MAT 345 Notes

Max Chien

Fall 2024

Contents

Introduction

This document contains notes taken for the class MAT 345: Algebra I at Princeton University, taken in the Fall 2024 semester. These notes are primarily based on lectures and lecture notes by Professor Jakub Witaszek. Other references used in these notes include *Algebra* by Michael Artin, *Abstract Algebra* by David Dummit and Richard Foote, *Contemporary Abstract Algebra* by Joseph Gallian, and *A Book of Abstract Algebra* by Charles Pinter. Since these notes were primarily taken live, they may contains typos or errors.

Chapter 1

Elementary Number Theory

This course will study algebraic structures, primarily groups, rings, and fields. These objects serve as abstractions of objects which we are familiar with performing algebra over, such as $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. As such, we will begin with a brief survey of algebraic operations over these familiar objects, before progressing to their abstracted counterparts.

1.1 The Euclidean Algorithm

The most important theorem of the structure of the integers is the following:

Theorem 1.1: Fundamental Theorem of Arithmetic

Let $n \in \mathbb{N}$. Then there is a unique representation of n as a product of powers of primes (up to ordering), as

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$$

Another important operation to abstract is that of division. This requires phrasing it in terms that are easily generalized to other objects:

Theorem 1.2: Division Algorithm

Let $n, d \in \mathbb{Z}$ with $d > 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that

$$n = qd + r$$

and

$$0 \leq r < d$$

Proof. **Existence:** Define

$$S = \{n - dx | x \in \mathbb{Z}, n - dx \geq 0\}$$

Let $r = \min S$ and let $q \in \mathbb{Z}$ be the corresponding value such that $n - qd = r$. Suppose that $r \geq d$. Then

$$n - (q+1)d = n - qd - d = r - d \geq 0$$

so $r - d \in S$, contradicting $r = \min S$. So $0 \leq r < d$. Thus we have shown existence.

Uniqueness: Let $n = qd + r = q'd + r'$. Then

$$d(q - q') + r - r' = 0$$

so $d|r - r'$. But we also have $-d < r - r' < d$, so $r - r' = 0$ and thus $r = r'$. It follows that $q = q'$. □

We call d the divisor, q the quotient, and r the remainder. Explicitly, we have

$$n = \left\lfloor \frac{n}{d} \right\rfloor d + (n \bmod d)$$

The proof of the Fundamental Theorem of Arithmetic requires the proof of some other lemmas:

Definition 1.3

Let $a, b \in \mathbb{Z}$. We write $a|b$ if there exists $c \in \mathbb{Z}$ such that $ac = b$.

Lemma 1.4: Euclid's lemma

Let p be prime and $a, b \in \mathbb{Z}$. If $p|ab$, then $p|a$ or $p|b$.

This, in turn, relies on another identity.

Definition 1.5

Let $a, b \in \mathbb{N}$. Then define $\gcd(a, b)$ to be a common divisor which divides any other common divisor.

We should note that we have not shown that $\gcd(a, b)$ exists and is unique. However, consideration of the extended Euclidean algorithm shows both of these, and moreover that $\gcd(a, b)$ is the largest common divisor of a and b.

Proposition 1.6: Bezout's Identity

Let $a, b \in \mathbb{Z}$ be nonzero. Then there exist $k, l \in \mathbb{Z}$ such that

$$ka + lb = \gcd(a, b)$$

Example 1.7

if $a = 9$ and $b = 24$, then

$$3 \cdot 9 + (-1) \cdot 24 = 3 = \gcd(9, 24)$$

Bezout's Identity follows from the **extended Euclidean Algorithm**.

The extended Euclidean algorithm takes two nonzero integers a, b and an integer m which is divisible by $\gcd(a, b)$, and produces integers k, l such that

$$ka + lb = m$$

First, we define the standard Euclidean algorithm. Note that we have the following:

$$\gcd(a, b) = \begin{cases} \gcd(a - b, b), & a \geq b \\ \gcd(a, b - a), & a < b \end{cases}$$

This holds since if $k|a$ and $k|b$, then $k|a - b$ and $k|b - a$. If $k|a - b$ and $k|b$, then $k|a$, so the top equality is proved. Similarly the second is true. Thus we proceed by applying the above equality repeatedly, until we have either $\gcd(a, a) = a$.

Example 1.8

We have

$$\gcd(24, 9) = \gcd(15, 9) = \gcd(6, 9) = \gcd(6, 3) = \gcd(3, 3) = 3$$

We can also skip steps by using the rule

$$\gcd(a, b) = \begin{cases} \gcd(a \bmod b, b), & a \geq b \\ \gcd(a, b \bmod a), & a < b \end{cases}$$

which holds by repeated application of the previous rule. This would give

$$\gcd(24, 9) = \gcd(6, 9) = \gcd(6, 3) = \gcd(3, 3) = 3$$

To extend the algorithm, we use the Euclidean algorithm and apply it to the following:

$$\begin{gathered} \blacksquare \cdot x + \blacksquare \cdot y = m \\ \blacksquare \cdot (x \bmod y) + \blacksquare \cdot y = m \\ \vdots \\ \blacksquare \cdot \gcd(x, y) + \blacksquare \cdot 0 = m \end{gathered}$$

We can then solve the bottom equality and pass back up the chain of equalities, preserving values which are unchanged in each step of the Euclidean algorithm.

Example 1.9

Let $x = 9, y = 24$ and $m = 12$. We have

$$\begin{aligned} \blacksquare \cdot 9 + \blacksquare \cdot 24 &= 12 \\ \blacksquare \cdot 9 + \blacksquare \cdot 6 &= 12 \\ \blacksquare \cdot 3 + \blacksquare \cdot 6 &= 12 \\ \blacksquare \cdot 3 + \blacksquare \cdot 3 &= 12 \\ \blacksquare \cdot 3 + \blacksquare \cdot 0 &= 12 \end{aligned}$$

We can then fill in the bottom line:

$$\begin{aligned} \blacksquare \cdot 9 + \blacksquare \cdot 24 &= 12 \\ \blacksquare \cdot 9 + \blacksquare \cdot 6 &= 12 \\ \blacksquare \cdot 3 + \blacksquare \cdot 6 &= 12 \\ \blacksquare \cdot 3 + \blacksquare \cdot 3 &= 12 \\ 4 \cdot 3 + 0 \cdot 0 &= 12 \end{aligned}$$

To move up to the next line, since the right term was changed when progressing down, the coefficient should stay the same when progressing up. In fact, the left hand coefficient stays the same as well:

$$\begin{aligned} 4 \cdot 3 + 0 \cdot 3 &= 12 \\ \Uparrow & \\ 4 \cdot 3 + 0 \cdot 0 &= 12 \end{aligned}$$

In the next line, we again change the left hand coefficient and keep the right hand (once again this changes nothing):

$$\begin{aligned} 4 \cdot 3 + 0 \cdot 6 &= 12 \\ \Uparrow & \\ 4 \cdot 3 + 0 \cdot 3 &= 12 \end{aligned}$$

Now, we keep the left hand coefficient and switch the right hand:

$$\begin{aligned} 4 \cdot 9 + (-4) \cdot 6 &= 12 \\ \Uparrow & \\ 4 \cdot 3 + 0 \cdot 3 &= 12 \end{aligned}$$

and finally:

$$\begin{aligned} 12 \cdot 9 + (-4) \cdot 24 &= 12 \\ \Uparrow & \\ 4 \cdot 9 + (-4) \cdot 6 &= 12 \end{aligned}$$

So we have found $k = 12, l = -4$.

Proof of Euclid's Lemma. If $p|a$, then we are done. So suppose it doesn't. Then $\gcd(p, a) = 1$. By Bezout's identity, there exist $k, l \in \mathbb{Z}$ such that

$$kp + la = 1$$

So $kpb + lab = b$. p divides the left hand side since it is in the product, and divides the right hand side since it divides ab. □

1.2 Modular Arithmetic

Definition 1.10

Let $a, b \in \mathbb{Z}$, and let $n > 0$ be an integer. Then a is **congruent** to b modulo n (denoted $a \equiv b \pmod{n}$) if

$$n|a - b$$

It follows that congruence modulo n is an equivalence relation for any n, dividing the integers into n classes based on their remainders after dividing by n.

We may equivalently define this congruence as follows:

Proposition 1.11

$a \equiv b \pmod{n}$ if and only if $a \bmod n = b \bmod n$ (where $a \bmod n$ represents the remainder of a when divided by n.)

A convenient example of modular arithmetic is the use of a 12-hour clock system, where the hour hand resets after each multiple of 12. We may similarly visualize modular arithmetic for any n as movement around a circle with n distinct positions.

Lemma

Let $a, b, c, d \in \mathbb{Z}$ and let $n \in \mathbb{N}$. Suppose that

$$\begin{cases} a \equiv c \pmod{n} \\ b \equiv d \pmod{n} \end{cases}$$

Then

$$\begin{cases} a + b \equiv c + d \pmod{n} \\ ab \equiv cd \pmod{n} \end{cases}$$

Essentially, the above lemma says that we may replace any number by another number which is equivalent modulo n (for addition and multiplication).

Example 1.12

We have

$$7 \cdot 22 \equiv 1 \cdot 4 \equiv 4 \pmod 6$$

Similarly,

$$(5+12)8+13 \equiv (5+5)1+6 \equiv 3 \cdot 1+6 \equiv 2 \pmod 7$$

Theorem 1.13

Let p be prime and let $k \in \mathbb{Z}$, and suppose p does not divide k. Then

$$k \bmod p, 2k \bmod p, \ldots, (p-1)k \bmod p$$

is a permutation of

$$1, 2, \ldots, p-1$$

Proof. Suppose that not all of these values are different, such that there exist $1 \leq n_1, n_2 \leq p-1$ but $n_1 k \bmod p = n_2 k \bmod p$. But this means that $(n_2 - n_1)k \bmod p = 0$, so p divides $(n_2 - n_1)k$. It doesn't divide k, so it divides $n_2 - n_1$. But $-p < n_2 - n_1 < p$. The only number in this range which p divides is 0, so $n_1 = n_2$.

Thus the list

$$k \bmod p, \ldots, (p-1)k \bmod p$$

is a list of $p-1$ distinct numbers between 1 and $p-1$. So each number occurs at least once, and we have just shown that they are distinct, so each number occurs exactly once. □

One interpretation of this is that if you repeatedly take k steps around a circle with p positions, then if p does not divide k, we will not repeat spaces until we have covered all of them.

Corollary 1.14

Let p be prime and $a \in \mathbb{Z}$ such that p does not divide a. Then there exists $b \in \mathbb{Z}$ such that

$$ab \equiv 1 \pmod p$$

For any b which satisfies the above, we call b a **multiplicative inverse** of a.

Proof. By Theorem 1.13, there exists some n with $1 \leq n \leq p-1$ such that $nk \bmod p = 1$ □

Note that multiplicative inverses found this way are *not* unique. Thus it is improper to write an expression of the form $\frac{1}{a} \pmod p$.

Remark

A multiplicative inverse may be found using the extended Euclidean algorithm.

Theorem 1.15: Fermat's Little Theorem

Let p be prime and $a \in \mathbb{Z}$ such that p does not divide a. Then

$$a^{p-1} \equiv 1 \pmod{p}$$

Example 1.16

With $a = 2, p = 7$ we have

$$\begin{aligned} 2^0 = 1 &\equiv 1 \pmod{7} \\ 2^1 = 2 &\equiv 2 \pmod{7} \\ 2^2 = 4 &\equiv 4 \pmod{7} \\ 2^3 = 8 &\equiv 1 \pmod{7} \\ 2^4 = 16 &\equiv 2 \pmod{7} \\ 2^5 = 32 &\equiv 4 \pmod{7} \\ 2^6 = 64 &\equiv 1 \pmod{7} \end{aligned}$$

Note that $7 - 1 = 6$ is not the first b with $a^b \equiv 1 \pmod{p}$. However, the remainders do occur in cycles, and the period of this cycle divides $p - 1$.

Lemma

Suppose n does not divide k. If

$$ak \equiv bk \pmod{n}$$

then

$$a \equiv b \pmod{n}$$

Proof. We have $n|(a-b)k$, so by Euclid's Lemma $n|a-b$. Thus $a \equiv b \pmod{n}$. □

Proof of Fermat's Little Theorem. Take the product

$$a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv a^{p-1}(p-1)! \pmod{p}$$

(Note that this is a simple equality). But Theorem 1.13 tells us that modulo p, these factors are a rearrangement of $1, \ldots, p-1$. So we have

$$(p-1)! \equiv a \cdot 2 \ldots \cdot (p-1) \pmod{p}$$

Combining these two congruences and applying the Lemma, we have

$$a^{p-1} \equiv 1 \pmod{p}$$ □

1.3 Fields

We recall the definition of a field:

Definition 1.17

A field is a nonempty set F together with two operations $+ : F \times F \to F$ and $\cdot : F \times F \to F$ as well as distinct elements $0 \neq 1 \in F$ such that

- $+$ and $\cdot$ are commutative.
- $+$ and $\cdot$ are associative.
- 0 is an additive identity and 1 a multiplicative identity.
- Additive inverses exist (denoted $-\alpha$).
- Multiplicative inverses exists for any $\alpha \neq 0$ (denoted α^{-1}).
- $\cdot$ distributes over $+$.

Some familiar examples of fields are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. A nonexample is $\mathbb{Z}$ (which does not have multiplicative inverses.)

Definition 1.18

Let p be prime. Then we define $\mathbb{F}_p = \{\ldots, \overline{-2}, \overline{-1}, \overline{0}, \overline{1}, \overline{2}, \ldots\}$, where the elements $\overline{k}$ are defined such that

$$\overline{a} = \overline{b} \iff a \equiv b \pmod{p}$$

We define

$$\overline{a} + \overline{b} = \overline{a+b}$$

and

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

Example 1.19

With $p = 6$, we have

$$\overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$$

Equivalently, since we identify numbers congruent modulo p, Theorem 1.13 we can simply write

$$\mathbb{F}_p = \{\overline{0}, \ldots, \overline{p-1}\}$$

all of which are distinct. Moreover, Corollary 1.14 assures us of the existence of multiplicative inverses. The remaining axioms are simpler to check, but this demonstrates that $\mathbb{F}_p$ is in fact a field.

Definition 1.20

The set $\mathbb{Z}/n\mathbb{Z}$ is defined similarly to $\mathbb{F}_p$ (where n is not necessarily prime), with only the operation of addition defined.

We can use this to prove the following theorem:

Theorem 1.21

Let p be prime with $p \equiv 1 \pmod 4$. Then $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$.

We can check the first few cases by hand:

$$\begin{aligned} 5 &= 1^2 + 2^2 \\ 13 &= 2^2 + 3^2 \\ 17 &= 1^2 + 4^2 \\ 29 &= 2^2 + 5^2 \end{aligned}$$

For the cases $p \geq 37$, we will develop a bit more theory.

Proof. □

Definition 1.22

$a \in \mathbb{F}_p$ is called a **quadratic residue** if $a = x^2$ for some $x \in \mathbb{F}_p$.

Equivalently:

Definition 1.23

$a \in \mathbb{Z}$ is a quadratic residue mod p if $a \equiv x^2 \pmod p$ for some $x \in \mathbb{Z}$.

Example 1.24

With $p = 5$, we have

$$\begin{cases} 0^2 \equiv 0 \\ 1^2 \equiv 1 \\ 2^2 \equiv 4 \\ 3^2 \equiv 4 \\ 4^2 \equiv 1 \end{cases} \pmod 5$$

so the quadratic residues are $0, 1, 4$ (note that 0 is always a quadratic residue.)

The necessary result is as follows:

Lemma

-1 (or $p-1$) is a quadratic residue mod p if and only if $p \equiv 1 \pmod 4$.

Proof. Skipped. □

We can now return to the previous proof.

Proof of Theorem 1.21. **Claim 1:** There exists $x, y \in \mathbb{Z}$ with $0 < x, y < p$ and

$$x^2 + y^2 \equiv 0 \pmod p$$

To show this, by the Lemma we have that -1 is a quadratic residue, so there exists $a \in \mathbb{Z}$ with

$$a^2 \equiv -1 \pmod p$$

or

$$1^2 + a^2 \equiv 0 \pmod p$$

Now let $x = 1$, $y = a \bmod p$. Claim 1 is proved.

Claim 2: There exist $x, y \in \mathbb{Z}$ with $x^2 + y^2 < 2p$ and $x^2 + y^2 \equiv 0 \pmod p$.

To show this, apply Claim 1 to produce x, y with $x^2 + y^2 \equiv 0 \pmod p$. Then let S be the set

$$S = \{(x_0, y_0), \ldots, (x_{p-1}, y_{p-1})\} \subseteq \mathbb{Z}^2$$

where

$$(x_i, y_i) = (ix \bmod p, iy \bmod p)$$

This set may be seen as the set of integer multiples of the point (x, y), modulo p.

Now, we claim that there exists $0 \leq i < j \leq p-1$ such that

$$d((x_i, y_i), (x_j, y_j)) < \sqrt{2p}$$

To show this, we draw circles of radius

$$\frac{\sqrt{2p}}{2}$$

around. If the claim is false then the circles do not overlap. All the circles are subsetes of

$$\left[-\frac{\sqrt{2p}}{2}, p + \frac{\sqrt{2p}}{2}\right]^2$$

If they do not overlap, then the total area is less than that of the square. But

$$1.57 \approx \frac{\pi}{2}p^2 = p\pi(\frac{\sqrt{2p}}{2})^2 \leq (p + \sqrt{2p})^2 = p(1 + \sqrt{\frac{2}{p}}) \leq p(1 + \sqrt{\frac{2}{37}})^2 \approx 1.51$$

We checked the lower cases, so the claim is proved. Then pick

$$(x', y') = (|x_j - x_i|, |y_j - y_i|)$$

We then show that p divides $(x')^2 + (y')^2$, but also this number is less than $2p$, so it is p. □

Chapter 2

Elementary Group Theory

In this chapter, we will introduce our first algebraic structure: the group. This will take some of the ideas we have discovered about number theory and translate it to the setting of an arbitrary set with one operation, sbuject to certain axioms which ensure the operation is "nice enough." Some motivating examples, then, will be the groups $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$, where we have already proved a few results in the preceding chapter.

2.1 Binary Operations

Definition 2.1

A **binary operation** on a set S is a function $* : S \times S \to S$.

In other words, $\star$ takes in two inputs in S and returns another. We typically denote $\star(a, b)$ as $a \star b$.

Example 2.2

- If $S = \mathbb{R}$, then we may define $a \star b = a + b$, or $a \star b = a \cdot b$.
- If S is the set of functions $f : X \to X$ for some set X, we may define $f \star g = f \circ g$.
- If S is the set of $n \times n$ matrices over a field, then the operation may be taken as addition or multiplication.

Certain operations possess properties which make them particularly nice to work with. In particular, we say that an operation $\star$ is **commutative** if $a \star b = b \star a$ for all $a, b \in S$, and it is **associative** if $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in S$. In the case that $\star$ is associative, then any finite combination of elements may be written without parentheses, as the order is irrelevant, so we may simply denote this as $a_1 \star a_2 \star \ldots \star a_n$.

Example 2.3

- Addition and multiplication are both commutative and associative on $\mathbb{R}$.
- Function composition is only associative.
- Matrix addition is commutative and associative, but multiplication is only associative.

As we see from the example above, commutativity is nice but not always present, but associativity is an extremely common property of operations that we work with often. However, for arbitrary binary operations it is not necessarily the case.

Example 2.4

Define a binary operation $\star$ on the set $S = \{0, 1\}$ by

$$\begin{cases} 0 \star 0 = 1 \\ 0 \star 1 = 1 \\ 1 \star 0 = 1 \\ 1 \star 1 = 0 \end{cases}$$

Then

$$(0 \star 1) \star 1 = 1 \star 1 = 0$$

but

$$0 \star (1 \star 1) = 0 \star 0 = 1$$

so this operation is not associative.

Definition 2.5

Let $\star$ be a binary operation on S. An element $e \in S$ is called an **identity** for $\star$ if

$$e \star x = x \star x = x$$

for all $x \in S$.

Proposition 2.6

Every binary operation has at most one identity.

Proof. Suppose e_1, e_2 are identities for $\star$ on S. Then

$$e_1 = e_1 \star e_2 = e_2$$

so $e_1 = e_2$. □

Definition 2.7

Let $\star$ be a binary operation on S with identity e. Then for $x \in S$, we say that $y \in S$ is an **inverse** of x if

$$x \star y = y \star x = e$$

If x has an inverse we say it is invertible.

Proposition 2.8

For $x \in S$ with $\star$ an associative binary operation on S with identity e,

1. x has at most one inverse $y \in S$.
2. If $la = e$ and $ar = e$, then $l = r$.
3. If a, b are invertible, then $a \star b$ is invertible and $(a \star b)^{-1} = b^{-1} \star a^{-1}$.
4. An element may have a left inverse or a right inverse, but not be invertible (but not both).

Proof. Skipped. □

2.2 Groups

We will now use our definition of binary operations to study sets equipped with the structure imposed by such an operation.

Definition 2.9

A **group** $(G, \star)$ consists of a nonempty set G with a binary operation $\star$ on G such that

1. $\star$ is associative.
2. There exists $e \in G$ which is an identity for $\star$.
3. For each $g \in G$, there exists an inverse element $h \in G$ for g under $\star$.

Under a slight abuse of notation, we will typically refer to $(G, \star)$ as G when the operation is clear.

Noting that we only required that $\star$ be associative, but not commutative, we give a special name for groups where $\star$ is commutative.

Definition 2.10

$(G, \star)$ is called **abelian** if $\star$ is commutative on G.

Let us make a few comments about notation. In general, e represents the identity of $\star$. However, we may sometimes write $+$ to denote a commutative operation and 0 its identity, and $\cdot$ an arbitrary operation with identity 1. When $\star$ is abelian we may write $-g$ to denote the inverse of g, and g^{-1} otherwise. We will also denote the repeated composition $\underbrace{g \star \ldots \star g}_{n \text{ times}}$ as ng for abelian groups and g^n for arbitrary groups.

Example 2.11

The following are examples of abelian groups:

- $(\mathbb{Z}, +)$
- $(\mathbb{F}, +)$
- $(\mathbb{F} \setminus \{0\}, \times)$
- $(M_{n\times m}(\mathbb{F}), +)$

The following are examples of nonabelian groups:

- $(\mathrm{GL}_n(\mathbb{R}), \times)$, where $\mathrm{GL}_n(\mathbb{R})$ is the set of $n \times n$ invertible real matrices.
- $(\mathrm{SL}_n(\mathbb{Z}), \times)$, where $\mathrm{SL}_n(\mathbb{Z})$ is the set of $n \times n$ matrices with determinant 1 and integer entries.
- S_n, where S_n is the group of **permutations** (a permutation on S is a bijection $f : S \to S$) on n elements.
- D_n, where D_n is the group of symmetries of the n-gon.[a]

[a] This is sometimes referred to as D_{2n}, since it has $2n$ elements.

Some other important matrix groups, which will not necessarily be important in this class, are:

- O_n, which is the set of real orthogonal matrices.
- SO_n, which is the set of real orthogonal matrices with determinant 1.
- U_n which is the set of complex orthogonal matrices.
- SU_n, which is the set of complex orthogonal matrices with determinant 1.
- SP_{2n}, which is the set of $P \in \mathrm{GL}_{2n}(\mathbb{R})$ such that $P^T S P = S$ for all S.
- $O_{3,1}$ (the Lorentz group), which is the set of $P \in \mathrm{GL}_4(\mathbb{R})$ with $P^T I_{3,1} P = I_{3,1}$.

Definition 2.12

The **order** of an element $g \in G$ is the smallest natural number $n \in \mathbb{Z}_{>0}$ such that

$$g^n = e$$

Definition 2.13

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

Although the word order appears to be used for different notions here, we will see that the order of $g \in G$ is the order of the subgroup $\langle g \rangle$ generated by g.

Consider the set $\mathbb{Z}/n\mathbb{Z}$. Under addition, it is an abelian group, but under multiplication it is not, since there are inverses missing. However, removing $\{0\}$ is not sufficient. For instance, consider $\overline{4} \in \mathbb{Z}/24\mathbb{Z}$. Every multiple of 4 mod 24 is a multiple of 4, so 1 is not equal to $n4$ for any $n \geq 1$. This only works when n is prime, which is why $\mathbb{F}_p$ is only a group for p prime. Alternatively, we can fix the set as follows:

Definition 2.14

Define $(\mathbb{Z}/n\mathbb{Z})^\times := \{\overline{a} | a \in \mathbb{Z}, \gcd(a, n) = 1\}$.

Then $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ is a group. Moreover, its order is $\phi(n)$, where $\phi(n)$ is Euler's totient function.

Example 2.15

For $n = 15$, $(\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\}$.

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

The orders of of 1, 2, 3, 4 are 1, 4, 4, and 2, respectively.

Note that the interior of the table above resembles a Sudoku board, in the sense that each row and column contains each of the elements 1, 2, 3, 4 exactly once.

Lemma 2.16

Let G be a finite group $G = \{g_1, \ldots, g_n\}$. Then the elements $gg_1, gg_2, \ldots, gg_n$ are a permutation of $g_1, \ldots, g_n$.

Proof. We need to show that $\phi_g : G \to G$ given by $\phi_g(x) = gx$ is a bijection. But if we consider $\phi_{g^{-1}}$, we have

$$(\phi_g \circ \phi_{g^{-1}})(x) = gg^{-1}x = x$$

and

$$(\phi_{g^{-1}} \circ \phi_g)(x) = g^{-1}gx = x$$

so ϕ_g has an inverse and is thus a bijection. □

Corollary 2.17

Let G be a finite abelian group of order n. Then for $g \in G$, $g^n = e$.

Proof. We have

$$(gg_1)(gg_2)\dots(gg_n) = g^n(g_1g_2\dots g_n)$$

and by Corollary 2.17,

$$(gg_1)(gg_2)\dots(gg_n) = g_1g_2\dots g_n$$

so $g^n = e$ by cancellation. □

Note that the above corollary applied to $(\mathbb{Z}/p\mathbb{Z} \setminus \{0\}, \times)$ recovers Fermat's Little Theorem, and applied to $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ for arbitrary n recovers Euler's Theorem.

2.3 Subgroups

Definition 2.18

A subgroup of a group $(G, \star)$ is a group $(H, \star|_H)$, where $H \subseteq G$ and $\star_H$ is the restriction of $\star$ to $H \times H$.

Equivalently, we have the following condition, which will allow for easier verification of subgroups.

Proposition 2.19

$H \subseteq G$ is a subgroup of G if and only if

1. $a, b \in H$ implies that $a \star b \in H$.
2. $e \in H$.
3. $a \in H$ implies $a^{-1} \in H$.

Definitions