Algebra III

Kexing Ying

July 24, 2021

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

Contents

1 Rings

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

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

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

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

and

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

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

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

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

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

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

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

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

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

and,

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

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

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

1.1 Subrings and Extensions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

□

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.2 Homomorphisms and Ideals

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

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

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

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

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

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

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

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

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

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

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

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

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

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

for all $P \in R[X]$. □

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

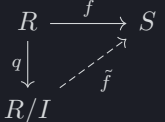
Definition 1.17 (Quotient Map)**.** Given R a ring and I an ideal of R, the quotient map is then the surjective ring homomorphism $q : R \to R/I : r \mapsto r + I$.

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

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

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

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

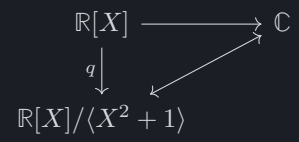


Proof. Uniqueness is clear and thus we will show $\tilde{f}$ is well-defined and is a ring homomorphism. Let $r \equiv s \mod I$, and will show $f(r) = f(s)$. Indeed, since $r - s \in I$, we have $r - s \in \ker f$ and so, $f(r) - f(s) = f(r - s) = 0$, hence $f(r) = f(s)$ and $\tilde{f}$ is well-defined.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

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

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

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



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

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

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

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

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

Since fields are integral domains, maximal ideals are prime.

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

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

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

1.3 Factorization and PIDs

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.4 Euclidean Domains

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

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

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

Proposition 1.16. Any Euclidean domain R is a PID.

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

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

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

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

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

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

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

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

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

1.5 Chinese Remainder Theorem

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

is an injection.

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

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

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

is an isomorphism.

Proof. It suffices to prove surjectivity.

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

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

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

2 Fields

2.1 Field Extensions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

For the last claim, it suffices to show that $\{f_j e_i\}_{i,j}$ as defined above is linearly independent. Suppose $\sum_{i,j} \lambda_{i,j} f_j e_i = 0$, then $0 = \sum_i (\sum_j \lambda_{i,j} f_j) e_i$ implying $\sum_j \lambda_{i,j} f_j = 0$ as $\{e_i\}$ is

linearly independent. Now as $\{f_i\}$ is also linearly independent, this implies $\lambda_{i,j} = 0$ for all i, j implying $\{f_j e_i\}_{i,j}$ is a basis of L over M. Thus, $[L : M] = \dim_M L = |\{f_j e_i\}_{i,j}| = rs = \dim_M K \dim_K L = [L : K][K : M]$ as required. □

2.1.1 One Element Extensions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.2 Finite Fields

Recall that any field contains a $\mathbb{F}_p$ or $\mathbb{Q}$ (the latter of which is impossible for finite fields). If K is a finite field and $\mathbb{F} \subseteq K$ for some prime p such that $[K : \mathbb{F}_p] = r < \infty$, then $|K| = p^r$ since each element of K is expressed uniquely by $a_1 e_1 + \cdots a_r e_r$ where $e_1, \cdots, e_r$ is a basis of K over $\mathbb{F}_p$ and $a_i \in \mathbb{F}_p$. Conversely, we asks whether or not there exists a field with p^r elements for any prime p, and if it exists, is it unique up to isomorphism.

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

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

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

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

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

Proposition 2.5. If K has characteristic p, then

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.2.1 Multiplicative Group

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

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

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

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

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

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

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

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

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

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

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

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

□

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