base map φ_0 is the identity mapping from R to itself.

Example 1.10. Let R, S be rings, and let $R \xrightarrow{\varphi_0} S$ be a given homomorphism, and we try to extend this to a homomorphism $R[x] \xrightarrow{\varphi} S[x]$. Consider the following commutative diagram.

$$\begin{tikzcd}
R \arrow[r, "\text{incl}_R"] \arrow[d, "\varphi_0"'] & R[x] \arrow[ddl, "\varphi"] \\
S \arrow[d, "\text{incl}_S"'] & \\
S[x] &
\end{tikzcd}$$

We have a homomorphism $\text{incl}_S \circ \varphi_0$ from R to $S[x]$, and we can extend this to a homomorphism $R[x] \xrightarrow{\varphi} S[x]$ such that $\varphi(x) = x$ by **Theorem** 1.4. As a concrete example, let p be a prime, and take $R = \mathbb{Z}$ and $S = \mathbb{Z}/p\mathbb{Z}$, with φ_0 the usual projection map (or reduction modulo p). Then, under this construction, the image of a polynomial with integer coefficients will be a polynomial with coefficients reduced modulo p.

Theorem 1.5 (**Substitution Principle, Multivariable Version**). *Given a ring homomorphism $R \xrightarrow{\varphi_0} R'$ and $c = (c_1, ..., c_k) \in R'^k$, there exists a unique ring homomorphism $R[x_1, ..., x_k] \xrightarrow{\varphi} R'$ extending φ_0 such that $\varphi(x_i) = c_i$ for each $1 \leq i \leq k$. The corresponding commutative diagram is given below.*

$$\begin{tikzcd}
R \arrow[r, hook] \arrow[d, "\varphi_0"] & R[x_1, ..., x_k] \arrow[dl, "\varphi"] \\
R' &
\end{tikzcd}$$

where $R \hookrightarrow R[x_1, ..., x_k]$ is the inclusion map.

Proof. The proof is the same as in **Theorem** 1.4, where multi-index notation is used. ■

Example 1.11. We can use **Theorem** 1.5 to prove the fact that $R[x, y] \cong R[x][y]$ in a very elegant fashion. To be completed.

Remark 1.5.1. The substitution principle is also called the *universal property* of polynomial rings because this property characterises polynomial rings up to unique isomorphism.

Example 1.12. We consider another application of the substitution principle. Let R be an arbitrary ring, and consider the set R^R (i.e, the set of all functions from R to R). This set has a natural ring structure, which follows from the ring structure on R, i.e R-valued functions can be added and multiplied (Caution:

multiplication here is *not* function composition) using the operations in R, and there is a zero function and a function that maps everything to the identity in R. Also, there is a natural inclusion map $R \hookrightarrow R^R$ that sends any element in R to the corresponding constant function. Now, we extend this map to a homomorphism $R[x] \xrightarrow{\text{ev}} R^R$ such that $\text{ev}(x) = \text{id}_R$ (the identity function on R) by **Theorem** 1.5. This homomorphism has a simple interpretation: any polynomial in $R[x]$ determines a function in R^R, and the homomorphism ev maps a polynomial to its corresponding function.

1.6. **Long division in Polynomial Rings.**

Here we shall encounter some usual ideas.

Theorem 1.6 (**Euclidean Division**). *Let $g(x), d(x) \in R[x]$ be polynomials where $d(x)$ is monic. Then, there exists* ***unique*** *polynomials $q(x), r(x) \in R[x]$ such that*

$$g = dq + r$$

and either $r = 0$ or $0 \leq \deg r < \deg d$.

Proof. This can easily be done by induction on the degree of g. If $\deg g < \deg d$ or $g = 0$, we can simply let $q = 0$ and $r = g$. Else, suppose $k = \deg g, l = \deg r$ with $k \geq l$. We can write

$$g(x) = ax^k + \text{lower terms}$$

and

$$d(x) = x^l + \text{lower terms}$$

and hence $g(x) - ax^{k-l}d(x)$ has deg $< k$. By induction, we can write

$$g - ax^{k-l}d = dq + r$$

where $r = 0$ or $\deg r < \deg d$. Hence, we have

$$g = d(ax^{k-l} + q) + r$$

and we are done.

Now, we move on to proving the uniqueness of q and r. Suppose

$$g = dq_1 + r_1 = dq_2 + r_2$$

where q_1, r_1 and q_2, r_2 satisfy the conditions in the statement of the theorem. So, we see that

$$r_1 - r_2 = d(q_2 - q_1)$$

It is clear that $\deg(r_1 - r_2) < \deg d$. Now, if $q_2 \neq q_1$, the last equation will imply that $\deg \text{LHS} < \deg \text{RHS}$, a contradiction. Hence, we see that $q_1 = q_2$ and $r_1 = r_2$. ■

Remark 1.6.1. This proof can be extended to the case when the leading coefficient of d is a unit. In particular, if $R = F$ is a field, then the statement holds for all $d \neq 0 \in F[x]$.

Theorem 1.7 (**Remainder/Factor Theorem**). *When $g(x) \in R[x]$ is divided by $(x - a)$, the remainder is $g(a)$.*

Proof. Observe that $(x - a)$ is monic, and hence by **Euclidean Division** 1.6, we can write

$$g(x) = q(x)(x - a) + r(x)$$

where either $r = 0$ or $\deg r < \deg(x - a) = 1$. Hence, if $r \neq 0$, we see that r is a constant polynomial, so we can write

$$g(x) = q(x)(x - a) + r$$

for some $r \in R$. Now, applying the map ev_a to both sides (which we know is a homomorphism by **Theorem** 1.3), then we have

$$g(a) = q(a)(a - a) + r = r$$

and this completes the proof of the theorem. ■

Exercise 1.7. For which rings R is it true that

$$\text{\# of distinct roots of any non-zero } g(x) \leq \deg(g)$$

Solution. The answer is exactly when R is an integral domain. First, suppose R is not an integral domain, and let $a, b \neq 0$ be zero divisors with $ab = 0$. Consider the polynomial ax. Clearly, it has two roots, contradicting the hypothesis.

Conversely, suppose R is an integral domain. We can induct on the degree of g to prove the claim. For the base case $\deg g = 0$, and there is nothing to prove. So suppose $\deg g = n > 0$. If a is a root of g, then we have

$$g(x) = (x - a)q(x)$$

for some $q(x) \in R[x]$ with $\deg q = n - 1$. Now, any *other* root b of $q(x)$ must be a root of $q(x)$, because

$$g(b) = (b - a)q(b)$$

and hence $b - a \neq 0$, implying that $q(b) = 0$ since R is a domain. By inductive hypothesis, q has atmost $n - 1$ distinct roots, and hence g has atmost n distinct roots.

1.7. More on Homomorphisms.

In this section, we will look at some important properties of *kernels* of homomorphisms.

Definition 1.8. For a ring homomorphism $R \xrightarrow{\varphi} S$, we define the *kernel* as

$$\ker(\varphi) := \{r \in R | \varphi(r) = 0\}$$

Exercise 1.8. Find the kernels of the following homomorphisms.

(1) $R[x] \xrightarrow{\text{ev}_c} R$ for $c \in R$.
(2) $R[x] \xrightarrow{\text{ev}} R^R$, atleast when R is a domain.

Solution. For (1), the kernel is simply all polynomials which have c as one of their roots. By the **Factor Theorem** 1.7, we know that this is the case if and only if the polynomial is a multiple of $(x - c)$. So, the kernel will be all multiples of $(x - c)$ (we will soon see how to frame this using ideals).

For (2), suppose first that R is an infinite integral domain. Then, any non-zero polynomial must have finitely many roots, as we saw in **Exercise** 1.7. So, the kernel of this map must be zero, and hence this map is injective.

Next, suppose R is a finite integral domain, i.e

$$R = \{a_1, ..., a_k\}$$

Consider the polynomial

$$\pi(x) = (x - a_1)...(x - a_k)$$

It is clear that $\pi(x)$ belongs to the kernel. Conversely, if a polynomial $f(x)$ is in the kernel, then all the elements $a_1, ..., a_n$ are roots of $f(x)$, and hence $\pi(x)|f(x)$ (since R is an integral domain). So it follows that the kernel is precisely all the multiples of $\pi(x)$.

Remark 1.7.1. We know that $\mathbb{R}$ is an infinite integral domain. So as we saw above, each polynomial in $\mathbb{R}[x]$ determines a *unique* function in $\mathbb{R}^{\mathbb{R}}$.

Remark 1.7.2. It can be easily shown that any *finite* integral domain is a field, but that is not important for this exercise.

1.8. **Ideals and More Homomorphisms.** Let us begin with the notion of an *ideal* in a ring.

Definition 1.9. Let R be any ring (not necessarily commutative). A subset I of R is called a (2-sided) *ideal* of R if I is an additive subgroup of R, and for any $a \in I$ and $r \in R$, it is true that $ar \in I$ and $ra \in I$.

Remark 1.7.3. In many sources, *ideals* are defined to be subrings which absorb multiplication. However, within our system of definitions, ideals *need not* be subrings as they need not contain the identity element.

Definition 1.10. Let R be a commutative ring, and let $a \in R$. The set

$$\{ra \mid r \in R\}$$

is called the *principal ideal* generated by a.

Example 1.13. Let F be a field. We show that the only ideals in F are the trivial ones, i.e 0 and F, and infact this property characterises fields. If F is a field, suppose I is any non-zero ideal. Then, $a \in I$ for some $a \neq 0$. Since I is an ideal, it must be true that $1 = aa^{-1} \in I$, and this means that $I = F$. So, the only ideals of F are 0 and F. Conversely, if the only ideals of a (commutative) ring F are the trivial ones, then we can show that every non-zero element is a unit. Infact, this is simple because we can just consider the principal ideal generated by a non-zero element, which will be the whole ring F, showing that the element must be a unit, i.e F must be a field.

Example 1.14. It can be shown that every ideal of $\mathbb{Z}$ and $F[x]$ is principal, where F is a field. This is true because both rings have a Euclidean Algorithm (we will see more of these rings further), and any ideal will be generated by an element contained in it with the least *size*, which in the case of $\mathbb{Z}$ is the absolute value, and in the case of $F[x]$, is the degree.

Example 1.15. In this and subsequent examples, we will be finding all homomorphisms from a given ring to another ring R. Here, we have to find all possible homomorphisms $\mathbb{Z} \xrightarrow{\varphi} R$. Since $1 \xrightarrow{\varphi} 1_R$, we see that

$$\varphi(k) = \begin{cases} 1_R + 1_R + ... + 1_R \quad (k \text{ times}) & , \ k > 0 \\ -\varphi(-k) & , \ k < 0 \end{cases}$$

and hence if a homomorphism exists, it is unique. Moreover, we can *define* the map φ as above, and it is easily checked that this is a homomorphism. So there is precisely one homomorphism from $\mathbb{Z}$ to R.

Definition 1.11. The unique homomorphism $\mathbb{Z} \xrightarrow{\varphi} R$ in **Example** 1.15 above is called the *characteristic map* of R, and is denoted $\mathbb{Z} \xrightarrow{\text{char}} R$. If the kernel of this map is $n\mathbb{Z}$ for some *unique* $n \geq 0$, then n is called the *characteristic* of R, and this number is denoted by char(R).

Remark 1.7.4. The characteristic of a ring R can equivalently be defined as the smallest natural number n (if it exists) such that $n \cdot 1_R = 0_R$. If no such number exists, the characteristic of R is then defined to be 0.

Exercise 1.9. If R is an integral domain, then what are the possible values of char(R)?

Solution. Suppose char$(R) \neq 0$. Then, it must be that char$(R) = p$ for some prime p. To prove this, suppose $p = ab$ for some $a, b \in \mathbb{Z}$. Then,

$$0 = p \cdot 1_R = (a \cdot 1_R)(b \cdot 1_R)$$

Since R is an integral domain, one of $a \cdot 1_R$ or $b \cdot 1_R$ must be zero, i.e one of a or b is $\pm p$ (because p is the least such integer), and hence p must be a prime.

Exercise 1.10. Find the kernel of the unique homomorphism $\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{C}$ where $x \to a$ for some fixed $a \in \mathbb{C}$ (the homomorphism is unique by the **Substitution Principle** 1.4.) Find the kernel explicitly for $a = \sqrt{2}, i, 1/3, \sqrt[n]{2}$ etc.

Solution. We will show that no matter what a is, the kernel will *always* be a principal ideal generated by *some* element of $\mathbb{Z}[x]$. First, suppose there is *no* polynomial in $\mathbb{Z}[x]$ for which $p(a) = 0$. Then, the kernel is simply the zero ideal, which we know is principal. So, suppose that the kernel is non-empty, i.e

$$\text{Ker } \varphi = \{p(x) \in \mathbb{Z}[x] \mid p(a) = 0\} \neq \phi$$

Let $d(x)$ be any element of *least degree* in Ker φ, and we also make the choice that the gcd of the coefficients of $d(x)$ is 1 (if it is not 1, then we can factor out the gcd from all the coefficients). We claim that

$$\text{Ker } \varphi = (d(x))$$

To prove this, suppose $p(x) \in$ Ker φ. We know that $p(x)$ and $d(x)$ are both polynomials in the ring $\mathbb{Q}[x]$. Since $\mathbb{Q}$ is a field, **Euclidean Division** 1.6 holds, and there are polynomials $q(x), r(x) \in \mathbb{Q}[x]$ such that

$$p(x) = q(x)d(x) + r(x)$$

where either deg $r <$ deg d or $r(x) = 0$. Let l_1 be the LCM of the denominators of the coefficients of $q(x)$, and similarly let l_2 be the LCM of the denominators of the coefficients of $r(x)$ (so that $l_1, l_2 \in \mathbb{Z}[x]$). Then, we can write

$$q(x) = \frac{q'(x)}{l_1} \text{ and } r(x) = \frac{r'(x)}{l_2}$$

where $q'(x), r'(x) \in \mathbb{Z}[x]$. So we get

$$l_1 l_2 p(x) = l_2 q'(x)d(x) + l_1 r'(x)$$

and this is an equation in $\mathbb{Z}[x]$. Clearly, we see that

$$l_1 r'(a) = 0$$

and hence $r'(a) = 0$. Since $\deg r'(x) = \deg r(x) < \deg d(x)$, by the *definition* of $d(x)$ it must be true that $r'(x) = 0$. Hence, we get

$$l_1 l_2 p(x) = l_2 q'(x)d(x) \implies l_1 p(x) = q'(x)d(x)$$

Suppose s is the gcd of the coefficients of $p(x)$. Then, the gcd of the coefficients of $l_1 p(x) = l_1 s$, and hence the gcd of the coefficients of $q'(x)d(x)$ is $l_1 s$. By our assumption, the gcd of the coefficients of $d(x)$ was 1, and hence it must be true that the gcd of the coefficients of $q'(x)$ is $l_1 s$. All this fuss was to show that

$$\frac{q'(x)}{l_1} \in \mathbb{Z}[x]$$

so that $p'(x)$ is divisible by $d(x)$. This shows that

$$\text{Ker } \varphi = (d(x))$$

completing the proof.

Some specific examples are given below.

$$\begin{aligned} a &= 2 & \text{Ker } \varphi &= (x^2 - 2) \\ a &= i & \text{Ker } \varphi &= (x^2 + 1) \\ a &= 1/3 & \text{Ker } \varphi &= (3x - 1) \\ a &= \sqrt[n]{2} & \text{Ker } \varphi &= (x^n - 2) \end{aligned}$$

Definition 1.12. For a subset $A = \{a_1, ..., a_n\}$ of a ring R, the set

$$\left\{ \sum_{i=1}^{n} r_i a_i \mid r_i \in R \right\}$$

is called the ideal of R *generated by* A. This is also denoted by $(a_1, ..., a_n)$ and is the *smallest* ideal of R containing A.

Example 1.16. Consider the ring $F[x, y]$ for some field F, and let

$$I_1 := \{f(x, y) \mid \text{constant term of } f = 0\}$$

We claim that

$$I_1 = (x, y)$$

so that I_1 is not a principal ideal. Suppose I_1 is a principal ideal, say $I_1 = (g)$. Since $x, y \in I_1$, we see that $g|x$ and $g|y$. But clearly, this is not possible, because the only choice for g is either a unit a or ax for some unit a, and either case is not possible.

Remark 1.7.5. In the ring $F[x, y]$, the polynomials x, y behave like prime numbers, and infact $F[x, y]$ has unique factorization. But unlike $\mathbb{Z}$, $F[x, y]$ does not have diophantine equations at our disposal.

Example 1.17. Here we consider another example of non-principal ideals. Let F be a field. Put

$$I_n := (x^n, x^{n-1}y, ..., y^n) \subset F[x, y]$$

Analogously, for a prime $p \in \mathbb{Z}$, put

$$J_n := (p^n, p^{n-1}y, ..., y^n) \subset \mathbb{Z}[y]$$

We show that I_n, J_n are non-principal ideals, and infact I_n, J_n cannot be generated by fewer than $n + 1$ elements. To be completed

Example 1.18. Consider the homomorphism $\mathbb{R}[x,y] \to \mathbb{R}[t]$ that is identity on the real numbers and that maps $x \mapsto t^2$ and $y \mapsto t^3$. Observe that the polynomial $y^2 - x^3$ is in the kernel of this homomorphism. We will show that the kernel is infact (y^2-x^3). It is clear that any polynomial in (y^2-x^3) will belong to the kernel. Conversely, suppose $g(x,y)$ belongs to the kernel. Now, identify $\mathbb{R}[x,y] \cong \mathbb{R}[x][y]$. Observe that $y^2 - x^3$ is a polynomial monic polynomial in y. So, by **Euclidean Division** 1.6, there are polynomials $q(x,y), r(x,y) \in \mathbb{R}[x][y]$ such that

$$g(x,y) = (y^2 - x^3)q(x,y) + r(x,y)$$

where either $r(x,y) = 0$ or the degree of y in $r(x,y)$ is *less* than the degree of y in $y^2 - x^3$, which is 2. We will show that $r(x,y) = 0$. We can write

$$r(x,y) = r_1(x)y + r_2(x)$$

where $r_1(x), r_2(x) \in \mathbb{R}[x]$. Moreover, it is also clear that $r(x,y)$ belongs to the kernel of the homomorphism. In particular, this means that

$$r_1(t^2)t^3 + r_2(t^2) = 0$$

Observe that $r_1(t^2)t^3$ has odd degree, while $r_2(t^2)$ has even degree. So, the only possibility is that $r_1 = r_2 = 0$, i.e $r(x,y) = 0$, implying that $g(x,y) \in (y^2 - x^3)$. This completes the proof.

1.9. **Operations on Ideals and Quotients.** We will now look at some operations on ideals.

Definition 1.13. Let R be an arbitrary ring, and let $I_1, ..., I_k$ be ideals in R. Define

$$I_1 \cdots I_k := \left\{ \sum_{i=1}^{n} a_{i1}a_{i2}...a_{ik} \mid a_{ij} \in I_j, n \geq 0 \right\}$$

and it can be easily checked that $I_1 \cdots I_k$ is an ideal of R.

Definition 1.14. A ring R is said to be a *principal ideal domain* (PID) if every ideal or R is principal.

Exercise 1.11. Let R be a PID, and let $a, b \in R$. What can be said about the ideals $aR \cdot bR$, $aR \cap bR$ and $aR + bR$?

Solution. It is easy to see that $aRbR = (ab)$, i.e the ideal generated by ab. Now, because R is a PID, we have

$$aR \cap bR = lR$$

for some $l \in R$, and we call l the *least common multiple* of a, b, denoted by lcm(a,b). Finally,

$$aR + bR = dR$$

where the element $d \in R$ is said to be the *greatest common divisor* of a, b, denoted by gcd(a,b) (we will soon define these terms).

Definition 1.15. Let R be a ring, and let I be a *proper* (2-sided) ideal of R. Consider the quotient group R/I, where R, I are seen as abelian groups. On this quotient group, define multiplication as

$$(a+I)(b+I) = ab + I$$

Then this definition makes R/I into a ring, and this ring is called the *quotient ring*.

Remark 1.7.6. In the above definition, we require the ideal to be *proper* because of our very definition of rings. In our definition, every ring must contain a multiplicative identity distinct from 0. Another reason why we require I to be proper is because of our definition of *ring homomorphisms* (in particular, the identity must be mapped to the identity), as we see in the next proposition.

Proposition 1.8. *Let R be a ring and let I be a proper ideal. Then the natural projection $R \xrightarrow{\pi} R/I$ is a ring homomorphism with* Ker *$\pi = I$.*

Proof. This is immediate from the definition of quotient rings. ■

Corollary 1.8.1. *Let R be a ring. A proper subset I of R is an ideal if and only if it is the kernel of some (ring) homomorphism.*

Proof. One direction is clear by **Proposition** 1.8. The other direction, that any kernel of some homormorphism is a proper ideal is clear by the definition of a homomorphism. This completes the proof. ■

Definition 1.16. Let R be a ring. A proper ideal P of R is called a *prime ideal* if given $ab \in P$ atleast one of a or b is in P, where $a, b \in R$.

Proposition 1.9. *Let R be a ring and let P be a proper ideal. Then, P is a prime ideal if and only if R/P is an integral domain. So, this can equivalently be taken as a definition of prime ideals.*

Proof. First suppose P is a proper ideal. To show that R/P is an integral domain, it is enough to show that there are no zero divisors. Let $\overline{a}$ denote the coset of an element $a \in R$ in R/P. Suppose

$$\overline{a} \cdot \overline{b} = \overline{ab} = 0$$

This implies that $ab \in P$, and hence one of a or b is in P, implying that one of $\overline{a}$ or $\overline{b}$ is 0. The converse is proven similarly. ■

Definition 1.17. Let R be a ring, and let M be a proper ideal of R. Then M is said to be a *maximal ideal* if the only ideals in R containing M are R and M. Equivalently, M is *maximal* if for any $a \notin M$, $aR + M = R$.

Proposition 1.10. *Let R be a ring and let M be a proper ideal. Then, M is a maximal ideal if and only if R/M is a field.*

Proof. This follows immediately by the **Correspondence Theorem** 1.13 and the fact that a ring is a field if and only if its only ideals are the trivial ones. ■

Remark 1.10.1. The above theorem implies that any maximal ideal is a prime ideal, because every field is also an integral domain.

Example 1.19. Let us see prime and maximal ideals in $F[x]$, where $F \in \{\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{F}_p\}$.To be completed.

1.10. **First Isomorphism Theorem.**

First I will begin by introduce the abstract notion of *quotienting by equivalence relations*. It may be a familiar idea, and it is ubiquitious in different parts of mathematics.

Definition 1.18. Let S be any set, and let $\sim$ be an equivalence relation on S. The *quotient set* of S by the relation $\sim$ is the set of all equivalence classes of the relation $\sim$, and this set is denoted by $S/\sim$.

Definition 1.19. Let S, T be two sets, and let $f : S \to T$ be a (set) map. Define a relation $\sim$ on S by: $x \sim y$ if and only if $f(x) = f(y)$. Then, $\sim$ is an equivalence relation on S, and $\sim$ is said to be *induced* by f. For any $t \in T$, the equivalence class $f^{-1}(t)$ is called a *fiber* of f.

Here is an abstract fact about quotienting.

Theorem 1.11 (**Isomorphism Theorem for Sets**). *Let $f : S \to T$ be a set map, and suppose $\sim$ is an equivalence relation on S with the quotient map $\pi : S \to S/\sim$. Then, there exists a function $\overline{f} : (S/\sim) \to T$ such that $f = \overline{f} \circ \pi$ if and only if every equivalence class of S under $\sim$ is contained in some fiber of f. Moreover, $\overline{f}$ has the following properties.*

(1) *If $\overline{f}$ exists, it is unique. Also, $\overline{f}$ is surjective if and only if f is surjective.*
(2) *$\overline{f}$ is injective if and only if each equivalence class of S under $\sim$ is equal to some fiber of f.*

Remark 1.11.1. If such an $\overline{f}$ exists, then f is said to *factor through* the quotient $S/\sim$.

Proof. Most of the theorem is just abstract non-sense; there is nothing hard to be proven. I will not write the proof right now. ■

We now state and prove the **First Isomorphism Theorem** 1.12 for groups, vector spaces and rings. A group homomorphism/linear map/ring homomorphism will be simply called a *morphism*.

Theorem 1.12 (**First Isomorphism Theorem**). *Let S, T be groups/vector spaces/rings, and let $f : S \to T$ be a given morphism. Also, suppose $S \xrightarrow{\pi} S/I$ is a given quotient morphism, where I is a normal subgroup/subspace/ideal of S. Then the following hold.*

(1) *$\exists\ S/I \xrightarrow{\overline{f}} T$ with $f = \overline{f} \circ \pi$ if and only if $I \subseteq$ Ker f. Moreover, such an $\overline{f}$ is unique and* Im$(f) =$ Im$(\overline{f})$.
(2) *$\overline{f}$ is injective if and only if $I =$ Ker f. In that case, $S/I \xrightarrow{\overline{f}}$ Im(f) is an isomorphism.*

Proof. For (1), it is clear that if such a map exists, then $I \subseteq$ Ker f and that $\overline{f}$ is unique. So, we only need to prove the existence in the case when $I \subseteq$ Ker f. For any coset $x + I \in S/I$ for any $x \in S$, we define $\overline{f} : S/I \to T$

$$\overline{f}(x + I) = f(x)$$

and because $I \subseteq$ Ker f, this map is a well-defined homomorphism with $f = \overline{f} \circ \pi$. (2) is easy to see. ■

1.11. **Correspondence Theorem.** This is also a very important isomorphism theorem in algebra. Let us begin by proving this theorem for groups.

Theorem 1.13. *Let G be any group, and let $N \trianglelefteq G$ (i.e normal subgroup). Let the quotient map be $G \xrightarrow{\pi} G/N$. Then, there is an inclusion preserving bijection between subgroups/normal subgroups of G/N and subgroups of G containing N.*

Proof. Suppose $f : S \to T$ is any *surjective* group homomorphism, where S, T are any groups. We will use the following two facts, which are elementary.

(1) For any subgroup/normal subgroup K of S, $f(K)$ is a subgroup/normal subgroup of T.
(2) For any subgroup/normal subgroup K of T, $f^{-1}(K)$ is a subgroup/normal subgroup of S *containing* Ker f.

Note that surjectivity of f is required to prove the first statement above when K is a normal subgroup. This gives us the required bijection: for any subgroup/normal subgroup K of G containing N, map K to $\pi(K)$. Similarly, if K is any subgroup/normal subgroup of G/N, its inverse image will be $\pi^{-1}(K)$. This gives us the required bijection (There are a lot of details to be filled in, however they are not difficult and make a good exercise). ■

Remark 1.13.1. Let us be a little more precise. Suppose H is *any* subgroup of G, i.e H need not contain N. Still, $\pi(H)$ is a subgroup of G/N, and hence under the above correspondence, $\pi(H)$ has a partner subgroup in G that contains N. It is easy to see that HN is a subgroup of G containing N, and hence the partner subgroup of $\pi(H)$ in G under the above correspondence is HN. Note that if $N \subseteq H$, then $HN = H$. Also, note that $\pi(H) = \{hN \mid h \in H\} = HN/N$. So, we have that $H \xrightarrow{\pi|_H} HN/N$ is a surjective map, and the kernel of this map is clearly $H \cap N$. So by the **First Isomorphism Theorem** 1.12, we see that $H/(H \cap N) \cong HN/N$. This is usually called the **Second Isomorphism Theorem**. For vector spaces, this isomorphism theorem reads $(U + V)/V \cong U/(U \cap V)$, where U, V are subspaces of a vector space W. For rings, this isomorphism theorem reads $(S+I)/I \cong S/(S \cap I)$, where S is any subring of a ring R, and I is any ideal of R.

Example 1.20. Consider the evaluation map ev$_c : R[x] \to R$ given by $x \mapsto c$. The kernel of this map is $(x - c)$, and hence by the **First Isomorphism Theorem** 1.12 we get

$$R[x]/(x - c) \cong R$$

Example 1.21. Consider the map $f : \mathbb{Z}[x] \to \mathbb{C}$ given by $x \mapsto i$. We see that Im $f = \mathbb{Z}[i]$, and as in **Exercise** 1.10 we see that Ker $f = (x^2 + 1)$. By the **First Isomorphism Theorem** 1.12, we get

$$\mathbb{Z}[x]/(x^2 + 1) \cong \mathbb{Z}[i]$$

Example 1.22. Let $\mathbb{Z} \to \mathbb{F}_p$ be the reduction homomorphism, where p is any prime. Then consider the reduction homomorphism $\mathbb{Z}[x] \to \mathbb{F}_p[x]$ such that $x \mapsto x$ and this map is clearly surjective. It is easy to see that Ker $= p\mathbb{Z}[x]$, and hence we get

$$\mathbb{Z}[x]/p\mathbb{Z}[x] \cong \mathbb{F}_p[x]$$

Example 1.23. Let us show that $R[x, y]/(y - x^3) \cong R[t]$. Consider the unique map $R[x, y] \xrightarrow{\varphi} R[t]$ that restricts to the standard inclusion $R \hookrightarrow R[t]$ on R and maps $x \mapsto t$, $y \mapsto t^3$. Just like in **Example** 1.18, it can be shown using **Euclidean Division** 1.6 that the kernel of this map is $(y - x^3)$. It is also easy to see that this map is surjective. Hence, by the **First Isomorphism Theorem** 1.12, it follows that $R[x, y]/(y - x^3) \cong R[t]$.

Example 1.24. Using the map given in **Example** 1.18, we can show that $R[x, y]/(y^2 - x^3)$ is isomorphic to the subring of $R[t]$ of all polynomials having no term of linear degree. Try to make this more precise.

Example 1.25. We try to figure out how the quotient $\mathbb{Z}[i]/(3+i,7)$ looks like. To be completed. This is the 0 ring.

Example 1.26. We try to figure out how the quotient $\mathbb{Z}[i]/(3+i,8)$ lookslike. To be completed.

Exercise 1.12. What can you say about the following rings: $\mathbb{Z}[i]/(2)$, $\mathbb{Z}[i]/(10+i)$ and $\mathbb{Z}[i]/(3)$?

Solution. To be completed.

1.12. **Combining the Isomorphism Theorems.** Here, we will see that the combination of the isomorphism theorems is a very strong tool.

Suppose R, S are rings, and suppose $R \xrightarrow{f} S$ is a surjective map. Then, by the **Correspondence Theorem** 1.13, there is an inclusion preserving bijection between ideals of S and ideals of R containing Ker$f$. Note that this is not a direct application of the **Correspondence Theorem** 1.13 we proved, but since $R/\text{Ker } f \cong S$, we might as well just work with S instead of the quotient $R/\text{Ker } f$.

Now, let K be an ideal of S, and consider the maps $R \xrightarrow{f} S \xrightarrow{\pi} S/K$. Clearly, the kernel of this composition is $f^{-1}(K)$ (note that $f(f^{-1}(K)) = K$, since f is surjective). Put $J = f^{-1}(K)$. So, by the **First Isomorphism Theorem** 1.12, we see that

$$R/J = R/f^{-1}(K) \cong S/K = S/f(J)$$

If we consider the special case when f is itself a quotient map, we can recover the so called **Third Isomorphism Theorem**.

As an application, let R be any ring and let $a, b \in R$. Let $J = aR + bR$ and let $I = aR$, so that $I \subset J$. Consider the surjective map $R \xrightarrow{\pi} R/aR$. Now observe that $\pi(J) = J/I = aR + bR/aR$. So by the above discussion (or the **Third Isomorphism Theorem**) we see that

$$\frac{R}{aR+bR} \cong \frac{R/aR}{(aR+bR)/aR}$$

Now it can be easily seen that $\bar{b}$, the image of b under in the quotient $aR+bR/aR$, generates this quotient. Hence, the above isomorphism can be written as

$$\frac{R}{aR+bR} \cong \frac{R/aR}{(\bar{b})}$$

and hence

$$\frac{R/(a)}{(\bar{b})} \cong \frac{R}{(a,b)}$$

and note that $\bar{b}$ is the image of b in the quotient $(aR+bR)/aR$. We can reverse the roles of a, b above, and we get

$$\frac{R/(a)}{(\bar{b})} \cong \frac{R}{(a,b)} \cong \frac{R/(b)}{(\bar{a})}$$

This isomorphism is interpretted as follows. We want to introduce new relations by collapsing a, b to zero. This can be first done by collapsing a, followed by collapsing b, or the other way around. This isomorphism says that no matter which order we choose, the resultant will be the same.

Example 1.27. Let $R = \mathbb{Z}[x]$ and $a = x^2+1$. Let $b = p$ for some prime p. The above isomorphism spells out

$$\frac{\mathbb{Z}[i]}{(p)} \cong \frac{\mathbb{Z}[x]}{(x^2+1,p)} \cong \frac{\mathbb{Z}[x]/(p)}{(\overline{x^2+1})} \cong \frac{\mathbb{F}_p[x]}{(x^2+1)}$$

where we used the fact that $\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[i]$. Now $\mathbb{F}_p$ is a field, and the ring $\mathbb{F}_p[x]/(x^2+1)$ is a *field* if and only if x^2+1 does not have any roots in $\mathbb{F}_p$. To be completed.

1.13. **Product Rings and Idempotents.** We can define *products* of an arbitrary collection of rings without much work, but for simpler notation we will just work with two rings first.

Definition 1.20. Let R_1, R_2 be any two rings. Define the *product* $R_1 \times R_2$ to be the *cartesian product* of these sets, which ring operations are done componentwise.

One can prove the universal property of the product easily.

Proposition 1.14. *Let S, R_1, R_2 be rings and suppose $S \xrightarrow{f_1} R_1, S \xrightarrow{f_2} R_2$ be homomorphisms. Then, there is a unique homomorphism $S \xrightarrow{f} R_1 \times R_2$ that matches f_1 and f_2 in the corresponding components.*

This gives us an external view of the product ring. Let us now have an internal view of the same.

Definition 1.21. An element $e \in R$ is said to be an *idempotent* if $e^2 = e$.

Theorem 1.15. *Let S be any ring. Then, $S \cong R_1 \times R_2$ for some rings R_1, R_2 if and only if S contains non-trivial idempotents.*

Proof. First, suppose $S \cong R_1 \times R_2$ for some rings R_1, R_2. Then, it is easy to see that the elements $(1,0)$ and $(0,1)$ are non-trivial idempotents in this ring.

Conversely, suppose S contains a non-trivial idempotent e, i.e $e^2 = e$ and $e \neq 0, 1$. We claim that

$$S \cong eS \times (1-e)S$$

where it can be easily seen that $(1-e)$ is also an idempotent. First, it is easy to see that eS is infact a ring, where the multiplicative identity is e (because e is an idempotent). However, eS is not a *subring*, because $e \neq 1$. Similarly, $(1-e)S$ is also a ring with identity $(1-e)$.

Now, consider the map $S \xrightarrow{\varphi} eS \times (1-e)S$ given by $s \to (es, (1-e)s)$. It is easy to check that this map is a ring homomorphism. We show that this is an isomorphism. First, suppose $s \in \operatorname{Ker} \varphi$. This means that $es = (1-e)s = 0$. Multiply both sides by e to get

$$es = e(1-e)s$$

but since e is an idempotent, the RHS is zero, implying that $es = 0$. But this implies that $(1-e)s = 0$, i.e $s = 0$. So φ is an injective map. To prove surjectivity, suppose $(ea, (1-e)b) \in eS \times (1-e)S$. Put $s = ea + (1-e)b$. Then it can be checked that $(es, (1-e)s) = (ea, (1-e)b)$, and this shows that φ is surjective. This completes the proof. ■

Example 1.28. Let us see an interesting case of combining the isomorphism theorems with products. Let R be a PID, and let $a, b \in R$ such that $\gcd(a, b) = 1$. In this case, we see that $(a, b) = R$ or equivalently $aR + bR = R$. Consider the quotient maps $R \xrightarrow{\pi_1} R/aR$ and $R \xrightarrow{\pi_2} R/bR$. Then, we have a map $R \xrightarrow{\pi_1 \times \pi_2} R/aR \times R/bR$.

It is clear that the kernel of this map is $aR \cap bR = aR \cdot bR = (ab)R$, and this is because the given ideals are coprime (proof required! However this is a special case of the CRT, which I have proven in HW-3). Using coprimality, we can also show that the map $\pi_1 \times \pi_2$ is surjective too. Hence, we have an isomorphism

$$R/(aR \cap bR) = R/(abR) \cong R/aR \times R/bR$$

Theorem 1.16 (**Chinese Remainder Theorem**). *Let R be any ring, and let $I_1, ..., I_k$ be ideals of R such that $I_i + I_j = R$ for each $i \neq j$, i.e the given ideals are pairwise coprime. Then,*

$$I_1 \cap ... \cap I_k = I_1 \cdot ... \cdot I_k$$

and the map

$$R/(I_1 \cdot ... \cdot I_k) = R/(I_1 \cap ... \cap I_k) \to R/I_1 \times ... \times R/I_k$$

given by

$$s \mapsto (s + I_1, ..., s + I_k)$$

is an isomorphism.

Proof. Proved in HW-3. ■

Example 1.29. Let us analyze the ring $F[x]/(x^2 + 4)$ where $F \in \{\mathbb{C}, \mathbb{R}, \mathbb{F}_2\}$. If $F = \mathbb{C}$, then we have the factorisation $(x^2 + 4) = (x + 2i)(x - 2i)$. Moreover, observe that $(x + 2i) - (x - 2i) = 4i$, and hence the ideals $(x + 2i), (x + 2i)$ are coprime in $\mathbb{C}[x]$. Applying the **CRT** 1.16, we have

$$\mathbb{C}[x]/(x^2 + 4) \cong \mathbb{C}[x]/(x + 2i) \times \mathbb{C}[x]/(x - 2i)$$

Now it is easy to see that both factors on the RHS are copies of $\mathbb{C}$. Hence, we see that $\mathbb{C}[x]/(x^2 + 4) \cong \mathbb{C}^2$.

If $F = \mathbb{R}$, then $x^2 + 4$ is an *irreducible*, and hence $\mathbb{R}[x]/(x^2 + 4)$ is a *field*. Moreover, it is not hard to see that $\mathbb{R}[x]/(x^2 + 4) \cong \mathbb{C}$.

Finally, if $F = \mathbb{F}_2$, then $x^2 + 4 = x^2$, so that $\mathbb{F}_2/(x^2)$ has a *nilpotent element*, namely $\overline{x}$. This is not possible in a field or product of fields.

Example 1.30. Here we analyze the ring $R[t]/(t^2 - t)$ for any ring R. Note that $t^2 - t = t(t - 1)$, and both the ideals (t) and $(t - 1)$ are coprime. So, it follows that

$$R[t]/(t^2 - t) \cong R[t]/(t) \times R[t]/(t - 1) \cong R^2$$

Exercise 1.13. Find a ring with exactly 21 ideals. Can you find one with characteristic 3 as well?

Solution. To be completed. Hint is $\mathbb{Z}/p^{20}\mathbb{Z}$

Exercise 1.14. Let R_1, R_2 be any rings. Show that ideals of $R_1 \times R_2$ are of the form $I_1 \times I_2$, where I_1 is an ideal of R_1 and I_2 is an ideal of R_2.

Solution. To be completed.

Exercise 1.15. Find an infinite ring R and a non-zero $f(x) \in R[x]$ such that $\text{ev}(f) = 0$ function in R^R. Use product rings.

Solution. To be completed.

1.14. **Fraction Fields.** In this section, we will see a generalisation of the construction of $\mathbb{Q}$ from the integral domain $\mathbb{Z}$.

Definition 1.22. Let D be any integral domain. Consider the set $D \times D/\{0\}$, i.e all elements of the form (a, b) with $b \neq 0$. Define a relation $\sim$ on this set as follows:

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

Proposition 1.17. *The relation $\sim$ as above is an equivalence relation on $D \times D/\{0\}$.*

Proof. Reflexivity and symmetry of $\sim$ are easy to see. Only transivity remains to be proven. So suppose

$$(a, b) \sim (c, d) \sim (e, f)$$

and so we have

$$ad = bc \quad , \quad cf = de$$

which implies that

$$afd = bcf = bde$$

and hence by cancelling d, we get $af = be$, which means $(a, b) \sim (e, f)$. This completes the proof. ■

Definition 1.23. Let D be an integral domain with $\sim$ as defined above. Consider the quotient set $(D \times D/\{0\})/\sim$, and denote any equivalence class $\overline{(a, b)}$ by the fraction $\frac{a}{b}$. On this quotient set, define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{cd} \quad , \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ab}{cd}$$

Then, it can be checked (check it!) that these operations are well-defined and make the quotient set into a *field* with

$$0 = \frac{0}{1} \quad , \quad 1 = \frac{1}{1}$$

This field is called the *fraction field* of D and is denoted by Fr(D).

Theorem 1.18 (Universal Property of Fr(D)). *Let D be any integral domain, and let* Fr(D) *be the field of fractions of D. Then the following properties hold.*

1. *The map $D \overset{i}{\hookrightarrow}$* Fr$(D)$ *given by $a \mapsto a/1$ is an injective homomorphism.*
2. *For any $u \neq 0$ in D, $i(u)$ is a unit in* Fr(D).
3. *If for some ring R there is a ring homomorphism $D \xrightarrow{\varphi} R$ such that $\varphi(u)$ is a unit in R for any $u \neq 0$, then φ factors uniquely through* Fr(D) *via i, i.e there is a unique homomorphism Ψ such that the following diagram commutes.*

$$\begin{tikzcd} D \arrow[r, "\varphi"] \arrow[d, "i"] & R \\ \mathrm{Fr}(D) \arrow[ur, "\Psi"] & \end{tikzcd}$$

Remark 1.18.1. Thus we can regard an integral domain D as a subring of its fraction field Fr(D).

Proof. Let us prove (1) and (2) together. To prove that i is injective, it is enough to show that Ker $i = 0$. So suppose $a \in$ Ker i, implying that

$$\frac{a}{1} = \frac{0}{1}$$

and clearly this implies that $a = 0$. This proves (1). To prove (2), suppose $a \neq 0 \in D$. Then, the inverse of $\frac{a}{1}$ is simply $\frac{1}{a}$, so that $i(a)$ is a unit. This proves (2).

Now, let us prove the given universal property in (3). Suppose R is a ring such that $D \xrightarrow{\varphi} R$ is a homomorphism with the given property. First, let us prove the *uniqueness* of the homomorphism Ψ, given that it exists. Let $a/u \in$ Fr(D). Then, we see that

$$\varphi(u)\Psi(a/u) = \Psi(u)\Psi(a/u) = \Psi(a/1) = \varphi(a)$$

where above we used the fact that Ψ restricts to φ on D. The above equation implies that

$$\Psi(a/u) = \varphi(a)\varphi(u)^{-1}$$

and hence uniqueness of Ψ follows. To prove existence, just *define* Ψ on Fr(D) by the above formula. This completes the proof. ■

Example 1.31. Let F be a field, and consider $F[x]$. The fraction field Fr$(F[x])$ is called the *field of rational functions* over F. It contains fractions of the form $p(x)/q(x)$ where $q(x)$ is a non-zero polynomial in $F[x]$.

Example 1.32. Let F be any field, and consider the characteristic map $\mathbb{Z} \xrightarrow{\text{char}} F$. If this map is injective, then any non-zero element of $\mathbb{Z}$ maps to a *unit* in F and hence F contains $\mathbb{Q}$ as a subfield, by the **Universal Property** 1.18. If it is not, then the kernel is of the form $p\mathbb{Z}$ for some prime p, and in that case F will contain $\mathbb{Z}/p\mathbb{Z}$ as a subfield.

1.15. **Adjoining Elements.**

We will see two situations where we want to attach new elements to a ring. The first is a concrete case and the second will be attaching a new element abstractly.

Definition 1.24. Let $R \subset S$ be rings such that R is a subring of S. Let $\alpha \in S$. Define

$$R[\alpha] := \left\{ \sum_{i=0}^{n} r_i \alpha^i \mid r_i \in R \right\}$$

Then, $R[\alpha]$ is the *smallest subring* of S that contains R and α. We can similarly define $R[A]$, where A is *any* subset of S, to be the *smallest subring* of S containing R and each element of A.

Let us try to relate $R[\alpha]$ to the polynomial ring $R[x]$, where R, α are as above. Consider the unique homomorphism $R[x] \xrightarrow{\varphi} R[\alpha]$ that restricts to the inclusion on R and that maps $x \to \alpha$. Suppose the kernel of this map is a principal ideal generated by a monic polynomial, i.e Ker $\varphi = (g(x))$ where $g(x)$ is a monic polynomial in $R[x]$. Then by the first isomorphism theorem, we see that

$$R[\alpha] \cong \frac{R[x]}{(g(x))}$$

Moreover, notice that $R[x]/(g(x))$ is an R-*module* with basis elements $\overline{1}, \overline{x}, \overline{x^2}, ..., \overline{x^{n-1}}$ where $n =$ deg$(g(x))$ (a *module* is just a vector space over a ring). So, this gives

$R[\alpha]$ an R-module structure with basis elements $1, \alpha, ..., \alpha^{n-1}$. Note that this discussion is always true when $R = F$ is a *field*. In that case, we have some definitions.

Definition 1.25. Let F, E be fields such that F is a subfield of E. Let $\alpha \in E$, and let $F[x] \xrightarrow{\varphi} F[\alpha]$ be the homomorphism as above. If Ker $\varphi = 0$, then α is said to be *trancendental* over F. If Ker $\varphi \neq 0$, then α is said to be *algebraic* over F. In simple words, *algebraic* elements are those which are roots of non-zero polynomials in $F[x]$, while *trancendental* elements are those which do not satisfy any non-zero polynomial in $F[x]$. If α is algebraic over F, the unique monic polynomial of minimal degree that generates Ker φ is called *the minimal polynomial of* α *over* F. If g is the minimal polynomial of α over F, then

$$\text{dim}_F F[\alpha] = \text{deg}(g(x)) = \text{degree of } \alpha \text{ over } F$$

Theorem 1.19. *Let E, F be fields with F a subfield of E, and let $\alpha \in E$. Then*

$$\alpha \textit{ is trancendental over } F \iff F[\alpha] \cong F[x] \iff \text{dim}_F F[\alpha] = \infty$$

Proof. The first equivalence is clear by the definition of trancendental numbers. The first and last equivalence are also clear by the definition of trancendental numbers (very lazy proof but its not difficult anyway). ■

Theorem 1.20. *Let E, F be fields with F a subfield of E, and let $\alpha \in E$. Then*

$$\alpha \textit{ is algebraic over } F \iff F[\alpha] \textit{ is a field} \iff \text{dim}_F F[\alpha] < \infty$$

Moreover, if α is algebraic over F, then its minimal polynomial is irreducible in $F[x]$.

Proof. Let us prove the equivalence of the first and last statements. If α is algebraic, then the map $F[x] \xrightarrow{\varphi} F[\alpha]$ given by $x \to \alpha$ has kernel Ker $\varphi = (g(x))$, where $g(x)$ is the minimal polynomial of α over F. In that case, we see that

$$F[\alpha] \cong \frac{F[x]}{(g(x))}$$

so that $\text{dim}_F F[\alpha] < \infty$. Conversely, if $\text{dim}_F F[\alpha] < \infty$, then the map φ *cannot* be injective, as $F[x]$ is an infinite dimensional vector space. So, φ is *not* injective, and hence α is algebraic over F.

Let us now prove the equivalence of the first two statements. If α is algebraic over F, then again we see that $F[\alpha] \cong F[x]/(g(x))$. Since $F[\alpha] \subset E$, $F[\alpha]$ is an integral domain, and hence $F[x]/(g(x))$ is an integral domain, implying that $(g(x))$ is a prime ideal. But this also implies that $g(x)$ is *irreducible* in $F[x]$, and hence this means that $F[x]/(g(x))$ is actually a *field*, so that $F[\alpha]$ is a field. Conversely, if $F[\alpha]$ is a field, then the map φ *cannot* be injective, because we know that $F[x]$ is not a field. So, it follows that α is algebraic over F. ■

Example 1.33. Consider the fields $\mathbb{Q} \subset \mathbb{C}$, and let $\sqrt[3]{2} \in \mathbb{C}$. Then, it can be checked that $x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$, and hence

$$\mathbb{Q}[\sqrt[3]{2}] \cong \frac{\mathbb{Q}[x]}{(x^3 - 2)}$$

Definition 1.26. Let R be any ring, and let A be a set of polynomials over R, i.e let A be any arbitrary subset of $R[x]$. *Attaching* or *adjoining* an element α to R satisfying polynomial conditions given in A means taking the quotient

$$\frac{R[x]}{(A)}$$

where (A) is the ideal generated by the set A. Intuitively, we are *adding* a new element α to our ring R such that α is a root of each polynomial in the set A.

Remark 1.20.1. As opposed to what one might think, attaching/adjoining new elements to rings abstractly as above need not mean adding in the colloquial sense. This is because the inclusion map $R \hookrightarrow R[x]/(A)$ need not be injective. As an example, suppose we want to adjoin an element α to $\mathbb{Z}/4\mathbb{Z}$ such that $2\alpha = 1$, i.e we want to attach an inverse of 2 to $\mathbb{Z}/4\mathbb{Z}$. The ring we will obtain is $\mathbb{Z}/4\mathbb{Z}[x]/(2x-1)$, and observe that

$$\frac{\mathbb{Z}/4\mathbb{Z}[x]}{(2x-1)} \cong \frac{\mathbb{Z}[x]}{(4, 2x-1)} \cong \frac{\mathbb{F}_2[x]}{(-1)} = 0$$

i.e this gives us the trivial ring.

Example 1.34. Suppose we attach an element α to $\mathbb{R}$ such that $\alpha^3 = 1$. This is the same as the quotient

$$\frac{\mathbb{R}[x]}{(x^3-1)} = \frac{\mathbb{R}[x]}{(x-1)(x^2+x+1)}$$

Now $(x-1)$ and (x^2+x+1) are coprime ideals. So by the CRT we have

$$\frac{\mathbb{R}[x]}{(x^3-1)} \cong \frac{\mathbb{R}[x]}{(x-1)} \times \frac{\mathbb{R}[x]}{(x^2+x+1)} \cong \mathbb{R} \times \mathbb{C}$$

Let F be a field, and let $g(x) \in F[x]$ be an irreducible polynomial. Then, $F[x]/(g(x))$ is a *field*; not only this, this is a field *containing* F, so it is a *field extension*. We denote

$$\frac{F[t]}{(g(t))} := F[\bar{t}]$$

where $\bar{t}$ is the attached root of $g(x)$ to F. Observe that by *construction*, the minimal polynomial of $\bar{t}$ over F is $g(t)$.

Exercise 1.16. Let F, E be fields with F a subfield of E. Let $\alpha, \beta \in E$ be algebraic elements over F. Then, show that a ring homomorphism $F[\alpha] \xrightarrow{\varphi} F[\beta]$ such that $\varphi(\alpha) = \beta$ and $\varphi|_F = \text{id}$ exists if and only if the minimal polynomials of α and β over F are equal.

Solution. To be completed.

2. Factorisation

2.1. **Unique Factorisation Domains.**

We begin with some basic definitions.

Definition 2.1. Let R be a ring. Elements $a, b \in R$ are said to be *associates* if $a = ub$ for some unit $u \in R$. If $c = ka$, then we say a *divides* c and that a is a *factor* of c. An element $p \in R$ is said to be *irreducible* if every factor of p is either a unit or an associate of p. We don't regard units as irreducibles.

Definition 2.2. An integral domain R is said to be a *unique factorisation domain* (UFD) if every non-zero non-unit element of R has a factorisation into a product of irreducibles in R, and the factorisation is unique upto the ordering of the irreducible factors and upto multiplying every irreducible factor by a unit.

So if R is a PID and if x is any non-zero non-unit in R, then we can write

$$x = p_1p_2...p_k$$

where each p_i is an irreducible in R, and that this factorisation is unique upto ordering of the factors and multiplying each factor by a unit. We will now prove a characteristaion of UFDs.

Theorem 2.1. *A domain D is a UFD if and only if:*

(1) *every irreducible is prime.*
(2) *Each infinite chain $(b_1) \subsetneq (b_2) \subsetneq (b_3) \subsetneq ...$ is eventually constant.*

Proof. Let's prove the forward direction first. So let D be a UFD, and let p be an irreducible. Let $a, b \in D$ such that $ab \in (p)$, implying that $ab = pk$, for some $k \in D$. Now, consider the unique prime factorisation of ab, which is clearly the product of the factorisations of a and b. The factorisation of pk contains p as an irreducible. Since $ab = pk$, this means that the factorisation of ab must contain an associate of p, which is true by unique factorisation. So, atleast one of a or b contains an associate of p in their factorisation, proving that one of a, b is in (p), and hence p is a prime. Next, suppose

$$(b_1) \subsetneq (b_2) \subsetneq (b_3) \subsetneq ...$$

is an infinite chain, implying that b_{i+1} is a *proper* factor of b_i for each i. In particular, b_i for $i \geq 2$ is a *proper* factor of b_1. Suppose the factorisation of b_1 is

$$b_1 = p_1p_2...p_k$$

So upto associates, b_1 has atmost 2^k distinct factors. This means that the chain must be eventually constant. This proves the forward direction.

The backward direction is also similarly proven. So suppose D is a domain in which properties (1) and (2) are satisfied. Let us first show that if factorisation into irreducibles exists, then it is indeed *unique*. This is a consequence of property (1). So let a be a non-zero non-unit such that

$$a = p_1p_2...p_k = q_1q_2...q_l$$

where each $p_1, ..., p_k, q_1, ..., q_l$ is an irreducible. Then, we see that

$$p_1|q_1...q_l$$

and since p_1 is an irreducible, it is a prime as well (which is property (1)). So, without loss of generality suppose $p_1|q_1$ after rearranging the q_i's if necessary. Because q_i is an irreducible, this implies that p_i and q_i are associates. So, we cancel them from either side of the equation, and continue this process. This proves *uniqueness* of factorisation. We will now show *existence* of factorisation as a result of property (2). So let b_1 be any non-zero non-unit in D. If b_1 is an irreducible, then we are done. If not, we claim that b_1 has an irreducible factor. To see this, observe that we can factor b_1 as $b_1 = p_1q_1$, where p_1 and q_1 are not units, which means that $(b) \subsetneq (p_1)$. If p_1 is an irreducible, then our claim is proven. Otherwise, again write $p_1 = p_2q_2$ as a product of non-unit factors. This way, we will get a chain

$$(b_1) \subsetneq (p_1) \subsetneq (p_2) \subsetneq ...$$

and by property (2), this chain is eventually constant. The corresponding generator will be an irreducible, and hence b_1 has an irreducible factor, say t_1. So we can write

$$b_1 = t_1b_2$$

where b_2 is not a unit. Again, if b_2 is an irreducible, then this is the required factorisation. Otherwise, $(b_1) \subsetneq (b_2)$. Continuing the same way, we see that b_2 has an irreducible factor, say t_2 so that $b_2 = t_2b_3$, and hence

$$b_1 = t_1b_2 = t_1t_2b_3$$

Continuing this way, we will get a chain

$$(b_1) \subsetneq (b_2) \subsetneq (b_3) \subsetneq ...$$

and by another application of property (2), we see b_1 indeed factors into irreducibles. This proves the existence part of the theorem, and hence we are done. ■

Remark 2.1.1. Rings in which condition (2) holds are examples of the so called *Noetherian Rings*. So any non-zero non-unit element of a ring satisfying condition (2) can be factored into irreducibles, but uniqueness of this factorisation need not hold.

Here is a more general fact about the relationship between irreducibles and primes.

Proposition 2.2. *Let D be any domain. Any prime in D is also an irreducible. Hence, by* **Theorem** 2.1*, irreducibles and primes are the same entity in any UFD.*

Proof. Let p be any prime in D. Suppose $p = ab$. Then, either $p|a$ or $p|b$, i.e either a or b is a unit. This proves the primes are irreducibles in domains. The rest of the statement is immediate. ■

Proposition 2.3. *Let D be any UFD, and let $a, b \in D$. Then* $\gcd(a, b)$ *exists, but need not be a linear combination of a and b.*

Remark 2.3.1. Note that in a PID, gcds can be written as linear combinations.

Proof. Let a, b be two elements. Suppose

$$a = \prod_{i=1}^{k} p_i^{\alpha_i}$$

$$b = \prod_{i=1}^{k} p_i^{\beta_i}$$

where each p_i is an irreducible and $\alpha_i, \beta_i \geq 0$. Then it is easy to see that

$$\gcd(a, b) = \prod_{i=1}^{k} p_i^{\min\{\alpha_i,\beta_i\}}$$

and hence gcds exist in D. Now, consider $\mathbb{Z}[x]$. We will show that $\mathbb{Z}[x]$ is a UFD. Moreover, we have

$$(2, x) = 1$$

but 1 cannot be written as a linear combination of 2 and x. ■

Proposition 2.4. *Let D be a domain. If* gcd(a, b) *exists for every $a, b \in D$, then every irreducible is prime in D. So, condition* (1) *of* **Theorem** 2.1 *can be replaced by the existence of gcds.*

Proof. Let p be any irreducible in D, and suppose $ab \in (p)$. So, we see that gcd$(ab, p) = p$. To be completed. ■

Example 2.1. We will see an example of a ring where irreducibles need not be primes. Consider the ring $\mathbb{Z}[\sqrt{-5}]$. For any element $a + b\sqrt{-5}$, we have *its* norm

$$N(a + b\sqrt{-5}) = a^2 + 5b^2$$

So, it is easy to see that condition (2) of **Theorem** 2.1 holds for this ring. However, observe that

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

and it is easy to see that $2, 3, 1+\sqrt{-5}$ and $1-\sqrt{-5}$ are all irreducibles in $\mathbb{Z}[\sqrt{-5}]$ by using the multiplicativity of the norm. Moreover, none of these are associates to each other. Hence, uniqueness of factorisation doesn't hold in this ring.

Example 2.2. Next, we will look at an example of a ring which violates condition (2) of **Theorem** 2.1. Consider the ring $\mathbb{Z} + x\mathbb{Q}[x]$, i.e all polynomials in $\mathbb{Q}[x]$ with integer constant terms. We have

$$\left(\frac{x}{2}\right) \subsetneq \left(\frac{x}{4}\right) \subseteq \left(\frac{x}{8}\right) \subsetneq \dots$$

Theorem 2.5. *Every PID is a UFD.*

Proof. We will apply **Theorem** 2.1 here. First, suppose p is an irreducible and suppose $ab \in (p)$. If $a \in (p)$, then we are done. Otherwise, let $(a, p) = (d)$, so that d is gcd(a, p). Since p is an irreducible, we see that d is a unit, i.e $(a, p) = R$, so that

$$ax + py = 1$$

for some $x, y \in R$. Multiplying both sides by b, we see that $b \in (p)$. So, every irreducible element is prime.

Next, suppose there is a chain

$$(b_1) \subsetneq (b_2) \subsetneq \dots$$

Take the union of all these ideals, i.e consider

$$I = \bigcup_{i \in \mathbb{N}} (b_i)$$

Clearly, I is an ideal, and it is a principal ideal, so that $I = (b)$ for some element $b \in R$. Clearly, $b = b_n$ for some n, and hence this chain is eventually constant. This completes our proof. ■

2.2. **Euclidean Domains.**

This is another important class of integral domains.

Definition 2.3. An integral domain D is called a *Euclidean Domain* if there is a function $\sigma : D \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that for each b and non-zero d in D, there are q and r in D such that $b = dq + r$ with $r = 0$ or $\sigma(r) < \sigma(d)$.

Proposition 2.6. *Every Euclidean Domain is a PID.*

Proof. The proof is really simply. Consider any ideal of the domain. If it is the zero ideal, then we are done. Otherwise, consider the element of having the least value of σ, and claim that this element generates the ideal (this is really like proving the Division Algorithm in Number Theory). ■

Example 2.3. It is *not* true that every PID is a Euclidean Domain. A counterexample is the ring

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$$

but proving so is not very easy.

Theorem 2.7. *$\mathbb{Z}[i]$ is a Euclidean Domain where the norm function σ is $\sigma(a+ib) = (a+ib)(a-ib) = a^2+b^2$.*

Proof. Check HW-2 for a proof. ■

2.3. **Gaussian Primes.** We have seen that $\mathbb{Z}[i]$ is a Euclidean Domain. In particular, it is a PID as well as a UFD. In this section, we will try to characterise primes in the ring $\mathbb{Z}[i]$, called *Gaussian Primes*. Note that because $\mathbb{Z}[i]$ is a PID, it is a UFD and hence we can interchangeably use the words *prime* and *irreducible* by the courtesy of **Proposition** 2.2. Here are some basic facts about $\mathbb{Z}[i]$.

Proposition 2.8. *The following facts hold in the ring $\mathbb{Z}[i]$.*

(1) *Let $n, k, l \in \mathbb{Z}$ and $n \neq 0$. Then $n|k+li$ in $\mathbb{Z}[i]$ if and only if $n|k$ and $n|l$ in $\mathbb{Z}$.*
(2) *$m+ni|k+li \implies m-ni|k-li$. This is because conjugation is a ring automorphism of $\mathbb{Z}[i]$.*
(3) *The only units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$.*

Proof. (1) and (2) are immediate. (3) can be seen using the multiplicativity of the norm in $\mathbb{Z}[i]$. ■

Proposition 2.9. *Let p be any prime in $\mathbb{Z}$. Then, exactly one of the two possibilities below holds.*

(1) *p is a prime in $\mathbb{Z}[i]$. In this case, p cannot be written as a sum of two squares in $\mathbb{Z}$, i.e $p \neq k^2+l^2$ for $k, l \in \mathbb{Z}$.*
(2) *$p = \pi\overline{\pi}$ for a Gauss prime $\pi = k+il$, where k, l are non-zero integers in $\mathbb{Z}$. Hence, $p = k^2+l^2$ in $\mathbb{Z}$.*

Proof. Suppose p is a prime in $\mathbb{Z}[i]$. Then, we claim that p *cannot* be written as a sum of two squares in $\mathbb{Z}$. This is because if $p = k^2+l^2$ for some $k, l \in \mathbb{Z}$, then clearly $k, l \neq 0$, and hence

$$p = (k+il)(k-il)$$

and neither of the terms on the RHS are units, implying that p is *not* a prime. So, we see that p cannot be written as a sum of two squares.

Next, suppose p is a prime in $\mathbb{Z}[i]$. Let π be an irreducible factor of p, i.e $\pi|p$. So we can write $p = \pi \cdot z$, for some $z \in \mathbb{Z}[i]$. Observe that

$$N(p) = p^2 = N(\pi)N(z)$$

and hence this means that $N(\pi) = N(z) = p$, i.e $\pi\overline{\pi} = p$. Now,

$$z = p/\pi = p\overline{\pi}/\pi\overline{\pi} = p\overline{\pi}/p = \overline{\pi}$$

So, we see that $p = \pi\overline{\pi}$, and also p is a sum of two squares. This completes the proof. ■

Theorem 2.10. *Let π be any Gaussian prime. Then, either π is an associate of an integer prime or $N(\pi)$ is a prime in $\mathbb{Z}$.*

Proof. Let π be any Gaussian prime. If π is an associate of an integer prime, then there is nothing to prove. So suppose π is *not* an associate of any integer prime. It is easy to see that $\overline{\pi}$ is a Gaussian prime (in particular, use (2) of **Proposition** 2.8). We claim that $N(\pi) = \pi\overline{\pi}$ is a prime in $\mathbb{Z}$. For the sake of contradiction, suppose $N(\pi)$ is *not* a prime in $\mathbb{Z}$. Then, $p_1p_2|N(\pi)$ for some primes $p_1, p_2 \in \mathbb{Z}$. By **Proposition** 2.9, three cases are possible.

(1) p_1 and p_2 are Gauss primes. In this case, observe that in the prime factorisation of $N(\pi)$, both p_1 and p_2 occur. However, $\pi\overline{\pi}$ is already *the* factorisation of $N(\pi)$ in $\mathbb{Z}[i]$. This means that after reordering if necessary, $\pi \sim p_1$ and $\overline{\pi} \sim p_2$, a contradiction to the fact that π is not associate to any integer prime.

(2) In the second case, exactly one of p_1 or p_2 is not a Gauss prime. Wlog suppose p_1 is a Gauss prime. Then $p_2 = \pi_0\overline{\pi_0}$ for some Gauss prime π_0. But this contradicts the uniqueness of factorisation of $N(\pi)$ in $\mathbb{Z}[i]$, because there are two prime factors $\pi, \overline{\pi}$ in the factorisation, but p_1, π_0 and $\overline{\pi_0}$ all occur in the factorisation of $N(\pi)$.

(3) In the last case, both p_1 and p_2 are not Gauss primes. So $p_1 = \pi_1\overline{\pi_1}$ and $p_2 = \pi_2\overline{\pi_2}$ for Gauss primes π_1 and π_2. Again, this contradicts the number of prime factors in the factorisation of $N(\pi)$ in $\mathbb{Z}[i]$.

So in all cases, there is a contradiction. Hence, $N(\pi)$ must be a prime. This completes the proof. ■

2.4. **Sum of Squares.** In this section, we will use the tools that we have developed to answer the question of when a positive integer is a sum of two squares.

Proposition 2.11. *An integer prime $p > 0$ is a sum of two squares if and only if p is not a Gauss prime, which is true if and only if $\mathbb{Z}[i]/(p)$ is not a field. So, a prime p is a sum of two squares if and only if $\dfrac{\mathbb{F}_p[x]}{(x^2+1)}$ is a not field, i.e if and only if x^2+1 has a root in $\mathbb{F}_p$.*

Proof. First, suppose an prime p can be written as a sum of two squares, i.e $p = k^2 + l^2$, where $k, l \neq 0$. Then we see that $p = (k+il)(k-il)$, and both of these are irreducibles in $\mathbb{Z}[i]$. So, p is not a Gauss prime. Conversely, if p is not a Gauss prime then by **Proposition** 2.9 we see that $p = \pi\overline{\pi}$ for some Gauss prime π. So, $p = N(\pi)$ and hence p can be written as a sum of two squares.

Because $\mathbb{Z}[i]$ is a PID, p is not a Gauss prime if and only if (p) is not a maximal ideal, which is true if and only if $\mathbb{Z}[i]/(p)$ is not a field. The rest of the statement is clear because we know that

$$\frac{\mathbb{Z}[i]}{(p)} \cong \frac{\mathbb{F}_p[x]}{(x^2+1)}$$

■

Theorem 2.12. *x^2+1 has a root in $\mathbb{F}_p$ if and only if $p = 2$ or $p = 1(\text{mod } 4)$, where p is a positive prime integer.*

Proof 1. Let us show the easy implication first. Suppose x^2+1 has a root in $\mathbb{F}_p$, where p is an odd prime. If α is a root, then we see that $\alpha^2 + 1 = 0$, i.e $\alpha^2 = -1$.

This implies that α has order 4 in the group $\mathbb{F}_p^\times$ of units. Since $|\mathbb{F}_p^\times| = p-1$, this implies that $4|p-1$, and hence $p = 1(\text{mod } 4)$.

Now we prove the converse, which is harder. If $p = 2$, it is clear that x^2+1 has a root in $\mathbb{F}_2$. So, we can assume that p is an odd prime and $p = 1(\text{mod } 4)$. We need to show that x^2+1 has a root in $\mathbb{F}_p$, i.e -1 is a square in $\mathbb{F}_p$. Observe that -1 is the *unique* element of order 2 in $\mathbb{F}_p^\times$; this is because $-1, 1$ are both roots of x^2-1, and since this is a polynomial of degree 2, these are the *only* roots. So, we have to show that this unique element of order 2 is a square in $\mathbb{F}_p^\times$. Consider the homomorphism $\varphi : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ given by $x \to x^2$ (since $\mathbb{F}_p^\times$ is an abelian group, this is indeed a group homomorphism). The image of φ is the group of all squares in $\mathbb{F}_p^\times$. Moreover, by what we have seen above,

$$\text{Ker } \varphi = \{1, -1\}$$

So we see that

$$\text{Group of all squares} \cong \frac{\mathbb{F}_p^\times}{\{1,-1\}}$$

Now the order of the group $\dfrac{\mathbb{F}_p^\times}{\{1,-1\}}$ is even, because $\dfrac{p-1}{2}$ is divisible by 2. So by Cauchy's Theorem, the group of all squares in $\mathbb{F}_p^\times$ has an element of order 2, i.e -1 is contained in the group of all squares, and hence the polynomial x^2+1 has a root in $\mathbb{F}_p$. This completes the proof. ■

Proof 2. For a second proof, we will use the result of **Theorem** 3.15. So, we know that $\mathbb{F}_p^\times$ is a cyclic group. So, we see that $\mathbb{F}_p^\times$ contains an element of order 4 if and only if $4||\mathbb{F}_p^\times|$, i.e if and only if $p = 1(\text{mod } 4)$. If this element is α, then just as in the first proof, we have $\alpha^2 = -1$. ■

Theorem 2.13. *Let n be any positive integer. Then, n can be written as a sum of two squares if and only if every prime factor in the prime factorisation of n that is 3 mod 4 has even power.*

Proof. Suppose $n \in \mathbb{Z}$ can be written as a sum of two squares. We claim that all prime factors which are 3 mod 4 occur with an even power in the factorisation of n. Suppose $n = k^2 + l^2 = (k+il)(k-il)$. Also, suppose

$$n = p_1^{t_1}...p_k^{t_k}$$

be the prime factorisation of n. Let p_i be a prime that is 3 mod 4. So, observe that in $\mathbb{Z}[i]$, p_i is still a prime and hence it occurs in prime factorisation of n in $\mathbb{Z}[i]$. Now, we know that $p_i|(k+il)(k-il)$ in $\mathbb{Z}[i]$. Since p_i is a Gauss prime, we see that either $p_i|(k+il)$ or $p_i|(k-il)$. But, this implies that p_i divides both of them, and hence p_i^2 divides n. This shows that p_i occurs with an even power, i.e t_i is even.

Conversely, suppose n has a prime factorisation in $\mathbb{Z}$ in which all primes that are 3 mod 4 occur with an even power. We write this factorisation as

$$n = 2^r p_1^{t_1}...p_k^{t_k} q_1^{s_1}...q_l^{s_l}$$

where each p_i is 1 mod 4 and each q_i is 3 mod 4. Observe that each q_i remains a Gauss prime, but each p_i can be factored as

$$p_i = \pi_i \overline{\pi_i}$$

where π_i is a Gauss prime. Also, we have that

$$2^r = (1+i)^r(1-i)^r$$

Now, we want to find $A + iB \in \mathbb{Z}[i]$ such that

$$n = (A+iB)(A-iB)$$

We now appeal to property (2) of **Proposition** 2.8 to find all the possible factorisations of $A+iB$. Note that if q^x is an irreducible factor of $A+iB$, then $\overline{q}^x$ will be an irreducible factor of $A-iB$. Keeping this is mind, we see that we can put

$$A+iB = u(1+i)^r(\pi_1^{c_1}\overline{\pi_1}^{d_1})...(\pi_k^{c_k}\overline{\pi_k}^{d_k})q_1^{s_1/2}...q_l^{s_l/2}$$

where u is some unit, and $c_i + d_i = t_i$. In this case, the factorisation of $A - iB$ will be

$$A-iB = \overline{u}(1-i)^r(\pi_1^{d_1}\overline{\pi_1}^{c_1})...(\pi_1^{d_k}\overline{\pi_1}^{c_k})q_1^{s_1/2}...q_l^{s_l/2}$$

and hence $n = (A+iB)(A-iB)$, i.e n can be written as a sum of two squares. Infact, we have also found the number of ways of writing n as a sum of two squares; there are four choices for the unit u, and since $c_i + d_i = t_i$, there are (t_i+1) choices for the pair (c_i, d_i). This gives us a total of $4(t_1+1)...(t_k+1)$ choices for $A+iB$, i.e the number of ways of writing n as a sum of two squares. ■

2.5. **Gauss Lemma.** Consider the rings $\mathbb{Z}[x] \subset \mathbb{Q}[x]$. The question which we ask is this: given a polynomial in $\mathbb{Z}[x]$, is there any way in which we can use $\mathbb{Q}[x]$ to decide whether the polynomial is irreducible in $\mathbb{Z}[x]$? What we would like to say is something like this:

$(*)$ *A polynomial is irreducible in $\mathbb{Z}[x]$ iff. it is irreducible in $\mathbb{Q}[x]$*

However, the above is *not* true. As a basic example, consider $2x \in \mathbb{Z}[x]$. Clearly, $2x$ reduces in $\mathbb{Z}[x]$ to non-trivial factors 2 and x. However, $2x \in \mathbb{Q}[x]$ is indeed irreducible. So to say that a polynomial is irreducible in $\mathbb{Z}[x]$ if and only if it is irreducible in $\mathbb{Q}[x]$ is not quite right. The problem here is that the coefficient 2 is irreducible in $\mathbb{Z}$. We will see that this is infact the *only* problem that arises, i.e if we factor out the gcd of the coefficients of the given polynomial, the statement in $(*)$ is infact true.

Definition 2.4. $f \in \mathbb{Z}[x]$ is said to be a *primitive polynomial* if the gcd of the coefficients of f is 1. So, all monic polynomials are primitive.

Proposition 2.14 (**Gauss' Lemma on Primitive Polynomials**). *Suppose $f, g \in \mathbb{Z}[x]$ are primitive polynomials. Then, fg is also a primitive polynomial.*

Proof. Clearly, the gcd of the coefficients of $f(x)g(x)$ is *not* zero, since $\mathbb{Z}[x]$ is an integral domain. For the sake of contradiction, suppose the gcd of the coefficients of $f(x)g(x)$ is *not* 1. Then, there is some prime $p \in \mathbb{Z}$ such that $p|f(x)g(x)$. Consider the reduction homomorphism $\varphi : \mathbb{Z}[x] \to \mathbb{F}_p[x]$. Clearly, we see that

$$0 = \varphi(f(x)g(x)) = \varphi(f(x))\varphi(g(x))$$

Since $\mathbb{F}_p[x]$ is an integral domain, this implies that one of $\varphi(f(x))$ or $\varphi(g(x))$ is 0, which contradicts the fact that $f(x)$ and $g(x)$ are primitive polynomials. This completes the proof. ■

Remark 2.14.1. This proof is valid over $D[x]$, where D is any UFD.

Theorem 2.15 (**Gauss' Lemma on Irreducibility**). *Let f be a primitive polynomial in $\mathbb{Z}[x]$. Then, f is irreducible in $\mathbb{Z}[x]$ if and only if it is irreducible in $\mathbb{Q}[x]$.*

Proof. We will prove both of these statements by proving the contrapositive, i.e if f is any primitive polynomial in $\mathbb{Z}[x]$, then f factors in $\mathbb{Z}[x]$ if and only if it factors in $\mathbb{Q}[x]$.

One direction is clear; if f factors in $\mathbb{Z}[x]$, then it clearly factors in $\mathbb{Q}[x]$ as well. So, we only need to show the harder direction.

So let $f \in \mathbb{Z}[x]$ be a primitive polynomial. Suppose f factors in $\mathbb{Q}[x]$, i.e

$$f(x) = g(x)h(x)$$

for some $g(x), h(x) \in \mathbb{Q}[x]$ such that neither $g(x)$ nor $h(x)$ are units in $\mathbb{Q}[x]$, or equivalently they have degree atleast 1. Now, we write

$$g(x) = \frac{g'(x)}{u}$$

where u is the lcm of the denominators of the coefficients of g, which implies that $g'(x) \in \mathbb{Z}[x]$. Next, let a be the gcd of the coefficients of $g'(x) \in \mathbb{Z}[x]$, and hence

$$g'(x) = ag_0(x)$$

where $g_0(x) \in \mathbb{Z}[x]$ is a primitive polynomial. So,

$$g(x) = \frac{a}{u}g_0(x)$$

Similarly, write

$$h(x) = \frac{b}{v}h_0(x)$$

for where $h_0(x) \in \mathbb{Z}[x]$ is a primitive polynomial. So, we have the equation

$$f(x) = \frac{ab}{uv}g_0(x)h_0(x)$$

and hence

$$uvf(x) = abg_0(x)h_0(x)$$

and this is clearly an equation in $\mathbb{Z}[x]$. Because g_0, h_0 are primitive, we know that $g_0(x)h_0(x) \in \mathbb{Z}[x]$ is also primitive by **Gauss' Lemma** 2.14. So, this clearly implies that $uv = ab$, and hence $f(x)$ factors in $\mathbb{Z}[x]$. This completes the proof. ■

So we can compile all results we have shown in the following statement.

Theorem 2.16 (**Irreducibles in $\mathbb{Z}[x]$**). *Irreducibles in $\mathbb{Z}[x]$ are of two types: integer primes p, and primitive polynomials $f \in \mathbb{Z}[x]$ that are irreducible in $\mathbb{Q}[x]$.*

Proposition 2.17. *Let $f_0, g_0 \in \mathbb{Z}[x]$ such that $f_0 | g_0$ in $\mathbb{Q}[x]$ and f_0 is primitive in $\mathbb{Z}[x]$. Then, $f_0 | g_0$ in $\mathbb{Z}[x]$.*

Proof. We can write $g_0(x) = f_0(x)h(x)$, for some $h(x) \in \mathbb{Q}[x]$. As before, we write

$$h(x) = \frac{a}{u}h_0(x)$$

where $h_0(x) \in \mathbb{Z}[x]$ is a primitive polynomial. So,

$$ug_0(x) = ah_0(x)f_0(x)$$

Again, $h_0(x)f_0(x)$ is primitive over $\mathbb{Z}[x]$ by **Gauss' Lemma** 2.14. So this implies that $u|a$, and hence $h(x) \in \mathbb{Z}[x]$. Hence, $f_0|g_0$ over $\mathbb{Z}[x]$, and this completes the proof. ■

Corollary 2.17.1. *Let $\alpha \in \mathbb{C}$, and consider the map* ev$_\alpha : \mathbb{Z}[x] \to \mathbb{C}$ *given by $x \to \alpha$. Then, the kernel of this map is a principal ideal in $\mathbb{Z}[x]$.*

Proof. (Recall that we proved this in **Exercise** 1.10). As in the referenced exercise, our claim is this: given that the kernel is non-zero, the generator is the primitive element of least degree in $\mathbb{Z}[x]$ that has α as one of its roots. The rest of the claim easily follows from **Proposition** 2.17. ■

Theorem 2.18. *The ring $\mathbb{Z}[x]$ is a UFD.*

Proof. We will use **Theorem** 2.1 to prove this claim. First, let us show that every irreducible in $\mathbb{Z}[x]$ is prime. By **Theorem** 2.16, we know the irreducibles in $\mathbb{Z}[x]$. If the given irreducible is irreducible in $\mathbb{Z}$, then it is a prime $p \in \mathbb{Z}$. In that case, we see that

$$\frac{\mathbb{Z}[x]}{(p)} \cong \mathbb{F}_p[x]$$

which is an integral domain, and hence (p) is a prime in $\mathbb{Z}[x]$. So, suppose the given irreducible is $f_0 \in \mathbb{Z}[x]$, where f_0 is primitive over $\mathbb{Z}[x]$ and irreducible over $\mathbb{Q}[x]$. We show that f_0 must be a prime over $\mathbb{Z}[x]$. So, suppose $f_0|g_0h_0$ for some $g_0, h_0 \in \mathbb{Z}[x]$. So, we see that $f_0|g_0h_0 \in \mathbb{Q}[x]$. Since f_0 is irreducible in $\mathbb{Q}[x]$, it is prime as well and hence without loss of generality suppose $f_0|g_0$ in $\mathbb{Q}[x]$. **Proposition** 2.17 then immediately tells us that $f_0|g_0 \in \mathbb{Z}[x]$, and hence f_0 is a prime in $\mathbb{Z}[x]$. So, every irreducible in $\mathbb{Z}[x]$ is prime.

The chain condition on principal ideals is easy to see. If we have an ascending chain of proper ideals in $\mathbb{Z}[x]$, i.e if we have a chain of proper divisors, then either the degree of the divisors keep getting smaller, or the gcd of the coefficients in $\mathbb{Z}$ get smaller. The degree cannot get smaller indefinitely, and the gcd of the coefficients also cannot get small indefinitely as $\mathbb{Z}$ is a UFD. Hence, the chain condition on principal ideals holds on $\mathbb{Z}[x]$ as well. So, $\mathbb{Z}[x]$ is a UFD. ■

2.6. **Generalisation to UFDs.** Observe that most of the proofs in the previous section don't use anything special about $\mathbb{Z}$. We can infact generalise most of those steps to UFDs. So, let D be a UFD, and let Fr(D) be the fraction field of D. Observe that we can take gcds over D, and hence we can define *primitive polynomials* in $D[x]$. Then, **Gauss' Lemma on Primitive Polynomials** 2.14 still works, and also **Gauss' Lemma on Irreducibility** 2.15 works. Hence, we can again characterise irreducibles in $D[x]$ as in **Theorem** 2.16, and **Proposition** 2.17 still holds. Finally, just as in **Theorem** 2.18, we can show that $D[x]$ is also a UFD.

Example 2.4. A particularly interesting example is this. Let F be a field, so that $F[t]$ is a PID, and hence a UFD. So, $F[t, x]$ is a UFD, and hence $F[x_1, ..., x_n]$ is a UFD for any $n \in \mathbb{N}$.

2.7. **Reductions mod p to prove irreducibility.** In this section, we will see a useful technique to factor out by prime ideals for proving irreducibility of certain polynomials. We begin with an example.

Example 2.5. Consider the polynomial $g(x) = 15x^4 - 9x^3 + 11$, and we consider the reduction homomorphism $\varphi : \mathbb{Z}[x] \to \mathbb{F}_2[x]$ that reduces coefficients mod 2. Then, we see that

$$\varphi(g(x)) = x^4 + x^3 + 1$$

Suppose g is reducible in $\mathbb{Z}[x]$, i.e $g(x) = h_1(x)h_2(x)$ for some non-units $h_1, h_2 \in \mathbb{Z}[x]$. Then,

$$\varphi(g(x)) = \varphi(h_1)\varphi(h_2)$$

Observe that the sum of the degrees of $h_1(x)$ and $h_2(x)$ is 4, and hence $\varphi(g(x))$ is a degree 4 polynomial as well, it follows that $\varphi(h_1), \varphi(h_2)$ have the same degrees as those of h_1 and h_2 respectively. So, this implies that x^4+x^3+1 is reducible in $\mathbb{F}_2[x]$. Clearly, this polynomial does not have any roots in $\mathbb{F}_2$, and hence it does not have any linear factors. The only possibility then is that $x^4 + x^3 + 1$ factors into two irreducible quadratic factors over $\mathbb{F}_2[x]$. Now, the only irreducible quadratic polynomial in $\mathbb{F}_2[x]$ is $x^2 + x + 1$. So, it must be true that

$$x^4 + x^3 + 1 = (x^2 + x + 1)^2 = x^4 + x^2 + 1$$

which is a contradiction. So, it follows that $15x^4 - 9x^3 + 1$ is *irreducible* in $\mathbb{Z}[x]$.

The above method shows a very useful technique, namely quotienting by prime ideals to determine irreducibility of polynomials. Let us try to state this technique in some generality. Let p be a prime in $\mathbb{Z}$, and consider the reduction homomorphism $\mathbb{Z}[x] \to \mathbb{F}_p[x]$ sending $g(x) \to \overline{g(x)}$ by reducing coefficients mod p. Let $g(x)$ be a primitive polynomial in $\mathbb{Z}[x]$ with leading coefficient c such that p does not divide c (this ensures that the degree of $\overline{g(x)}$ is equal to that of $g(x)$). If $g = h_1h_2$ non-trivially in $\mathbb{Z}[x]$, then $\overline{g} = \overline{h_1h_2}$ non-trivially in $\mathbb{F}_p[x]$ (as deg$(g) =$ deg$(\overline{g}) =$ deg$(\overline{h_1}) +$ deg$(\overline{h_2})$ and hence deg$(\overline{h_i}) =$ deg(h_i)). So, if $\overline{g}$ is irreducible in $\mathbb{F}_p[x]$, then g is irreducible in $\mathbb{Z}[x]$ (and hence in $\mathbb{Q}[x]$).

Example 2.6. Here is an example where this test fails. We have

$$3x^4 + 2x^2 - 1 = (3x^2 - 1)(x^2 + 1)$$

but mod 3, it is $-(x^2 + 1)$ which is irreducible in $\mathbb{F}_3[x]$.

Example 2.7. The polynomial $x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Z}[x]$, but for every prime p this polyomial factors in $\mathbb{F}_p[x]$. To be completed.

2.8. **Eisenstein Criterion.** This is another important irreducibility criterion that uses the theme of quotienting by prime ideals.

Theorem 2.19 (Eisenstein's Criterion). *Let $f(x) = a_nx^n + ... + a_1x + a_0 \in \mathbb{Z}[x]$ be any polynomial, and let $p \in \mathbb{Z}$ be a prime such that*

(1) *p does not divide a_n.*
(2) *p divides a_i for every $0 \leq i \leq n-1$.*
(3) *p^2 does not divide a_0.*

Then, $f(x)$ is irreducible in $\mathbb{Q}[x]$. So, if $d = \text{gcd}(a_n, a_{n-1}, ..., a_0)$, then $\frac{1}{d}f(x)$ is irreducible in $\mathbb{Z}[x]$.

Proof. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial satisfying the given conditions. Suppose $f(x)$ factors non-trivially in $\mathbb{Q}[x]$, i.e $f(x) = g(x)h(x)$ in $\mathbb{Q}[x]$, where g, h are non-zero non-unit elements of $\mathbb{Q}[x]$. Using **Gauss' Lemma** 2.14, we can deduce that $f(x)$ can be factored non-trivially in $\mathbb{Z}[x]$ (this is easy to prove!). So, without loss of generality we assume that $g(x), h(x) \in \mathbb{Z}[x]$. Now, consider the reduction homomorphism mod p. Let

$$g(x) = b_rx^r + ... + b_0$$
$$h(x) = c_sx^s + ... + c_0$$

for some r, s with $r + s = n$ and $b_r, c_s \neq 0$. Observe that

$$\overline{f}(x) = \overline{a_n}x^n \quad \text{in } \mathbb{F}_p[x]$$

and hence

$$\overline{g}(x)\overline{h}(x) = \overline{a_n}x^n \quad \text{in } \mathbb{F}_p[x]$$

The above implies that $\overline{g}(x)$ and $\overline{h}(x)$ must be *monomials* in $\mathbb{F}_p[x]$; otherwise, their product won't be a monomial. So, the only choice is $\overline{g}(x) = \overline{b_r}x^r$ and $\overline{h}(x) = \overline{c_s}x^s$. So, this means that $p|b_0$ and $p|c_0$, which in turn implies that $p^2|b_0c_0 = a_0$, a contradiction. So, $f(x)$ must be an irreducible in $\mathbb{Q}[x]$. The rest of the statement is clear. ■

Remark 2.19.1. As usual, this criterion can easily be extended to $D[x]$, where D is a UFD, and we replace $\mathbb{Q}$ by the fraction field Fr of D. More generally, suppose D is *any* integral domain, and let $f(x) = a_nx^n + ... + a_0 \in D[x]$ be a *primitive* polynomial (in this setting, a *primitive polynomial* will be one in which the coefficients don't have any non-unit common divisors) such that $a_i \in P$ for each $0 \leq i \leq n-1$, $a_n \notin P$ and $a_0 \notin P^2$, where P is some prime ideal of D. Then by the exact same reasoning as above, we can conclude that $f(x)$ is irreducible over $D[x]$. Ofcourse, here we cannot pass to the ring Fr$[x]$ as we might not be able to take gcds.

Example 2.8. Consider the polynomial $x^n - 2 \in \mathbb{Q}[x]$. By **Eisenstein's Criterion** 2.19 with $p = 2$, we see that this problem is irreducible over $\mathbb{Q}[x]$. This is a fancy way of saying that the n^{th} root of 2 is *irrational*.

Example 2.9. Let $D = F[t]$, where F is some field. Consider the polynomial $x^n - t \in F[t, x] \cong F[t][x]$. By taking our prime to be $t \in F[t]$, we can deduce that $x^n - t$ is an irreducible element in $F[t, x]$.

Example 2.10. In this example, we will see a general techique called *shifting*. Consider the polynomial

$$f(x) = \frac{x^5 - 1}{x - 1} = 1 + x + x^2 + x^3 + x^4$$

in $\mathbb{Q}[x]$. We show that this polynomial is irreducible. Note that there is no obvious way of applying **Eisenstein's Criterion** 2.19. However, if we consider $f(x+1)$, then we get

$$f(x+1) = \frac{(x+1)^5 - 1}{x} == \sum_{i=1}^{5} \binom{5}{i} x^{i-1}$$

and now we can easily apply the criterion with $p = 5$ to deduce irreducibility.

The last example can be generalised to showcase an interesting phenomenon. Suppose F is an field, and consider the unique map $F[x] \to F[x]$ given by sending $x \to x + c$ for any $c \in F$. This is easily seen to be an automorphism of $F[x]$; so, a polynomial is irreducible in $F[x]$ if and only if its image under this map is an irreducible. This is exactly what we did above, and these kind of polynomials have a name.

Definition 2.5. Let p be any prime. The cyclotomic polynomial $\phi_p(x)$ is defined as

$$\phi_p(x) := \prod_{\zeta}(x - \zeta) = \frac{x^p - 1}{x - 1} = 1 + x + ... + x^{p-1}$$

where the above product is taken over all primitive p^{th} roots of unity.

Proposition 2.20. *$\phi_p(x)$ is irreducible in $\mathbb{Q}[x]$ for any prime $p \in \mathbb{Z}$.*

Proof. As mentioned in the remark above, consider the shifting automorphism $\mathbb{Q}[x] \to \mathbb{Q}[x]$ given by $x \to x+1$. Now,

$$\phi_p(x+1) = \sum_{i=1}^{p} \binom{p}{i} x^{i-1}$$

and the claim is proven by applying **Eisenstein's Criterion** 2.19 with prime p. ∎

2.9. **Rational Root Test.** Now we will present a fairly useful test to check for existence of roots for some polynomials.

Theorem 2.21 (**Rational Root Test**). *Let* $\gcd(a,b) = 1$ *in* $\mathbb{Z}$*,* $b \neq 0$*. Let* $g(x) = c_n x^n + \ldots + c_0 \in \mathbb{Z}[x]$*. Then,*

$$\frac{a}{b} \text{ is a root of } g \iff (bx-a) | g \in \mathbb{Z}[x]$$

Moreover, if a/b is a root of b, then $b|c_n$ and $a|c_0$.

Proof. This is a straightforward application of **Gauss' Lemma** 2.14. The other assertion about divisibility is also immediate. ∎

3. Field Theory

We will begin this section by understanding quotients of $F[x]$ where F is a field. We know that $F[x]$ is a PID. So, every ideal I of $F[x]$ is of the form $(g(x))$, where $g(x) \in F[x]$. Moreover, to make the generator g unique, we can impose the condition that g must be monic.

Exercise 3.1. What can be said about the *size* of the quotient $F[x]/(g(x))$? Try relating to vector spaces.

Solution. If $p(x) \in F[x]$, then by **Euclidean Division** 1.6, there are $q(x), r(x) \in F[x]$ such that $p(x) = q(x)g(x) + r(x)$ and $\deg(r(x)) < \deg(g(x))$. So, it follows that if $n = \deg(g(x))$, the elements $\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}$ span the quotient $F[x]/(g(x))$, and clearly these elements are linearly independent. So it follows that $F[x]/(g(x))$ is an F-vector space over dimension n, so that

$$F[x]/(g(x)) \cong F^n$$

as F-vector spaces.

Exercise 3.2. When is $F[x]/(g(x))$ a field? An integral domain?

Solution. $F[x]/(g(x))$ is a field precisely when $g(x)$ is irreducible, because in that case the only ideals of $F[x]/(g(x))$ will be the trivial ones. Moreover, because $F[x]$ is a PID, it can be seen that a polynomial is irreducible if and only if it is prime. One direction is clear; if a polynomial is irreducible, then it is clearly prime. If a polynomial is prime, then it cannot be *reducible*; if it was reducible, it would factor into factors of lesser degree. But that would contradict the primality of the polynomial, as it cannot divide any of its factors of lesser degree. So, $F[x]/(g(x))$ is a field if and only if it is an integral domain.

Exercise 3.3. Show that $E_1 = \mathbb{Q}[t]/(t^2-5)$ is a field. Find $\overline{t^3}^{-1}$ in E_1.

Solution. Clearly, $t^2 - 5$ is irreducible in $\mathbb{Q}[t]$. So, $\mathbb{Q}[t]/(t^2-5)$ is a field. Now, observe that $\overline{t^3} = \overline{5t}$. Moreover, $\overline{t}^{-1} = \overline{\frac{-t}{5}}$. So, it follows that $\overline{t^3}^{-1} = \overline{\frac{-t}{25}}$. In general, if we are given some $\overline{h(x)} \neq 0$, inverses can be found using *diophantine equations*: because t^2-5 is irreducible, its gcd with any such $h(x)$ is 1, and hence there are $a(x), b(x) \in F[x]$ such that

$$a(x)(t^2-5) + b(x)h(x) = 1$$

So, $\overline{h(x)}^{-1} = \overline{b(x)}$.

Exercise 3.4. Construct fields of size 4 and 8.

Solution. We consider the field $\mathbb{F}_2$. To construct a field of size 2^n, our stratey will be to find an *irreducible polynomial* in $g(x)$ $\mathbb{F}_2[x]$ of degree n. It will then immediately follow that $\mathbb{F}_2[x]/(g(x))$ is a field of order 2^n.

If $n = 2$, $g(x)$ must be a quadratic polynomial. Now, there are four quadratic polynomials in $\mathbb{F}_2[x]$: x^2 , x^2+1, x^2+x and x^2+x+1. Out of these, only the polynomial x^2+x+1 is irreducible. So, it follows that $\mathbb{F}_2[x]/(x^2+x+1)$ is a field of order $2^2 = 4$.

If $n = 3$, $g(x)$ is a cubic polynomial. There are 8 cubic polynomials: x^3 , x^3+1 , x^3+x, x^3+x+1, x^3+x^2 , x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1. Out of these, only the polynomials x^3+x+1 and x^3+x^2+1 are irreducible. So, it follows that $\mathbb{F}_2[x]/(x^3+x+1)$ and $\mathbb{F}_2[x]/(x^3+x^2+1)$ are both finite fields of order 8. However, we show that

$$\frac{\mathbb{F}_2[x]}{x^3+x+1} \cong \frac{\mathbb{F}_2[x]}{x^3+x^2+1}$$

so essentially, a *unique* field is created by this process. Showing this is easy: just consider the map $\mathbb{F}_2[x] \to \mathbb{F}_2[x]$ that sends $x \to x+1$.

Remark 3.0.1. We can actually repeat the above process for any prime p and any positive integer n to obtain a *unique* field of order p^n. We will prove this later.

Exercise 3.5. Prove that there are *unique* fields of size 4 and size 8.

Solution. To be completed.

Exercise 3.6. Classify all rings of order 4.

Solution. To be completed.

3.1. Field Extensions.

In this section, we will introduce the notion of *field extensions* and their *degrees*.

Definition 3.1. Let F, E be fields such that $F \subset E$. Then, E is said to be an *extension* of F, and this is denoted by E/F (Note: this is *not* a quotient). The dimension of E as a vector space over F is called the *degree* of the extension E/F, and this is denoted by $[E : F]$. If $[E : F]$ is finite, then E/F is said to be a *finite extension*.

Proposition 3.1 (Multiplicativity of Degree). *Let $F \subset E \subset K$ be field extensions. Then,*

$$[K : F] = [K : E][E : F]$$

So, both $[K : E]$ and $[E : F]$ divide $[K : F]$.

Proof. The idea is easy. Let $\{v_\alpha\}_{\alpha\in I}$ be an E-basis of K, and let $\{w_\beta\}_{\beta\in J}$ be an F-basis of E. Then, we claim that

$$\{w_\beta v_\alpha\}_{\beta\in J,\alpha\in I}$$

is an F-basis of K. It is easy to see that any element of K can be written as an F-linear combination of these elements. So, it is enough to show linear independence. Suppose

$$\sum_{\alpha\in I,\beta\in J} c_{\beta,\alpha} w_\beta v_\alpha = 0$$

for $c_{\beta,\alpha}\in F$. So, this means that

$$\sum_{\alpha\in I}\left(\sum_{\beta\in J} c_{\beta,\alpha} w_\beta\right) v_\alpha = 0$$

Because $\{v_\alpha\}$ is an E-basis of K, it follows that

$$\sum_{\beta\in J} c_{\beta,\alpha} w_\beta = 0$$

for each $\alpha\in I$. Again, since $\{w_\beta\}$ is an F-basis of E, it follows that

$$c_{\beta,\alpha} = 0$$

for each $\alpha\in I,\beta\in J$. This completes the proof. ■

Exercise 3.7. Let K be a finite field with $|K| = p^n$. Let $E\subset K$ be a subfield with $|E| = p^d$. Then $d|n$.

Solution. Clearly, the characteristic of K is p, and let $F = \mathbb{Z}/p\mathbb{Z}$ be the prime subfield of K. Then,

$$F\subset E\subset K$$

By **Proposition** 3.1, we see that

$$[K:F] = [K:E][E:F]$$

Now, $[K:F] = n$ and $[E:F] = d$, and this implies that $d|n$.

3.2. Reviewing Algebraic Elements and Minimal Polynomials.

In this section, we will review some of the ideas we saw in the section on **Adjoining Elements.**. We will also see a new definition.

Definition 3.2. Let $F\subset E$ be fields, and let $\alpha\in E$ be an arbitrary element. As before, $F[\alpha]$ is the *smallest subring* of E containing both F and E. We define

$$F(\alpha) := \text{smallest } \textit{subfield} \text{ of } E \text{ containing } F \text{ and } \alpha$$

Similarly, we can define $F[\alpha_1,...,\alpha_n]$ and $F(\alpha_1,...,\alpha_n)$. It is easy to see that $F(\alpha)$ is the fraction field of $F[\alpha]$.

Consider the evaluation map $F[x]\xrightarrow{\text{ev}_\alpha} F[\alpha]$ given by $x\to\alpha$. We know that if Ker ev$_\alpha = 0$, then α is *trancendental* over F, and in this case we see that $F[x]\cong F[\alpha]$, i.e $F[\alpha]$ is *not* a field, so that $F[\alpha]\subsetneq F(\alpha)$. Also, in this case, we see that dim$_F\, F[\alpha] = \infty$, and hence it follows that $[F(\alpha):F] = \infty$. On the other hand, if Ker ev$_\alpha\neq 0$, then it is generated by a monic irreducible polynomial, which is nothing but the *minimal polynomial* of α over F, and in this case we say that α is *algebraic* over F. If $f(x)$ is the minimal polynomial of α over F, then we have

$$\frac{F[x]}{(f(x))} \cong F[\alpha]$$

i.e $F[\alpha]$ is a field, and hence $F[\alpha] = F(\alpha)$. Also, in this case we see that $[F(\alpha) : F] = [F[\alpha] : F] = \deg f$. The above discussion implies that

$$\alpha \text{ is algebraic over } F \iff [F(\alpha) : F] < \infty$$

3.3. Attaching a Single Element.

Let us begin this section with an exercise.

Exercise 3.8. Let $\alpha = \sqrt[7]{2} \in \mathbb{R}$ and $\beta = \frac{1}{2019} + 2020\alpha^2 + 2021\alpha^5$. Show that $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$ (Hint: Use **Multiplicativity of Degree** 3.1).

Solution. First, observe that α is a root of the polynomial $x^7 - 2 \in \mathbb{Q}[x]$, which is irreducible in $\mathbb{Q}[x]$ by **Eisenstein's Criterion** 2.19. So, we see that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 7$. Now, observe that

$$\mathbb{Q} \subset \mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha)$$

and so by **Multiplicativity of Degree** 3.1, we see that

$$7 = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}]$$

and since 7 is a prime, one of $[\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)]$ or $[\mathbb{Q}(\beta) : \mathbb{Q}]$ is 7. Now, we claim that $\beta \notin \mathbb{Q}$. For the sake of contradiction, suppose $\beta \in \mathbb{Q}$. But that would imply that α is a root of the polynomial

$$2021x^5 + 2020x^2 + \frac{1}{2019} - \beta \in \mathbb{Q}[x]$$

which is a contradiction. So, it follows that $[\mathbb{Q}(\beta) : \mathbb{Q}] > 1$, and hence $[\mathbb{Q}(\beta) : \mathbb{Q}] = 7$. So, it follows that $[\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] = 1$, and hence $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. This prevented us from explicitly calculating the minimal polynomial of β over $\mathbb{Q}$, which would have been very cumbersome.

Proposition 3.2. *Let $F \subset E$ be fields with $[E : F] = n$ and let $\alpha \in E$. Then, α is algebraic over F and* $\deg(\min_F \alpha) \mid n$.

Proof. This is easy to see: the elements $1, \alpha, \alpha^2, ..., \alpha^n$ must be linearly dependent over F, and hence α satisfies some polynomial in $F[x]$, i.e α is algebraic over F. Now, observe that $[F(\alpha) : F] = \deg(\min_F \alpha)$, and since $F \subset F(\alpha) \subset E$, **Multiplicativity of Degree** 3.1 implies that $\deg(\min_F \alpha) \mid n$. ■

Definition 3.3. Let E/F be a field extension. Then, this extension is said to be *algebraic* if every $\alpha \in E$ is algebraic over F. So, **Proposition** 3.2 shows that all finite extensions are algebraic.

Trying to make a converse for **Proposition** 3.2 leads to interesting questions as given in the following examples.

Example 3.1. **Proposition** 3.2 shows that all elements in a finite extension E/F are algebraic over F. We ask whether the converse is true, i.e if all elements in an extension E/F are algebraic over F, is the extension finite. The answer is *no*. For a counterexample, let

$$S = \{\sqrt[n]{3} \mid n \in \mathbb{N}\}$$

and consider the extension $\mathbb{Q} \subsetneq \mathbb{Q}(S)$. This extension contains elements of arbitrarily large degree over $\mathbb{Q}$, because $x^n - 3$ is irreducible over $\mathbb{Q}[x]$ for each $n \in \mathbb{N}$ by **Eisenstein's Criterion** 2.19. So, by the divisibility part of **Proposition** 3.2, it follows that this extension is not finite. However, as we shall see shortly, this is indeed an algebraic extension.

Example 3.2. Proposition 3.2 shows that if E/F is an extension of degree d and if $\alpha \in E$, then the degree of α over F is a divisor of n. We ask the opposite question: given any divisor d of n, is there an element in E of degree d over F? The answer is again a *no*. To be completed.

Proposition 3.3. *Let $F \subset M \subset E$ be fields, and suppose $\alpha \in E$ such that α is algebraic over F. Then*

$$\text{deg}(\text{min}_M\alpha) \leq \text{deg}(\text{min}_F\alpha)$$

This can be represented as the following diamond diagram.

$$\begin{tikzcd}
& M[\alpha] & \\
F[\alpha] \arrow[ur] & & M \arrow[ul, "e\leq d"'] \\
& F \arrow[ul, "d"] \arrow[ur] &
\end{tikzcd}$$

where $d =$ deg(min$_F\alpha$) and $e =$ deg(min$_M\alpha$).

Proof. It is clearly seen that α is algebraic over M as well. Also, observe that min$_M\alpha$ | min$_F\alpha$ and hence the claim follows. Pictorially, this proposition states that moving up the diagram can only decrease the degree. ■

3.4. **Attaching Multiple Elements and Diamond Diagrams.** Now consider the following situation. Let $F \subset E$ be fields, and suppose $\alpha, \beta \in E$ are algebraic over F. So, it follows that $F[\alpha] = F(\alpha)$ and $F[\beta] = F(\beta)$ are both *fields*. We can even attach α and β simultaneously to get $F[\alpha, \beta]$; this is the same as attaching the element α to the field $F[\beta]$, and hence $F[\alpha, \beta] = F(\alpha, \beta)$ because α is algebraic over $F[\beta]$. This explanation can also be extended by induction to the situation of attaching arbitrary algebraic elements $\alpha_1, ..., \alpha_n$ to get $F[\alpha_1, ..., \alpha_n] = F(\alpha_1, ..., \alpha_n)$. This situation can be explained by the following diamond diagram.

$$\begin{tikzcd}
& F[\alpha, \beta] & \\
F[\alpha] \arrow[ur, "e_2\leq d_2"] & & F[\beta] \arrow[ul, "e_1\leq d_1"'] \\
& F \arrow[ul, "d_1"] \arrow[ur, "d_2"'] \arrow[uu, "n"] &
\end{tikzcd}$$

In the above diagram, the numbers next to the arrows are the degrees of the extensions, and note that we are using **Proposition** 3.3. Now, by **Multiplicativity of Degree** 3.1, we see that

$$n = d_1e_2 = d_2e_1 \leq d_1d_2 \tag{†}$$

Proposition 3.4. *Let $F \subset E$ be fields. Then*

$$K := \{\alpha \in E \mid \alpha \text{ is algebraic over } F\}$$

is a subfield of E.

Proof. Clearly, $0 \in K$ and K is closed under additive inverses. Next, suppose α, β are algebraic over f, i.e there are $p(x), q(x) \in F[x]$ with $p(\alpha) = q(\beta) = 0$. Then we show that $\alpha + \beta$ is also algebraic. To show this, it is enough to show that

$$[F(\alpha+\beta) : F] < \infty$$

Because both α, β are algebraic, it follows that $F[\alpha, \beta] = F(\alpha, \beta)$ is a field, and hence

$$[F(\alpha, \beta) : F] < \infty$$

Because $F(\alpha+\beta) \subset F(\alpha, \beta)$, it follows that

$$[F(\alpha+\beta) : F] < \infty$$

implying that $\alpha + \beta$ is algebraic over F. So, K is an additive subgroup of F. Clearly, $1 \in K$, and K is closed under inverses. A similar proof as above shows that K is closed under multiplication. So, K is a subfield of E. ■

Remark 3.4.1. However, K/F need not be a finite extension. This was exactly the point of **Example** 3.1.

Proposition 3.5. *Let $F \subset E$ be fields, and suppose $\alpha, \beta \in E$ are algebraic over F. Suppose $[F(\alpha) : F] = d_1$ and $[F(\beta) : F] = d_2$, where d_1, d_2 are coprime. Then, $[F(\alpha, \beta) : F] = d_1 d_2$.*

Proof. From (†) above, we see that $d_1 \mid n$ and $d_2 \mid n$, which implies that $d_1 d_2 \mid n$ since d_1, d_2 are coprime. However, (†) also implies that $n \leq d_1 d_2$, and hence it follows that $n = d_1 d_2$. This completes the proof. ■

Exercise 3.9. Let $g(x) = x^3 - 2$ in $\mathbb{Q}[x]$. Let E *be the splitting field of* $g(x)$ *in* $\mathbb{C}$, i.e

$$E := \mathbb{Q}(\text{all roots of } g \text{ in } \mathbb{C})$$

So, E is the smallest subfield of $\mathbb{C}$ such that in $E[x]$, $g(x)$ factors as a product of linear factors. Find $[E : \mathbb{Q}]$.

Solution. Let $\omega = e^{\frac{2\pi i}{3}}$, and let $\alpha = \sqrt[3]{2}$. Then, the roots of $g(x)$ in $\mathbb{C}$ are $\{\alpha, \omega\alpha, \omega^2\alpha\}$. Observe that the field $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha)$, which is immediate. So, we just need to find $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}]$. But we can do this using **Proposition** 3.5; observe that the minimal polynomial of α over $\mathbb{Q}$ has degree 3, and that of ω is 2 (because $\omega^2 + \omega + 1 = 0$). So, it follows that

$$[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = 2 \cdot 3 = 6$$

Note that here we had the liberty of just attaching pre-existing roots in $\mathbb{C}$ until the polynomial completely splits. However, we want to generalise this idea, and we do this by attaching abstract roots. So, consider the polynomial $x^3 - 2 \in \mathbb{Q}[x]$, and put $E_0 = \mathbb{Q}$. This polynomial is irreducible; so, we attach an abstract root of this polynomial by constructing

$$E_1 = \frac{\mathbb{Q}[t_1]}{(t_1^3 - 2)}$$

Now, the polynomial $x^3 - 2 \in E_1[x]$ has a root in E_1, namely $\overline{t_1}$. So, we can write

$$x^3 - 2 = (x - \overline{t_1})q(x) = (x - \overline{t_1})(x^2 + \overline{t_1}x + \overline{t_1}^2)$$

where $q(x) \in E_1[x]$ is some degree 2 polynomial. I claim that $q(x)$ is *irreducible* in $E_1[x]$; observe that $E_1 \cong \mathbb{Q}(\alpha)$, and $\mathbb{Q}(\alpha)$ does not contain the complex roots $\omega\alpha, \omega^2\alpha$ of $x^3 - 2$. So, it implies that E_1 contains exactly one root of $x^3 - 2$, and hence $q(x) \in E_1[x]$ must be irreducible. So, we again attach an abstract root of $q(x)$ to E_1 by defining

$$E_2 = \frac{E_1[t_2]}{(q(t_2))}$$

At this point, note that $x^3 - 2$ completely factors into linear factors in E_2. Now, we will show that E_2 is indeed the splitting field $\mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha)$, i.e $E_2 \cong \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha)$. First, note that $\mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) = \mathbb{Q}(\alpha, \omega\alpha)$. Now, $\mathbb{Q}(\alpha, \omega\alpha) = \mathbb{Q}(\alpha)[\omega\alpha]$. Moreover, observe that

$$\mathbb{Q}(\alpha) \cong \frac{\mathbb{Q}[t_1]}{(t_1^2 - 2)} = E_1$$

Moreover, the minimal polynomial of $\omega\alpha$ over the field $\mathbb{Q}(\alpha)$ is

$$t_2^2 + \alpha t_2 + \alpha^2$$

which is easy to see. So, it follows that

$$\mathbb{Q}(\alpha)[\omega\alpha] \cong \frac{\mathbb{Q}(\alpha)[t_2]}{(t_2^2 + \alpha t_2 + \alpha^2)} \cong \frac{E_1[t_2]}{(q(t_2))} = E_2$$

So, it follows that the abstract construction gives us the splitting field. We shall see a generalisation of this technique in the upcoming sections.

3.5. **Some Results in Finite Fields.** In this section, we will prove some results about finite fields. We will *assume* in some results the existence of a finite field of size p^n for any $n \in \mathbb{Z}$ and any prime $p \in \mathbb{Z}$. We will prove this existence in the section 3.6 **Splitting Fields and Construction of Finite Fields.**

The first question that we ask is this: how to factor $x^{p^n} - x$ in $\mathbb{F}_p[x]$? Suppose a field E is given to us, with $|E| = p^n$. Then by problem **9. (iii)** of HW-1, each $\alpha \in E$ is a root of the polynomial

$$x^{p^n} - x = x(x^{p^n - 1} - 1)$$

Now, suppose $g(x) \in \mathbb{F}_p[x]$ is a monic irreducible polynomial of degree n (we don't know if there is such a polynomial yet). Then, consider the field

$$E = \frac{\mathbb{F}_p[t]}{(g(t))}$$

and hence $|E| = p^n$. By *construction*, the minimal polynomial of the element $\overline{t} \in E$ over $\mathbb{F}_p$ is $g(x)$. Because $\overline{t} \in E$ is a root of $x^{p^n} - x \in \mathbb{F}_p[x] \subset E[x]$, it follows that

$$g(x) \mid x^{p^n} - x \quad \text{in } \mathbb{F}_p[x]$$

Now, we know that $\mathbb{F}_p[x]$ is a UFD. So, any two *distinct* monic irreducible polynomials over $\mathbb{F}_p[x]$ are coprime, and hence it follows that

$$\left(\prod_{g \text{ monic irreducible of degree } n \text{ in } \mathbb{F}_p[x]} g(x)\right) \mid x^{p^n} - x \quad \text{in } \mathbb{F}_p[x]$$

Infact, we can do more than this. We start by proving a simple proposition.

Proposition 3.6. *If R is any ring with $x \in R$ and $r \mid s$, then $x^r - 1 \mid x^s - 1$. In particular, if $d \mid n$ and if p is a prime, then $x^{p^d} - x \mid x^{p^n} - x$ in $R[x]$.*

Proof. The proof of this is an immediate calculation. If $s = rk$ for some $k \in \mathbb{Z}$, then

$$x^s - 1 = x^{rk} - 1 = (x^r)^k - 1$$

and clearly the extreme right hand side is divisible by $x^r - 1$. Now, if $d \mid n$, then $p^d - 1 \mid p^n - 1$ in $\mathbb{Z}$. So, we see that

$$x^{p^d-1} - 1 \mid x^{p^n-1} - 1$$

in $R[x]$, and hence

$$x^{p^d} - x \mid x^{p^n} - 1$$

in $R[x]$, completing the proof. ■

Theorem 3.7. *Consider the polynomial $x^{p^n} - x \in \mathbb{F}_p[x]$. Then*

$$\left(\prod_{h \text{ monic irreducible of degree } d \text{ in } \mathbb{F}_p[x], d|n} h(x)\right) \mid x^{p^n} - x \quad \textit{in } \mathbb{F}_p[x]$$

where in the above product d is ranging over all divisors of n.

Proof. To prove this, suppose h is a monic irreducible polynomial of degree d in $\mathbb{F}_p[x]$, where $d \mid n$ is a *fixed* divisor of n. By the exact same reasoning as in the beginning of this section, i.e by constructing a field of size p^d, we can conclude that

$$h(x) \mid x^{p^d} - x \in \mathbb{F}_p[x]$$

and hence it follows that

$$\left(\prod_{h \text{ monic irreducible of degree } d \text{ in } \mathbb{F}_p[x]} h(x)\right) \mid x^{p^d} - x \quad \text{in } \mathbb{F}_p[x]$$

Because d is a divisor of n, an application of **Proposition** 3.6 shows that $x^{p^d} - x \mid x^{p^n} - x$ in $\mathbb{F}_p[x]$. So, it follows that

$$\left(\prod_{h \text{ monic irreducible of degree } d \text{ in } \mathbb{F}_p[x]} h(x)\right) \mid x^{p^n} - x \quad \text{in } \mathbb{F}_p[x]$$

Ranging d over all divisors of n and using the fact that any distinct irreducibles over $\mathbb{F}_p[x]$ are coprime, the claim follows. ■

We will now show that the factors of $x^{p^n} - x$ in $\mathbb{F}_p[x]$ given in **Theorem** 3.7 actually give the factorisation of $x^{p^n} - x$ in $\mathbb{F}_p[x]$.

Theorem 3.8. *Consider the polynomial $x^{p^n} - x \in \mathbb{F}_p[x]$. Then,*

$$x^{p^n} - x = \left(\prod_{h \text{ monic irreducible of degree } d \text{ in } \mathbb{F}_p[x], d|n} h(x)\right)$$

Remark 3.8.1. In the proof, we will assume that for any $n \in \mathbb{N}$, there is a finite field E such that $|E| = p^n$.

Proof. By **Theorem** 3.7, it is enough to show the following.

(1) If $h(x) \in \mathbb{F}_p[x]$ is an irreducible such that $h(x) \mid x^{p^n} - x$, then deg$(h(x)) \mid n$.
(2) No square of an irreducible in $\mathbb{F}_p[x]$ divides $x^{p^n} - x$.

Let E be a field of cardinality p^n, and clearly $\mathbb{F}_p$ is contained in E (this is the only place where we assume the existence of finite fields).

First, let us show (1). So, let $h(x) \in \mathbb{F}_p[x]$ be an irreducible such that $h(x) \mid x^{p^n} - x$ in $\mathbb{F}_p[x]$. By problem **9. (iii)** of HW-1, we know that every element of E is a root of the polynomial $x^{p^n} - x$. In particular, this means that $h(x)$ has a root in E. Let $\alpha \in E$ be this root. Then, the subfield $\mathbb{F}_p(\alpha) \subset E$ is a field of degree d over $\mathbb{F}_p$, because α has degree $d =$ deg$(h(x))$ over $\mathbb{F}_p$. So by **Multiplicativity of Degree** 3.1 we have

$$n = [E : \mathbb{F}_p] = [E : \mathbb{F}_p(\alpha)][\mathbb{F}_p(\alpha) : \mathbb{F}_p] = d[E : \mathbb{F}_p(\alpha)]$$

which implies that $d \mid n$. This proves (1).

Consider the factorisation of $x^{p^n} - x$ over the UFD $\mathbb{F}_p[x]$. We know the factorisation of $x^{p^n} - x$ over the UFD $E[x]$; it is simply a product of p^n linear factors. This immediately implies that the factorisation of $x^{p^n} - x$ in $\mathbb{F}_p[x]$ *cannot* contain any squares of irreducibles. This completes the proof of the theorem. ■

Theorem 3.9 (**Uniqueness of Finite Fields**). *Suppose E_1 and E_2 are two finite fields with $|E_1| = |E_2| = p^n$ for some prime $p \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then, $E_1 \cong E_2$. Moreover, $|$Aut$(E_i)| = n$ and Aut(E_i) is cyclic, and is generated by the Frobenius map $x \mapsto x^p$.*

Proof. Suppose E_1, E_2 are two fields of cardinality p^n. From **Theorem** 3.15, we know that both $E_1^\times$ and $E_2^\times$ are cyclic groups. So, take a generator α of the group $E_1^\times$. Because E_1 is a finite extension over $\mathbb{F}_p$, we know that α is algebraic over $\mathbb{F}_p$. So, consider the minimal polynomial min$_{\mathbb{F}_p}\alpha$. Because $E_1^\times$ is generated by α, we see that $E_1 = \mathbb{F}_p(\alpha)$, and hence

$$E_1 = \mathbb{F}_p(\alpha) \cong \frac{\mathbb{F}_p[x]}{(\text{min}_{\mathbb{F}_p}\alpha)}$$

so that min$_{\mathbb{F}_p}\alpha$ has degree n. Now, by **Theorem** 3.7, we see that min$_{\mathbb{F}_p}(\alpha) \mid x^{p^n} - x$ in $\mathbb{F}_p[x]$. But, we also know that $x^{p^n} - x$ splits into linear factors over the field E_2 (by problem **9. (iii)** of HW-1). So, the polynomial min$_{\mathbb{F}_p}\alpha$ has a root in E_2. Let this root be $\beta \in E_2$. So, clearly we see that min$_{\mathbb{F}_p}\beta =$ min$_{\mathbb{F}_p}\alpha$ because min$_{\mathbb{F}_p}\alpha$ is *irreducible* over $\mathbb{F}_p$, and hence we see that

$$E_1 \cong \frac{\mathbb{F}_p[x]}{(\text{min}_{\mathbb{F}_p}\alpha)} = \frac{\mathbb{F}_p[x]}{(\text{min}_{\mathbb{F}_p}\beta)} = \mathbb{F}_p(\beta) \subset E_2$$

So, E_2 contains a copy of the field E_1. By comparing cardinalities, it follows that $E_1 \cong E_2$, and this completes the proof of the first part of the theorem. Need to write the proof of the rest of the theorem. ■

Corollary 3.9.1. *For every positive integer $n \in \mathbb{N}$, there is an irreducible polynomial of degree n over the field $\mathbb{F}_p$.*

Proof. As mentioned in the beginning of this section, we assume that there is a finite field E with $|E| = p^n$. Now, consider the generator α of the cyclic group $E^\times$. As in the above proof, we see that deg(min$_{\mathbb{F}_p}\alpha) = n$. So this is the required irreducible polynomial. ■

Theorem 3.10 (**Subfields of Finite Fields**). *Let E be a finite field with $|E| = p^n$. Then,*

$$E \text{ has a unique subfield } M \text{ with } |M| = p^d \iff d \mid n$$

Proof. One direction is clear; if M is a subfield of E with $|M| = p^d$, then **Multiplicativity of Degree** 3.1 implies that $d \mid n$. Moreover, the subfield M will be unique; this is because the polynomial $x^{p^d} - x$ completely splits over the field M (again by problem **9. (iii)** of HW-1), and this polynomial can have atmost p^d roots. So, only the harder direction needs to be proven.

Let d be any divisor of n. Consider the polynomial $x^{p^d} - x$ over E. By **Proposition** 3.6, we see that $x^{p^d} - x \mid x^{p^n} - x$ in $\mathbb{F}_p[x]$. Now, the polynomial $x^{p^n} - x$ completely splits into linear factors in E, and hence it follows that $x^{p^d} - x$ has *all* its roots in E. Clearly, there are p^d roots of this polynomial, because the polynomial $x^{p^n} - x$ in $E[x]$ does not have any root with multiplicity greater than 1. Now, we will show that all roots of $x^{p^d} - x$ in E form a *field*; that will be the required field M. It is clear that 0 and 1 are roots of $x^{p^d} - x$. Now, suppose $\alpha \neq 0$ is a root. So, we see that

$$\alpha^{p^d} - \alpha = 0$$

So, we have

$$\frac{1}{\alpha^{p^d}} - \frac{1}{\alpha} = \frac{-(\alpha^{p^d} - \alpha)}{\alpha^{p^d+1}} = 0$$

and hence α^{-1} is also a root, so that the set of roots is closed under multiplicative inverses. Next, suppose p is odd. So, we have

$$(\alpha)^{p^d} - (-\alpha) = -\alpha^{p^d} + \alpha = -(\alpha^{p^d} - \alpha) = 0$$

and hence it implies that $-\alpha$ is also a root. If $p = 2$, then we have

$$(-\alpha)^{2^d} - (-\alpha) = \alpha^{2^d} + \alpha = -\alpha^{2^d} + \alpha = 0$$

and hence again $-\alpha$ is a root, where we have used the fact that $-1 = 1$ in E in this case. So, the set of roots is also closed under additive inverses. The fact that the set of roots is closed under multiplication is clear, and the fact that the set of roots is closed under addition follows by using the fact that the **Frobenius Map** $x \mapsto x^p$ is a *homomorphism* in E. So, it follows that the set of roots of $x^{p^d} - x$ is a field itself, and this completes the proof. ■

Exercise 3.10. Find gcd$(x^a - 1, x^b - 1)$ in $\mathbb{Z}[x]$.

Solution. To be completed.

3.6. **Splitting Fields and Construction of Finite Fields.** The idea in this section will be very similar to what we did in **Exercise** 3.9, and we will give a construction of finite fields.

Definition 3.4. Let F be a field, and let $g(x) \in F[x]$ be a given polynomial. A *splitting field* of F is an extension E/F such that $g(x)$ factors completely in $E[x]$, i.e

$$g(x) = \prod_{i=1,...,n} (x - \alpha_i)$$

and that $E = F[\alpha_1, ..., \alpha_n]$.

Theorem 3.11. *Let F be any field, and let $g(x) \in F[x]$ be any polynomial. Then, there exists a splitting field for $g(x)$.*

Proof. This is a very natural construction, and very similar to what we did in **Exercise** 3.9. Put $E_0 = F$. Consider $E_i[x]$, and factor $g(x)$ into irreducibles in the UFD $E_i[x]$. If $g(x)$ factors completely into linear factors, then stop. Otherwise, $g(x)$ has an irreducible factor of degree atleast 2. Say this factor is $q(x)$. Then, put

$$E_{i+1} = \frac{E[t_i]}{(q(t_i))}$$

So, $\overline{t_i}$ is a root of $q(x)$ in the E_{i+1}, i.e $q(x)$ has a linear factor in $E_{i+1}[x]$. Continue this process until $g(x)$ factors completely into linear factors. Suppose this stops at the field E_k. So, observe that

$$F = E_0 \subset E_1 \subset ... \subset E_i \subset E_{i+1} \subset ... \subset E_k$$

as E_{i+1} contains E_i as constants. So, observe that $g(x)$ has all its roots in E_k. So suppose $\alpha_1, ..., \alpha_n$ are the roots of $g(x)$, where $n = \deg(g(x))$. Consider the subfield $F(\alpha_1, ..., \alpha_n) = F[\alpha_1, ..., F_{\alpha_n}] \subset E_k$. This subfield is the required splitting field. ■

Finally, we have all but one tool to construct a finite field. So let us define the tool first.

Definition 3.5. Let F be any field, and let $f(x) = c^n x^n + ... + c_0 \in F[x]$. The *derivative* $f'(x) \in F[x]$ is defined as

$$f'(x) = nc^n x^{n-1} + ... + c_1$$

i.e $f'(x)$ is defined exactly as the derivative in calculus.

Proposition 3.12. *Let $f(x) \in F[x]$ be a polynomial. Then f has a multiple root α in an extension K/F if and only if α is a root of f and f'.*

Proof. Suppose $\alpha \in K$ is a root of $f(x)$. Then, $f(x) = (x - \alpha)g(x)$ for some $g(x) \in K[x]$. So, α is a multiple root of f if and only if it is a root of $g(x)$. Now,

$$f'(x) = (x - \alpha)g'(x) + g(x)$$

So, $g(\alpha) = 0$ if and only if $f'(\alpha) = 0$. So, f has a multiple root in K if and only if it is the root of both f and f'. ■

Proposition 3.13. *Let $f(x) \in F[x]$. Then, there exists a field extension K/F in which f has a multiple root if and only if f and f' are not relatively prime. Infact, we can take K to be the splitting field of f.*

Proof. Let K/F be a field extension containing all roots of f. In particular, we can let K to be the splitting field of f. By **Proposition** 3.12 f has a multiple root in K if and only if both f and f' have a common factor, i.e if and only if f and f' are not relatively prime. ■

Theorem 3.14 (**Existence of Finite Fields**). *Let p be any prime, and let $n \in \mathbb{N}$ be any positive integer. Then, there is a field E such that $|E| = p^n$. By* **Theorem** 3.9*, this field is unique upto isomorphism, and is denoted by $\mathbb{F}_{p^n}$.*

Proof. Let E be the splitting field of the polynomial $x^{p^n} - x \in \mathbb{F}_p[x]$. We show that E must be equal to the set of roots of $x^{p^n} - x$. But this is easy: observe that E has characteristic p, and hence the **Frobenius Map** $x \mapsto x^p$ is a homomorphism. So by the exact same reasoning as in **Theorem** 3.10, we conclude that E is equal to the set of roots of the polynomial $x^{p^n} - x$ in $E[x]$.

Since $x^{p^n} - x$ has atmost p^n roots, it follows that $|E| \leq p^n$. To show that $|E| = p^n$, we must show that $x^{p^n} - x$ has distinct roots. But this is easy to see by using the derivative as in **Proposition** 3.13; observe that $(x^{p^n} - 1)' = -1$ in $\mathbb{F}_p[x]$, and hence it follows that all roots of $x^{p^n} - x$ are distinct. This completes the proof. ■

3.7. **Cyclicity of Subgroups of Multiplicative Groups of Fields.** In this section, we will prove a result that will be very important in studying finite fields.

Theorem 3.15. *Let F be any field, and let $F^\times$ be the multiplicative group of units of F. Then any finite subgroup of $F^\times$ is cyclic.*

To prove this result, we will use a simple fact from abelian group theory.

Proposition 3.16. *Let G be any abelian group, and let x, y be elements of G with orders k, l respectively. Then, G contains an element of order* lcm(k, l).

Proof. First, suppose gcd$(k, l) = 1$. In that case, we see that lcm$(k, l) = kl$. We will show that the element xy has order kl. To show this, first suppose $(xy)^m = x^m y^m = 1$. We will show that $y^m = x^m = 1$ necessarily. For the sake of contradiction, suppose $y^m \neq 1$. Then, y^m is a power of x, and hence the order of y^m divides the order of x. Clearly, the order of y^m divides the order of x, and hence the order of y^m is a common factor of k and l. Since $y^m \neq 1$, this contradicts the fact that gcd$(k, l) = 1$. Hence, $x^m = y^m = 1$, i.e lcm$(k, l) = kl | m$. So, it follows that the order of xy is kl.

Next, let k, l be arbitrary, i.e gcd$(k, l) = 1$ is not necessary. Let

$$k = p_1^{a_1} ... p_n^{a_n}$$
$$l = p_1^{b_1} ... p_n^{b_n}$$

be the prime factorisations of k and l respectively. Now, we can easily find an element of order $p_i^{\max\{a_i, b_i\}}$ for each $1 \leq i \leq n$. The product of all these elements has order

$$p_1^{\max\{a_1, b_1\}} ... p_n^{\max\{a_n, b_n\}} = \text{lcm}(k, l)$$

because the orders of all these elements are pairwise coprime, and hence we can apply the case above. This completes the proof. ■

Proof of **Theorem** 3.15. Let G be any finite subgroup of $F^\times$, and let n be the lcm of the orders of all elements of G. If $y \in G$, then we have $y^n = 1$; now the polynomial $x^n - 1$ in $F[x]$ has atmost n roots, and hence we see that $|G| \leq n$. Moreover, by **Proposition** 3.16 we know that G contains an element α of order n, and hence $n | G$. This forces $|G| = n$, and hence $G = \langle \alpha \rangle$, i.e G is a cyclic group, completing the proof. ■