This section[1] introduces the basics of abstract algebra, including groups, rings, modules, fields, and ideals. The material covered are standard in algebra textbooks like Artin (1991). For students who want to learn how to think about abstract algebra, we recommend Alcock (2021).

0.1 Group theory

There are at least two motivations to study group theory for lattice-based cryptography. First, more advanced algebraic structures such as rings and fields are build upon the concepts of groups. Second, it provides a different view of lattices which are additive subgroups of $\mathbb{R}^n$.

Group **Definition 0.1.1.** *A **group** $G = (S, \cdot)$ is a set of elements together with a binary operator "$\cdot$" such that*

- *closed: for all $a, b \in S$, we have $a \cdot b \in S$,*
- *unique identity element: there exists a unique identity element $e \in S$ with respect to the binary operator,*
- *associative: for all $x, y, z \in S$, we have $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,*
- *unique inverse element: for all $x \in S$, there exists an element $y \in S$ such that $x \cdot y = e$.*

A group is an abstract algebraic structure. Elements in S can be integers, fractions, matrices, functions, etc. The group operator can be addition, multiplication, matrix multiplication, function composition, etc. The pair forms a group as long as the four groups axioms are satisfied.

When dealing with binary operators, one often wonders whether or not the same result will be produced if switching the order of the two inputs. That is, does $x \cdot y = y \cdot x$ for all $x, y \in S$? For some groups this is true, but not in general. For example, the condition is true for the additive group of integers $(\mathbb{Z}, +)$), but not the multiplicative group of $n \times n$ integer matrices $(M, \times)$. Such a property is called abelian or commutative.

Definition 0.1.2. *A group $(G, \cdot)$ is **abelian** (or **commutative**) if $x \cdot y = y \cdot x$ for all $x, y \in G$.*

In cryptography, we almost always work with abelian groups such as the integer group or the polynomial group.

The number of elements in a group can be finite or infinite. For groups with finitely many elements, we can definite the group order and element order as follows.

Order **Definition 0.1.3.** *The **order** of a group G is the number of elements in G.*

Definition 0.1.4. *For an element a in a group $(G, \cdot)$, if there exists a positive integer k such that $\underbrace{a \cdots a}_{k} = e$ is the group identity, then the element a has **order** k. If no such an integer k exists, then a has infinite order.*

Orders of groups and group elements are useful when working with finite groups. Every non-zero element in $(\mathbb{Z}, +)$ has infinite order. Let $\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$ be the group of integers modulo 3. The order of the group $(\mathbb{Z}/3\mathbb{Z}, +)$ is 3. The orders of the elements 0, 1, 2 are 1, 3, 3, respectively.

Some important examples of groups are:

- **Symmetric group** S_n: the set of all permutations of the indices $[n] := \{1, \ldots, n\}$. The group has order $|S_n| = n!$.
- **Cyclic group**: a group that is generated by a single element. For example, $(\mathbb{Z}, +)$ is an infinite cyclic group that is generated by 1. Another example is $(\mathbb{Z}/n\mathbb{Z}, +)$ which is a finite cyclic group of order n that is generated by 1. The element $g \in G$ that generates the entire group G is called a **generator**. The common notation is $G = \langle g \rangle$ or $G = C_n$ if G has a finite order n.
- **Dihedral group** D_n: a group of symmetries - reflection f and rotation r - of a regular n-gon. For example, $D_4 = \{e, f, r, r^2, r^3, fr, fr^2, fr^3\}$. The group operation is function composition.

[1] This section is part of the work *A Tutorial Introduction to Lattice-based Cryptography and Homomorphic Encryption* by the authors Yang Li, Kee Siong Ng, Michael Purcell from the School of Computing, Australian National University @2022.

- **Klein four group** K_4 **or** V_4 - a group of 4 elements in which each non-identity element has order 2 and the composition of two non-identity elements produces the third one. The Klein four group is isomorphic to the product of two cyclic groups of order 2, i.e., $V_4 \cong C_2 \times C_2$.

Definition 0.1.5. *Let $(G, \cdot)$ be a group. A subset H of G is a* ***subgroup*** *of $(G, \cdot)$ if H forms a group with G's operator.*

Sometimes we omit the group operator for simplicity. An important type of subgroups is normal subgroup.

Normal subgroup

Definition 0.1.6. *Let G be a group. A subgroup N of G is* ***normal*** *if N is invariant under group conjugation. That is, for all elements $g \in G$ and all elements $h \in N$, we have $g^{-1}hg \in N$.*

The notation for normal subgroups is $H \triangleleft G$ (or $H \trianglelefteq G$). Normal subgroups are important because they partition a group G into **cosets**, i.e., quotient group or factor group, which is important toward learning quotient rings. In addition, quotient groups regroup elements into non-overlapping classes which may help to reveal underlying structures of the original group that are difficult to be seen without the action of grouping.

To introduce quotient groups, we first introduce equivalence relations, based on which group elements are put together.

Definition 0.1.7. *A binary relation $\sim$ on a set S is said to be an* ***equivalence relation*** *if it satisfies the following axioms for all $a, b, c \in S$:*

- *reflexive: $a \sim a$,*
- *symmetric: $a \sim b$ if and only if $b \sim a$,*
- *transitive: if $a \sim b$ and $b \sim c$, then $a \sim c$.*

Left coset

Definition 0.1.8. *Given a subgroup H of G, we can define a* ***left coset*** *of H in G as the set of elements obtained by applying a fixed element of G (under the group operation) on the left of H. That is, for each element $g \in G$, the left coset of H is*

$$gH = \{gh \mid h \in H\}.$$

Right coset

The **right coset** is defined respectively. Let $G = (\mathbb{Z}, +)$ and $H = (2\mathbb{Z}, +)$. The left cosets of H in G are $0 + 2\mathbb{Z}$ and $1 + 2\mathbb{Z}$, because any additional cosets constructed by the other elements of G will be identical to these two. We denote the cosets by $\bar{0}$ and $\bar{1}$, respectively.

Each coset is an equivalence class with the equivalence relation "belong to the same coset". This can be checked easily. For elements $a, b \in G$, they belong to the same coset (i.e., $aH = bH$) if and only if $b^{-1}a \in H$. Given a normal subgroup $H \triangleleft G$, it divides G into several equal-sized equivalence classes.

Quotient group

Definition 0.1.9. *The* ***quotient group*** *of G by a normal subgroup $H \triangleleft G$, denoted by G/H, is the set of cosets of H in G.*

An important observation is that the set of cosets forms a group with the group operation in G. The identity element in the quotient group is precisely the normal subgroup H. That is why G/H is called a quotient GROUP. For example, the set $\{\bar{0}, \bar{1}\}$ and addition form a group, in which $\bar{0}$ is the identity. It can be checked that the normal subgroup assumption is necessary because it ensures the set of cosets forms a group. This is not always true if H is just an ordinary subgroup of G.

Index

Given a subgroup H of G, all cosets of H have the same size, so we have a quantity, namely the **index** of H in G and denoted by $|G : H|$, that is defined as the number of coset of H in G. If H is a normal subgroup of G, then the index $|G : H| = |G/H|$ is equal to the order of the quotient group.

We sometimes have a function f acts on a group $(G, \cdot)$ by mapping elements of G to another set H. In that case, we would like to know whether or not the same group structure is preserved in H by the function f. This function is formally defined as a group homomorphism.

Group homomorphism

Definition 0.1.10. *A* ***homomorphism*** *from a group $(G, \cdot)$ to a group $(H, *)$ is a function $f : G \rightarrow H$ such that for all elements $a, b \in G$ it holds that*

$$f(a \cdot b) = f(a) * f(b).$$

In other words, the relationship between the two elements in G are mapped to the relationship between the two corresponding elements in H. There are different types of group homomorphisms, depending on the function type and the function's codomain. The two important groups homomorphisms are isomorphisms and automorphisms.

Isomorphism **Definition 0.1.11.** *A homomorphism is called an* ***isomorphism*** *if it is bijective.*

If there is an isomorphism between two groups $(G, \cdot)$ and $(H, *)$, then they are isomorphic and denoted by $(G, \cdot) \cong (H, *)$. Isomorphisms are important because they tell you when two groups are identical. In addition, knowing one group will tell you everything about the other. An example of a group isomorphism is $f : (\mathbb{R}, +) \to (\mathbb{R}^+, \times)$ given by the function $f(x) = e^x$. A special case of isomorphism is between a group and itself, which we will see when introducing Galois theory.

Definition 0.1.12. *A homomorphism is called an* ***automorphism*** *if it is an isomorphism such that the domain and codomain are the same. That is, an isomorphism $f : G \to G$.*

0.2 Ring theory

Unlike groups, rings are algebraic structures associate with two binary operators, addition and multiplication such that ring axioms are satisfied.

Ring **Definition 0.2.1.** *A* ***ring*** *$R = (S, +, \times)$ is a set with two operations, namely addition and multiplication, such that the following ring axioms are satisfied:*

- *$(S, +)$ is an abelian group under addition,*
- *$(S, \times)$ is closed under multiplication, associative and contains the unique multiplicative identity 1,*
- *multiplication is distributive with respect to addition, i.e., $a \times (b + c) = a \times b + a \times c$ for all $a, b, c \in S$.*

A ring R is **commutative** (called commutative ring) if multiplication is also commutative in R. For example, the set of integers forms a commutative ring with integer addition and multiplication. However, none of the integers except 1 has a multiplicative inverse in the integer set. The set of $n \times n$ (real or integer) matrices forms a non-commutative ring with matrix addition and multiplication. Not all matrices have inverses. An important ring in lattice-based cryptography is the **ring of polynomials** or **polynomial ring** $\mathbb{Q}[x]$ or $\mathbb{Z}[x]$ with polynomial addition and multiplication as the ring operations. Again, not all polynomials in the ring $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$ have inverses in the same ring.

The pair $(S, \times)$ in a ring R almost forms a multiplicative group, but it lacks of multiplicative inverses in general. Without multiplicative inverses (of non-zero elements), division cannot be carried out in rings. For this purpose, we introduce division rings.

Definition 0.2.2. *A* ***unit*** *in a ring R is any element that has a multiplicative inverse in R.*

For example, 1 is the only unit in the ring of integers. But 1, 2 are both units in the ring $(\mathbb{Z}_3, +, \times)$.

Division ring **Definition 0.2.3.** *A* ***division ring*** *is a ring R in which every non-zero element is a unit. That is, every non-zero element has a multiplicative inverse in R.*

In a division ring, the pair $(S, \times)$ forms a multiplicative group, but not necessary abelian. If it is abelian, the ring is a field, which will be introduced in the next subsection. Similar to a group and its subgroups, subrings can be defined with respect to a ring.

Definition 0.2.4. *Let $(R, +, \times)$ be a ring. A subset $S \subset R$ is a* ***subring*** *if $(S, +, \times)$ forms a ring with the ring's addition and multiplication.*

The concept of a vector space can be generalized to a *module* which is defined similarly, but over a ring instead of a field. The main difference is that every element in a field has a multiplicative inverse, so a vector in a vector space can be scaled up or down by a scalar and its multiplicative inverse. However, not every element in a ring has a multiplicative inverse, so an element in a module cannot always be scaled up and down.

Module **Definition 0.2.5.** *Let R be a ring and 1 being its multiplicative identity. A* ***left R-module*** *M consists of an abelian group $(M, +)$ and an operation $\cdot : R \times M \to M$ such that for all $r, s \in R$ and $x, y \in M$, the following are satisfied:*

- $r \cdot (x + y) = r \cdot x + r \cdot y$
- $(r + s) \cdot x = r \cdot x + s \cdot x$
- $(rs) \cdot x = r \cdot (s \cdot x)$
- $1 \cdot x = x$

The concept of a **right R-module** is defined similarly. The distinction between a left and right module arises from the fact that the underlying ring R is not necessary commutative. In general, unless mentioned otherwise, a module refers to a left module. For example, a Z-module is a module over the integer ring Z which is commutative.

Definition 0.2.6. *Suppose M is a left R-module and N is a subgroup of M. Then N is an **R-submodule** (or just **submodule**) if for any $n \in N$ and any $r \in R$, we have $r \cdot n \in N$.*

The definition of submodule is similar to subspace of a vector space, where the subspace is closed under addition and scalar multiplication. A important type of module is called a free module.

Free module

Definition 0.2.7. *A **free module** is a module that has a basis.*

Here a basis is a set of linearly independent vectors that generates M. That is, every element of M can be written as a linear combination of the set of linearly independent vectors, where the coefficients are taken from the underlying ring R. So a **free $\mathbb{Z}$-module** is a module with a basis such that every element in the module is an integer combination of the basis.

Ideals

Similar to a normal subgroup, an ideal can partition a ring into cosets which form a ring with less elements, known as the *quotient ring*. As noted, not all subgroups can partition a group into a quotient group. Similarly, an ideal must have some special properties in order to construct a quotient ring.

First, a ring is an additive group with an extra operation, an ideal of the ring should be a normal subgroup under addition (in fact, being a subgroup is enough as a ring is an abelian group under addition which implies normality), so an ideal must be closed under addition. Second, for cosets to be closed under multiplication, ideals must be closed under multiplication by any ring elements. More specifically, an ideal I partitions a ring R into a set of equivalence classes, each denoted by $[a] := a + I = \{a + r \mid r \in I\}$. Since we want this set of equivalence classes to form a ring, it must satisfy

- $[a] + [b] = (a + I) + (b + I) = (a + b) + (I + I) = (a + b) + I = [a + b]$
- $[a][b] = (a + I)(b + I) = ab + aI + bI + II = ab + I = [ab]$.

So we can see that ideals have to satisfy at least three criteria. First, closed under addition by itself. Second, closed under multiplication by itself. Third, closed under addition by all elements in the ring. Noted that the third criterion includes the second, so at least two criteria need to be satisfied. The formal definition of an ideal is stated as below.

Definition 0.2.8. *For an arbitrary ring $(R, +, \times)$, the subset $I \subset R$ is a **left ideal** of the ring if it satisfies:*

- *$(I, +)$ is an additive subgroup of the group $(R, +)$,*
- *I is closed under left multiplication by all elements of R. That is, for every $r \in R$ and every $x \in I$, their product $rx \in I$.*

An **right ideal** is defined respectively. If I is both a left and right ideals, then it is a two-sided ideal of the ring. Again, since most rings considered in cryptography are commutative, we do not distinguish left and right ideals. Throughout, we use the term ideals for two-sided ideals unless mentioned otherwise. For example, the set of even integers form an ideal in the integer ring, because even integers are closed under addition and any integer multiplied by an even integer is still even.

Note that although an ideal is closed under addition and multiplication, it is not a ring because it does not necessary have a multiplicative identity, which is required by our definition of rings.

Ideals can be generated by a set of elements $a_1, \ldots, a_n \in R$, denoted by

$$(a_1, \ldots, a_n) = \{r_1 a_1 + \cdots + r_n a_n : r_i \in R\},$$

with the special case of $(a) = aR = Ra = \{ra : r \in R\}$. A **zero ideal** is an ideal contains only the zero element, i.e., $\{0\}$ or (0). A **unit ideal** is the ring itself. A **proper ideal** is a non-unit ideal.

Intuitively, one can think of an ideal of a ring R as a subset of R that absorbs R, so it is closed under addition, and multiplication by ring elements. Ideal is an important concept that will frequently appear in lattice-based cryptography. It helps to build a quotient ring or even a field if the ideal used is maximal. This is similar to the construction of quotient groups via normal subgroups.

Quotient ring

Definition 0.2.9. *The **quotient ring** of a ring R by an ideal I, denoted by R/I, is the set of cosets of I in R.*

The quotient ring R/I has the additive identity $\bar{0} = 0 + I$ (similar to a normal subgroup being the identity of the quotient group) and the multiplicative identity $\bar{1} = 1 + I$.

Some ideals have additional properties that can make the corresponding quotient rings special. Below we introduce three special ideals.

- Prime ideal → integral domain
- Principal ideal → principal ideal domain
- Maximal ideal → (residual) field

A prime ideal can be thought as a generalization of a prime number. Recall that if p is a prime number and $p|ab$ for integers a and b, then either $p|a$ or $p|b$.

Prime ideal

Definition 0.2.10. *An ideal P of a ring R is **prime** if it satisfies the following two properties:*

- *$P \neq R$,*
- *for any two elements $a, b \in R$, if their product $ab \in P$, then either $a \in P$ or $b \in P$.*

The set of even integers in the ring of integers is a prime ideal. To see why prime ideals are important, we introduce the concept of integral domains that are defined upon commutative rings.

Integral domain

Definition 0.2.11. *An **integral domain** is a non-zero commutative ring in which the product of two non-zero elements is non-zero.*

Integral domains are generalizations of the rings of integers of algebraic number fields that will be discussed in a later section. Integral domains provide a natural setting to study division, because they allow the cancellation of a non-zero factor a in an equation like $ab = ac$.

Proposition 0.2.12. *If $I \subsetneq R$ is a prime ideal, then the quotient ring R/I is an integral domain.*

Proof. I being a prime ideal implies that no two elements that are not in I can be multiplied to an element in I. Since I is the additive identity in the quotient ring R/I, it is the zero element in the quotient ring. This implies that no two non-zero elements (i.e., elements not in $\bar{0}$) can be multiplied to a zero element (i.e., an element in $\bar{0}$). □

For example, $12\mathbb{Z}$ is not a prime ideal, so the quotient ring $\mathbb{Z}/12\mathbb{Z}$ is not an integral domain because $3 \cdot 4 = 12 \equiv 0 \bmod 12$. But $\mathbb{Z}/5\mathbb{Z}$ is an integral domain. Another example is the ring of polynomials whose coefficients come from an integral domain.

Proposition 0.2.13. *If R is an integral domain, then the ring of polynomials $R[x]$ is also an integral domain.*

Proof. R is integral domain, the product of the leading coefficients of two non-zero polynomials is also non-zero, so $R[x]$ is an integral domain. □

Principal ideal

Definition 0.2.14. *An ideal in a ring R is **principal** if it can be generated by a single element of R through multiplication by every element of R.*

For example, $2\mathbb{Z}$ is a principle ideal in the integer ring, because it can be generated by 2 multiplying every element of $\mathbb{Z}$.

Definition 0.2.15. *A **principal ideal domain (PID)** is an integral domain in which every ideal is principal.*

As will be explained in detail later, fields are commutative division rings that possess nice properties for building cryptosystems. Given a ring R, one can construct a field by taking the quotient ring with a maximal ideal of R.

Maximal ideal

Definition 0.2.16. *A* ***maximal ideal*** *in a ring is an ideal that is maximal among all the proper ideals of the ring.*

In other words, if I is a maximal ideal in a ring R, then I is contained in only two ideals of R, i.e., I itself and the entire ring R. An important observation is that every maximal ideal is a prime ideal. This can be easily seen if we define the divisibility of ideals.

Proposition 0.2.17. *If I is a maximal ideal of a commutative ring R, then the quotient ring R/I is a field.*

Proof. (Sketch) I being a prime ideal is not sufficient to construct a field. Because the quotient ring R/I may have a proper ideal that is not the trivial ideal. That is, there may be an ideal I' in R/I that is not equal to $\{0\}$ or R/I. Hence, multiplication of an element in I' by an element not in I' will only get to elements in I'. This implies that not all non-zero elements in R/I have multiplicative inverses. □

The quotient ring R/I constructed using the maximal ideal is called a **residual field**.

Another concept that will be mentioned later and could help to understand the structure of fields are the characteristic of a ring. If it helps, the characteristic of a ring can be thought as the cyclic period of a ring. For example, the ring $\mathbb{Z}/4\mathbb{Z}$ has a characteristic 4 which is the rings cyclic period.

Characteristic

Definition 0.2.18. *The* ***characteristic*** *of a ring R, denoted by $char(R)$, is the smallest number of times that the ring's multiplicative identity 1 can be added to itself to get the additive identity 0. If the ring's multiplicative identity can never be summed to get 0, then the ring has a characteristic zero.*

The characteristic of a ring R may also be taken as the smallest positive integer n such that $\underbrace{a + \cdots + a}_{n} = 0$ for every element $a \in R$ (if the characteristic exists). For example, the characteristic of $\mathbb{Z}_3$ is 3 because $1 + 1 + 1 = 3 \equiv 0 \bmod 3$ or $2 + 2 + 2 = 6 \equiv 0 \bmod 3$. We will talk more about the characteristics of fields in the following subsection.

kernel

The First Isomorphism Theorem for rings is the fundamental method for identifying quotient rings. In the below, ring homomorphism is defined analogously to group homomorphism, and the kernel of a map $\varphi : R \to S$ is the subset of R that map to the zero element in S: $ker(\varphi) = \{r \in R : \varphi(r) = 0\}$.

First Isomorphism Theorem

Theorem 0.2.19. *Let R and S be rings and let $\varphi : R \to S$ be a ring homomorphism. Then*

1. *the kernel of φ is an ideal of R;*
2. *the image of φ is a subring of S; and*
3. *$R/ker(\varphi)$ is isomorphic to the image of φ.*

0.3 Field theory

A field is a commutative division ring. That is, a field is a ring if $(S^*, \times)$ is an abelian group under multiplication, where $S^* := S \setminus \{0\}$ is the set of non-zero elements. More formally, we have the next definition.

Field

Definition 0.3.1. *A* ***field*** *$F = (S, +, \times)$ is a set with two binary operators, addition and multiplication, such that the following field axioms are satisfied:*

- *$(S, +)$ is an abelian group under addition,*
- *$(S^*, \times)$ is an abelian group under multiplication,*
- *multiplication is distributive with respect to addition, that is, $a \times (b + c) = a \times b + a \times c$ for all $a, b, c \in S$.*

Examples of fields are the field of rational numbers, real numbers and complex numbers. The smallest field is $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$, because a field must contain at least two distinct elements 0 and 1.

A field is an integral domain, because non-zero elements have multiplicative inverses, which eliminates the possibility that their product is zero.

Sometimes, it is easier to construct a field from a given commutative ring rather than build it from scratch. One can construct a field from a commutative ring in two ways, by building the field of fractions or by quotienting the commutative ring by a maximal ideal as discussed earlier in Proposition 0.2.17.

Field of fractions

Definition 0.3.2. *Let R be an integral domain. The* ***field of fractions*** $Frac(R)$ *is the set of equivalence classes on $R \times (R \setminus \{0\})$ defined by*

$$Frac(R) = \{(p, q) \in R \times (R \setminus \{0\}) \mid (p, q) \sim (r, s) \iff ps = qr\}.$$

This definition generalizes the idea of creating fractions from integers. For example, if $R = \mathbb{Z}$ then $\frac{p}{q} \in [(p, q)] \subseteq Frac(\mathbb{Z}) = \mathbb{Q}$. More precisely, let $p = 5, q = 20$ then $5/20$ is an element in the equivalence class consists of $\{1/4, 5/20, 25/100, \dots\}$, which is also called the set of all equivalent fractions. The reason for R being an integral domain is because we can have the usual addition and multiplication in the field of fractions without running into the trouble of having a zero divisor. For example, $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, since R is an integral domain it is guaranteed that $bd \neq 0$.

Proposition 0.3.3. *A non-zero commutative ring R is a field if and only if it has no ideals other than (0) and R.*

Proof. If R is a field, then every non-zero element has a multiplicative inverse. If I is a non-zero ideal of R and $a \in I$, then $a^{-1}a = 1 \in I$. So $I = R$. If R has no proper non-zero ideal, then the ideal $I = R$ is a principal ideal. That is, $I = (a)$ for $a \neq 0$. Hence, there must exist an element $b \in R$ such that $ab = 1$. Hence, R is a field. □

This proposition implies an important property of a field: its only ideals are the zero ideal and the field itself.

Finite field

One type of fields that is essential in cryptography is called **finite fields**. These are fields with finitely many elements. The number of elements in a finite field is the **order** of the field (just like the order of a group). For example, $\mathbb{Z}_2 = \{0, 1\}$ is a finite field of order 2.

Field characteristics is an important concept that can be used to decide the separability of extension fields. We will see more about the connection between field characteristic and separability in a later section.

$Char(F) = 0$ or prime

Lemma 0.3.4. *The characteristic of any field is either 0 or a prime number.*

Proof. Let n be the characteristic of the field F. It is easy to see that $n \neq 1$, because a field is not a trivial ring, so $1 \neq 0$. Assume $n = pq$ is a composite number, where $1 < p, q < n$. This implies that $\underbrace{(1 + \cdots + 1)}_{p}\underbrace{(1 + \cdots + 1)}_{q} = \underbrace{1 + \cdots + 1}_{n} = 0$. Hence, we have $pq = 0$ which contradicts with the fact that the field is also an integral domain. □

Corollary 0.3.5. *This lemma implies that the characteristic of any finite field is a prime number.*

Corollary 0.3.6. *The characteristic of a subfield is the same as the characteristic of the field.*

Theorem 0.3.7. *In a field of characteristic p where p is prime, the only p-th roots of unity is 1.*

In a field of prime characteristic p, we have $x^p - 1 = (x - 1)^p$ because after expanding $(x - 1)^p$, all terms except x^p and -1^p have coefficients that are multiples of p, which vanish when taking modulo p. Hence, solving $x^p - 1 = 0$ is equivalent to solving $(x - 1)^p = 0$, where the only solution is $x = 1$.

So far in this section, we have introduced the concepts of groups, rings, fields and other related concepts. These will serve as a foundation for studying the Galois theory and algebraic number theory.

References

L. Alcock. *How to think about Abstract Algebra.* Oxford University Press, 2021.

M. Artin. *Algebra.* Prentice Hall, 1991.