ALGEBRA FOR CRYPTOLOGISTS

JOHN W. JONES

These notes were written for the beginning of MAT 448, *Cryptography II*. There are basic notions from abstract algebra, particularly from group theory, which are essential throughout the course. On the other hand, we will not need advanced aspects of group theory like the Sylow theorems, so we will cover everything we need relatively quickly.

Contents

1. Notation and conventions

Note that in proofs by contradiction, we use the symbol $\lightning$ to indicate that a contradiction has been reached.

1.1. **Famous sets.** Here we collect definitions and notation to be used throughout. It is intended more as a reference than an introduction. In particular, we specify what natural algebraic structures these sets possess even though those structures are not defined until later sections.

We let

$\mathbb{Z}$: the set of integers (a group under + and a ring)
$\mathbb{Q}$: the set of rational numbers (a group under + and a field)
$\mathbb{R}$: the set of real numbers (a group under + and a field)
$\mathbb{C}$: the set of complex numbers (a group under + and a field)
$\mathbb{Q}^\times$: $\{a \in \mathbb{Q} \mid a \neq 0\}$ (a group under multiplication)
$\mathbb{R}^\times$: $\{a \in \mathbb{R} \mid a \neq 0\}$ (a group under multiplication)

$\mathbb{C}^\times$: $\{a \in \mathbb{C} \mid a \neq 0\}$ (a group under multiplication)
$\mathbb{Z}_n$: integers modulo n (a group under $+$ and a ring)
$\mathbb{N}$: $\{a \in \mathbb{Z} \mid a \geq 0\}$

A superscript of $+$ means we want the positive elements, so

$$\mathbb{Z}^+ = \{a \in \mathbb{Z} \mid a > 0\},$$

and similarly for $\mathbb{Q}^+$ and $\mathbb{R}^+$.

If we have a set R and positive integer $n \in \mathbb{Z}^+$, then we let

$$M_n(R) = \{n \times n \text{ matrices with entries from } R\}.$$

We will only use this when R is a ring, specifically $R = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_n$, or $\mathbb{Z}$. In each case, we are also interested in the group

$$\mathrm{GL}_n(R) = \{A \in M_n(R) \mid \det(A) \in R^\times\}.$$

For this definition, $\mathbb{Z}_n^\times$ is defined in Section 1.3 below; $\mathbb{Z}^\times = \{-1, 1\}$.

1.2. **Functions.** If we have a function $f : A \to B$, then we assume f is defined for every element of A, so A is the domain of f. We refer to B as the codomain of f, as opposed to its image:

$$\mathrm{Im}(f) = f(A) = \{f(a) \mid a \in A\} \subseteq B$$

1.3. $\mathbb{Z}_n$**.** An essential construction for us is $\mathbb{Z}_n$. There are three ways of viewing it. First, we fix $n \in \mathbb{Z}^+$.

First, we can think of integers up to congruences. If $a, b \in \mathbb{Z}$, we define

$$a \equiv b \pmod{n} \iff n \mid b - a.$$

Here, we are dealing with integers, but only think of them as different if they are not congruent modulo n. Every integer is congruent to its remainder on division by n, and no two remainders from $\{0, \ldots, n-1\}$ are congruent modulo n, so we have n things (see Section 17.2 for more on remainders and the Division algorithm).

Building on this idea gives the second point of view, namely that $\mathbb{Z}_n = \{0, \ldots, n-1\}$, and when we perform operations, we always replace the result with its remainder on division by n. This is very concrete and well-suited for implimentation on a computer, but is less elegant mathematically. To assist in working with this version, we define

$$a \bmod n = \text{ the remainder when } a \text{ is divided by } n.$$

This is the unique integer r such that $0 \leq r < n$ and $a = nq + r$ for some integer q.

The third approach also builds on the first. One can show that congruence modulo n is an equivalence relation on $\mathbb{Z}$, in which case we have equivalence classes:

$$[a]_n = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}.$$

From the comments above, we again get a set with n things, namely $\{[0]_n, [1]_n, \ldots, [n-1]_n\}$, but with the classes, $[0]_n = [n]_n$, and $[5]_n = [n+5]_n = [-n+5]_n$.

We can sum up the connections between these points of view as follows. If $n \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$

Classes		Relation		Remainders
$[a]_n = [b]_n$	$\iff$	$a \equiv b \pmod{n}$	$\iff$	$(a \bmod n) = (b \bmod n)$

In all cases, we want to be able to add and multiply elements of $\mathbb{Z}_n$. From the point of view of congruences, this says that we can replace one integer with another it is congruent to when performing addition or multiplication.

Proposition 1.1. *Let $n \in \mathbb{Z}^+$, $a, b, c, d \in \mathbb{Z}$ with*

$$a \equiv b \pmod{n} \quad \textit{and} \quad c \equiv d \pmod{n}.$$

Then,

(1) $a + c \equiv b + d \pmod{n}$
(2) $ac \equiv bd \pmod{n}$
(3) $a - c \equiv b - d \pmod{n}$

We leave the proofs as exercises to the reader. Note, the final part can be deduced from the first two since $a - c = a + (-1) \cdot c$.

Exercise 1: Prove Proposition 1.1.

The corresponding statement in terms of congruence classes looks like this:

Corollary 1.2. *Let $n \in \mathbb{Z}^+$, $a, b, c, d \in \mathbb{Z}$ with*

$$[a]_n = [b]_n \quad \textit{and} \quad [c]_n = [d]_n.$$

Then

(1) $[a + c]_n = [b + d]_n$
(2) $[ac]_n = [bd]_n$
(3) $[a - c]_n = [b - d]_n$

Phrased in this way, it shows that addition, multiplication, and subtraction of congruence classes is well-defined. That is, the operations can be computed by chosing elements from the classes, and the final result does not depend on the choices.

Using $\mathbb{Z}_n = \{0, \ldots, n-1\}$, we can write down complete addition and multiplication tables for small n. For example, here are the operation tables for $\mathbb{Z}_4$.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

We consider another instance of something being *well-defined*. If $[a]_n \in \mathbb{Z}_n$, then we would like to define $\gcd([a]_n, n)$ to be simply $\gcd(a, n)$. Since it is possible for a single congruence class to be represented by many different integers, we have to prove that the final result does not depend on this choice.

Proposition 1.3. *If $n \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$ with $[a]_n = [b]_n$, then $\gcd(a, n) = \gcd(b, n)$.*

Proof. Since $[a]_n = [b]_n$, $a \equiv b \pmod{n}$, which implies that

$$a = b + nk \tag{1}$$

for some $k \in \mathbb{Z}$. Since $\gcd(b, n) \mid b$ and $\gcd(b, n) \mid n$, we get from equation 1 that $\gcd(b, n) \mid a$. Since $\gcd(b, n) \mid n$ as well, we get $\gcd(b, n) \leq \gcd(a, n)$.

We can also solve equation 1 for b: $b = a + n(-k)$. Repeating the same argument with the roles of a and b reversed gives $\gcd(a, n) \leq \gcd(b, n)$. Together with the first part, we get $\gcd(a, n) = \gcd(b, n)$. □

Example. To see an example where something is *not* well-defined, supposed we wanted to define $\gcd([a]_n, [b]_n)$ to be $\gcd(a, b)$. This will not work in general; here is a counterexample. Let $n = 3$, $a = b = 1$. Then $\gcd(a, b) = \gcd(1, 1) = 1$. But, $[1]_3 = [4]_3$. On one hand, we would have $\gcd([1]_3, [1]_3) = 1$, and on the other hand $\gcd([1]_3, [1]_3) = \gcd([4]_3, [4]_3) = \gcd(4, 4) = 4$. The result depends on what integers we pick for representing the congruence classes.

By Proposition 1.3, we can define

$$\mathbb{Z}_n^\times = \{[a]_n \in \mathbb{Z}_n \mid \gcd(a, n) = 1\},$$

and define the Euler phi-function for $n \in \mathbb{Z}^+$:

$$\varphi(n) = |\mathbb{Z}_n^\times|.$$

Note, although $\mathbb{Z}_1 = [0]_1$ has only one element, $\gcd(0, 1) = 1$ so $\mathbb{Z}_1^\times = \{[0_1]\} = \{[1]_1\}$, giving $\varphi(1) = 1$.

2. Groups

Here we introduce definitions and some notions from group theory. As we will see, they apply to crytography in many situations and can unify ideas applied in different places.

We start with something more basic, the notion of a binary operation which is central to the definition of group.

2.1. **Binary operations.**

Definition 2.1. A binary operation $*$ on a set S is a function

$$* : S \times S \to S.$$

We write $a*b$ for the value of this function on the ordered pair $(a, b) \in S$.

Note:

- by saying that $*$ is a function, it implies that $a * b$ is defined for every pair of elements $a, b \in S$.
- The codomain is S, so always $a * b \in S$.

Example. Three familiar examples are given by addition, subtraction, and multiplication on $\mathbb{Z}$.

Example. Similarly, addition, subtraction, and multiplication are each binary operations on $\mathbb{R}$, but division is not a binary operation since $5 \div 0$ is not defined as a real number.

Example. On the other hand, division is a binary operation on $\mathbb{R}^\times$.

There are several properties of interest which a binary operation may satisfy.

Definition 2.2. Let $*$ be a binary operation on a set S.

- $*$ is associative if for all $a, b, c \in S$,
$$a * (b * c) = (a * b) * c.$$
- $*$ is commutative if for all $a, b \in S$,
$$a * b = b * a.$$
- $*$ has identity e if $e \in S$ and for all $a \in S$,
$$a * e = e * a = a.$$

Example. Addition and multiplication on $\mathbb{Z}$ are both commutative, associative, and have identity (0 for addition and 1 for multiplication). Note, subtraction is neither commutative ($3-5 \neq 5-3$) nor associative ($1 - (2 - 3) \neq (1 - 2) - 3$), and does not have an identity element.

Exercise 2: Prove that $\mathbb{Z}$ does not have an identity element under subtraction.

Our first proposition shows that if there is an identity element for a binary operation, then it is unique.

Proposition 2.3. *If $*$ is a binary operation on a set S, then there is at most one identity element for $*$.*

Proof. Suppose to contrary that e and e' are both identity elements for $*$ on S. Then

$$e * e' = e \text{ since } e' \text{ is an identity element, and}$$
$$e * e' = e' \text{ since } e \text{ is an identity element.}$$

Thus $e = e'$. □

We have one more definition.

Definition 2.4. Let $*$ be a binary operation on a set S which has identity e. If $a \in S$, we say that $b \in S$ is an inverse of a if

$$a * b = b * a = e.$$

When an inverse exists, it is unique.

Proposition 2.5. *Let $*$ be an associative binary operation on a set S which has identity e, and $a \in S$. Then a has at most one inverse in S.*

Proof. Suppose b and c are both inverses of a. Then

$$b * (a * c) = b * e = b$$

and

$$(b * a) * c = e * c = c.$$

Since the operation is associative, $b * (a * c) = (b * a) * c$, so $b = c$. □

Example. In $\mathbb{Z}$ under addition where 0 is the identity, every integer $n \in \mathbb{Z}$ has an inverse $-n$ because $n + (-n) = 0 = (-n) + n$. On the other hand, for $\mathbb{Z}$ under multiplication (where 1 is the identity), the only elements with inverses are 1 and -1 (because $1 \cdot 1 = 1$ and $(-1) \cdot (-1) = 1$).

Notation. In almost every binary operation we encounter, it will already be naturally an addition or a multiplication. Addition in every case will be commutative, and we will only use $+$ for binary operations which are commutative. In these cases, the inverse of a will be denoted by $-a$.

In other cases, we will generally use $\cdot$ instead of $*$ for the operation, or use no symbol at all for the operation and just write ab for $a * b$. In

these cases, we are not assuming the operation is commutative unless it is explicitly mentioned. The inverse of an element a (if it exists) is then denoted by a^{-1}.

2.2. **Definition of group.**

Definition 2.6. A group is a set G with a binary operation $*$ such that

(1) $*$ is associative
(2) G has an identity element for $*$
(3) every element of G has an inverse.

Example. Addition is a group operation on many familiar sets: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Note, $\mathbb{Z}^+$ is not a group for addition because it does not have an identity element. Similarly, $\mathbb{N}$ is not a group for addition because it contains elements which do not have inverses (such as 3, or 5, or any positive integer).

Example. Multiplication is a group operation on other familiar sets: $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$, and $\mathbb{R}^+$.

Remark. From Propositions 2.3 and 2.5, we know that the identity element of a group is unique and that each element has a unique inverse.

Definition 2.7. A group G is abelian if the operation is commutative.

It might seem more natural to call these groups commutative groups, but the terminology is universally accepted in mathematics[1]. The additive and multiplicative groups given above are all abelian. Here is an example which is not.

Example. Let $G = \mathrm{GL}_2(\mathbb{R})$, the set of 2×2 matrices over the real numbers non-zero determinant. This is a group under matrix multiplication with identity being the 2×2 identity matrix and inverses being inverse matrices (using that for 2×2 matrices over $\mathbb{R}$, a matrix has an inverse if and only if it has non-zero determinant). However, this group is not commutative.

3. Subgroups

We often have groups which are subsets of bigger groups. Suppose G is a group and $H \subseteq G$. If we restrict the domain of the binary operation from $G \times G$ to $H \times H$, and then want the results to always lie in H. In other words, for all a, b,

$$a, b \in H \implies a * b \in H.$$

[1]The term *abelian comes from the name of a mathematician, Abel.*

When this happens, we say that H is closed under $*$.

Definition 3.1. If G is a group with operation $*$ and $H \subseteq G$, then we say that H is a subgroup of G if

(1) H is closed under $*$,
(2) the identity element e for G is in H,
(3) for all $a \in H$, its inverse (in G) is contained in H.

One could say that a subset is a subgroup if it is closed under the binary operation, contains the identity, and is closed under inverses.

Our definition is not an literal match to the concept (subset which is also a subgroup). The missing steps are explored in the exercises.

Example. Addition is a binary operation on $\mathbb{R}$. If we restrict to rational numbers $a, b \in \mathbb{Q}$, then $a + b \in \mathbb{Q}$, so $\mathbb{Q}$ is closed for $+$.

Example. On the other hand, division is a binary operation on $\mathbb{Q}^+$, the set positive rational numbers. However, if we try to restrict to positive integers $a, b \in \mathbb{Z}^+$, then $a \div b$ is a positive rational number, but it need not be a positive integer. For example, $3 \div 7 \notin \mathbb{Z}^+$. So $\mathbb{Z}^+$ is not closed under division.

The first problem makes it easier to prove that an element of a group is the identity element.

Exercise 3: Let G be a group with identity e. Then $c * c = c$ if and only if $c = e$.

Exercise 4: We would like to define subgroup as follows: "If G is a group and $H \subseteq G$, then H is a *subgroup* of G if the binary operation for G induces a binary operation on H and H is a group for that operation." A subset which is a subgroup under our definition definitely satisfies this definition as well. To show the implication goes both ways, prove that if H satisfies the quoted statement, then

(1) H is closed for $*$,
(2) $e_G = e_H$ (hint, use problem 3)
(3) for all $a \in H$, the inverse of a in G is in H.

4. Groups acting on sets

Groups are fun, but they are much more fun when they are doing something, like acting on a set.

Definition 4.1. Let G be a group and S a set. An action of G on S is a function

$$\cdot : G \times S \to S$$

such that

(1) for all $s \in S$, $e \cdot s = s$ where e is the identity of G;
(2) for all $g_1, g_2 \in G$ and all $s \in S$, $g_1 \cdot (g_2 \cdot s) = (g_1 g_2) \cdot s$.

In the second condition, both dots on the left hand side represent the action where as $g_1 g_2$ on the right hand side is multiplication within the group.

We will see several examples of group actions in the next section where they have applications to cryptography, so we just give two quick ones now.

Example. The group $G = \mathbb{Z}$ acts on $S = \mathbb{R}$ by $n \cdot a = n + a$. In other words, we use addition to define the action.

Exercise 5: Prove that the action of $\mathbb{Z}$ on $\mathbb{R}$ given by $n \cdot a = n + a$ is a group action.

Example. If G is a group, define an action of G on G by $g \cdot a = ga$. In other words, we use the group operation to define the action. This particular action is famous and is known as left translation.

Exercise 6: Prove that if G is a group, then left translation gives a group action.

5. Cryptosystems from group actions

For background and notation for cryptosystems, see Section 18.

Suppose G is a group which acts on a set A, and we find a way to match elements of A with the plaintexts. Then we will let A also be the set of ciphertexts, and G is the set of keys. Given a key $k \in G$ and a plaintext $P \in A$, our encryption function is

$$e_k(P) = k \cdot P$$

where the right hand side comes from the group action. The decryption function uses the inverse of k in the group:

$$d_k(C) = k^{-1} \cdot P$$

To check that this works, we compute:

$$\begin{aligned} d_k(e_k(P)) &= d_k(k \cdot P) \\ &= k^{-1} \cdot (k \cdot P) \\ &= (k^{-1}k) \cdot P && \text{property 2 of group action} \\ &= e \cdot P \\ &= P && \text{property 1 of group action} \end{aligned}$$

We now consider some classic ciphers, and see how they are examples of this one idea.

5.1. **Shift Cipher.** For the shift cipher, $\mathcal{P} = \mathcal{C} = \mathcal{A} = \mathcal{K} = \mathbb{Z}_n = G$. We let G act on itself by left translation, so for a key $k \in G$, our encryption is given by

$$e_k(p) = p + k$$

where the addition is taken modulo n since we are working in $\mathbb{Z}_n$. Decryption is simply

$$d_k(c) = c - k.$$

5.2. **Affine Cipher.** For the affine cipher, we let $\mathcal{A} = \mathcal{P} = \mathcal{C} = \mathbb{Z}_n$. Our group is the affine group modulo n:

$$\mathit{Aff}(n) = \{ax + b \mid a \in \mathbb{Z}_n^\times \text{ and } b \in \mathbb{Z}_n\}$$

where the operation is composition.

Exercise 7: Verify that if $n \in \mathbb{Z}^+$, then $\mathit{Aff}(n)$ is a group.

If $ax + b \in \mathcal{K} = \mathit{Aff}(n)$, then $ax + b$ acts on $m \in \mathbb{Z}_n$ by

$$(ax + b) \cdot m = am + b$$

with the computation done modulo n. This gives encryption functions

$$e_{ax+b}(p) = ap + b.$$

Since $a \in \mathbb{Z}_n^\times$, there exists $a' \in \mathbb{Z}_n^\times$ such that $aa' \equiv 1 \pmod{n}$. Then

$$d_{ax+b}(c) = a'(c - b).$$

5.3. **Hill Cipher.** For the Hill cipher, we let $\mathcal{A} = \mathbb{Z}_n$ and pick $m \in \mathbb{Z}^+$. Then we take $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n^m$. The group

$$G = \mathrm{GL}_m(\mathbb{Z}_n) = \{A \in M_m(\mathbb{Z}_n) \mid \det(A) \in \mathbb{Z}_n^\times\}$$

is the group of matrices over $\mathbb{Z}_n$ which are invertible for matrix multplication. It acts on $\mathbb{Z}_n^m$ in the usual way of matrix times vector.

If $A \in \mathcal{K} = \mathrm{GL}_m(\mathbb{Z}_n)$ and $\vec{p} \in \mathbb{Z}_n^m$, then encryption is

$$e_A(\vec{p}) = A\vec{p}$$

and decryption is

$$d_A(\vec{c}) = A^{-1}\vec{c},$$

where A^{-1} is the inverse of A modulo n.

5.4. **Permutation Cipher.** Let $n \in \mathbb{Z}^+$. A permutation on a set A is a bijective function $f : A \to A$. The symmetric group on A is

$$S_A = \{f : A \to A \mid f \text{ is a permutation}\}.$$

This is a group under composition:

- the composition of bijective functions is bijective
- function composition is always associative
- the identity function $I_A : A \to A$ given by $I_A(a) = a$ for all $a \in A$ acts as the identity under composition
- bijective functions have inverse functions (which are also bijective)

For any set A, S_A acts on A by $f \cdot a = f(a)$ for any $f \in S_A$ and any $a \in A$.

In the special case of $A = \{1, \ldots, n\}$, we write S_n for the set of permutations. Then S_n acts on n tuples from another set B by

$$\sigma \cdot (b_1, \ldots, b_m) = (b_{\sigma(1)}, \ldots, b_{\sigma(n)}).$$

So, we fix n and take $\mathcal{A}^n = \mathcal{P} = \mathcal{C}$ and $\mathcal{K} = S_n$. If $\sigma \in S_n$, encoding is given by

$$e_\sigma(a_1, \ldots, a_n) = (a_{\sigma(1)}, \ldots, a_{\sigma(n)})$$

and decoding by

$$d_\sigma(a_1, \ldots, a_n) = (a_{\sigma^{-1}(1)}, \ldots, a_{\sigma^{-1}(n)}).$$

5.5. **Substitution Cipher.** If $\mathcal{A}$ is our alphabet, we let $\mathcal{P} = \mathcal{C} = \mathcal{A}$ and key space $\mathcal{K} = S_{\mathcal{A}}$. Then for any $f \in S_{\mathcal{A}}$, we encrypt and decrypt by

$$e_f(p) = f(p) \quad \text{and} \quad d_f(c) = f^{-1}(c).$$

Many other ciphers are special cases of the substitution cipher, such as shift, affine, and RSA. If $n = |\mathcal{A}|$, then the size of the key space is $n!$, which grows very quickly. This means that to communicate a key with large n, one must transmit many bits. The more specialized ciphers have smaller key spaces, and hence, transmitting the key is easier. If $\mathcal{A}$ is an ordinary alphabet from a natural language, then this cipher can be readily attacked with frequency analysis.

5.6. **Vigenère Cipher.** We first introduce a way to construct new groups from others which we will need later.

If G_1 and G_2 are groups with operations $*_1$ and $*_2$, then we can make $G_1 \times G_2$ into a group with the operation

$$(a_1, a_2) * (b_1, b_2) = (a_1 *_1 b_2, a_2 *_2 b_2)$$

It has identity (e_1, e_2) and the inverse of an element (a_1, a_2) is (a_1^{-1}, a_2^{-2}) where the inverses are computed in G_1 and G_2 respectively. The resulting group is called the *direct product* of G_1 and G_2, and is denoted $G_1 \times G_2$. In some cases, it may also be denoted by $G_1 \oplus G_2$.

This construction can be iterated with a list of groups $G_1, \ldots, G_n$. The elements then are n-tuples where the ith coordinate comes from G_i.

For a Vigenère cipher, we take m to be a positive integer, and let $\mathcal{P} = \mathcal{C} = \mathcal{A}^m$. Let $n = |\mathcal{A}|$ and identify $\mathcal{A}$ with $\mathbb{Z}_n$. Our group is $G = \mathbb{Z}_n \times \mathbb{Z}_n \times \cdots \times \mathbb{Z}_n$ where we use m copies of $\mathbb{Z}_n$. So a key is an m-tuple of elements of $\mathcal{A}$, i.e., an m-letter word. The group action is G acting on itself by left translation.

5.7. **RSA.** The main feature of RSA is that it is a public key cryptosystem. But under the hood, it works on the same principle of groups acting on sets.

Let N be a positive integer which is a product of distinct primes. We let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_N$. The traditional choice for the group is $G = \mathcal{K} = \mathbb{Z}_{\varphi(N)}^{\times}$. It acts on $\mathbb{Z}_N$ as follows

$$\begin{aligned} \mathbb{Z}_{\varphi(N)}^{\times} \times \mathbb{Z}_N &\to \mathbb{Z}_N \\ (a, b) &\mapsto b^a \end{aligned}$$

For encryption, we pick a key a such that $\gcd(a, \varphi(N)) = 1$, i.e., such that $a \in \mathbb{Z}_{\varphi(N)}$ and then

$$e_a(m) = m^a \bmod N.$$

For decryption, we find b such that $ab \equiv 1 \pmod{\varphi(N)}$, but this is just $a^{-1} \in \mathbb{Z}_{\varphi(N)}^{\times}$ and

$$d_a(c) = c^b \bmod N.$$

It may be hard to see why we take the hypothesis that the prime factors of N must be distinct. We illustrate the problem with an example.

Example. Let $N = 9 = 3^2$, so $\varphi(N) = 6$. Then $1 \equiv 7 \pmod{\varphi(N)}$ and certainly $\gcd(1, 6) = 1$, so $1 \in \mathbb{Z}_6^{\times}$. If we compute the group action with 1 and $3 \in \mathbb{Z}_9$, we get $3^1 = 3$, but if we use 7, we get $3^7 \equiv 0 \pmod 9$, a different result. This is not a group action because the "action" needs to be a function, and it is not well-defined.

Exercise 8: Suppose N is a product of distinct primes and $m = \varphi(N)$. Prove that if $[a]_m = [b]_m \in \mathbb{Z}_m$ and $[c]_N \in \mathbb{Z}_N$, then $[c^a]_N = [c^b]_N$.

5.8. **LFSRs.** For background on LFSRs, see Chapter 20.

If an n-stage LFSR has associated matrix $C \in \mathrm{GL}_n(\mathbb{Z}_2)$, then groups enter directly since the order of C in the group $\mathrm{GL}_n(\mathbb{Z}_2)$ gives the longest period one can achieve from the LFSR.

In general, if a group G acts on a set S, we can make a stream cipher with one more ingredient, a function $f : S \to \{0, 1\}$. Then we choose an element $g \in G$ and an initial element $s_0 \in S$. We construct a sequence of elements of S, and the corresponding stream of $x_i \in \{0, 1\}$ via

$$s_n = g \cdot s_{n-1} \qquad x_n = f(s_n).$$

In the case of an LFSR, the group is $\mathrm{GL}_n(\mathbb{Z}_2)$, the set $S = \mathbb{Z}_2^n$, and the action is the usual matrix times vector giving vector. Then $g = C$, the matrix associated to the LFSR, and $s_0 \in \mathbb{Z}_2^n$ is the initial load of the LFSR. The function f is given by $f(a_1, \ldots, a_n) = a_n$.

5.9. **Pseudo-random number generators.** It is worth noting that a small generalization of this construction produces another important object in cryptography. Many aspects of cryptography make use of random number numbers. Often times, these need not be truely random, and a computer language's random number generator is good enough. These are not random; they are completely determined by the algorithm used and an initial seed.

A commonly used pseudo-random number generator is a *linear congruenential generator*. Suppose you want pseudo-random numbers in $\mathbb{Z}_{2^k}$. Then pick a large positive integer $m > 2^k$, $a \in \mathbb{Z}_m^\times$, and $b \in \mathbb{Z}_m$. Starting with an initial seed $s_0 \in \mathbb{Z}_m$, we construct the sequence defined recursively by $s_n = as_{n-1} + b \bmod m$. The random numbers are then given by something like taking the top k-bits of s_n, i.e., it uses a function $f : \mathbb{Z}_m \to \mathbb{Z}_{2^k}$ which extracts k bits.

This fits our setup for a stream cipher from a group action where

$$G = \mathit{Aff}(m) = \{ax + b \mid a \in \mathbb{Z}_m^\times \text{ and } b \in \mathbb{Z}_m\}$$

and $S = \mathbb{Z}_m$ (the action given by plugging a value into the linear polynomial). The only difference is the codomain of the function f. In a stream cipher, it would be a function $f : S \to \mathbb{Z}_2$; for the random number generator, it is $f : S \to \mathbb{Z}_{2^k}$.

6. Isomorphisms and homomorphisms

Consider the following two operation tables for $\{1, -1\}$ under multiplication and $\mathbb{Z}_2$:

$\cdot$	1	-1
1	1	-1
-1	-1	1

$+$	0	1
0	0	1
1	1	0

Then we can get from the table on the left to the table on the right by simply renaming elements systematically. In particular, if we take the table on the left and use the following replacements:

$$1 \mapsto 0$$
$$-1 \mapsto 1$$

This is the idea of an isomorphism. Renaming elements from one set to elements of another is formalized as a bijective function between the sets $f : G_1 \to G_2$. The idea that the group tables match up can be thought of elements $a \in G_1$ have their old name, $a \in G_1$, and a new name $f(a) \in G_2$. Then the group tables matching after renaming amounts to,

> if we take any two elements of G_1, multiply in G_1, and then rename the result, it is the same as first renaming the elements and then multiplying them in G_2.

Formally, this leads to

Definition 6.1. If G_1 is a group with operation $*$ and G_2 is a group with operation $*'$, then an isomorphism from G_1 to G_2 is a bijective function

$$f : G_1 \to G_2$$

such that

$$f(a * b) = f(a) *' f(b) \qquad \text{for all } a, b \in H.$$

We then say that G_1 and G_2 are *isomorphic* and write $G_1 \cong G_2$.

The idea of "same except for renaming of elements" should behave like an equivalence relation. The formal proof of this is left as a sequence of exercises.

Exercise 9: Prove that every group is isomorphic to itself. (Hint: for any set G, there is a simple bijective function $G \to G$.)

Exercise 10: Suppose G_1 is isomorphic to G_2. Prove that G_2 is isomorphic to G_1. (Hint: the hypothesis gives you a bijective function

$G_1 \to G_2$; you need to start by constructing a bijective function $G_2 \to G_1$.

Exercise 11: Suppose G_1 is isomorphic to G_2 and G_2 is isomorphic to G_3. Prove G_1 is isomorphic to G_3.

Here is an example of an isomorphism from familiar objects.

Exercise 12: Prove that the group $\mathbb{R}$ under addition is isomorphic to the group $\mathbb{R}^+$ under multiplication. (Hint: try an exponential map.)

It is useful to consider functions between groups which respect the operations, but are not necessarily bijective:

Definition 6.2. If H is a group with operation $*$ and K is a group with operation $*'$, then a function

$$f : H \to K$$

such that

$$f(a * b) = f(a) *' f(b) \qquad \text{for all } a, b \in H$$

is called a homomorphism from H to K.

Example. The inclusion map $i : \mathbb{Z} \to \mathbb{Q}$ (defined by $i(n) = n$ for all integers n) is a homomorphism which is 1-1, but not onto.

Example. If n is a positive integer, the map $f : \mathbb{Z} \to \mathbb{Z}_n$ given by

$$f(a) = \text{ the congruence class of } a \text{ modulo } n$$

is a homomorphism called the reduction map. It is onto, but not 1-1.

Example. If H and K are any two groups, the constant function $f : H \to K$ given by $f(a) = e_K$ for all $a \in H$ is a homomorphism, called the trivial map. If H and K have more than one element each, it is neither 1-1 nor onto.

We collect the basic properties of homomorphisms in the next proposition.

Proposition 6.3. *If $f : H \to K$ is a group homomorphism, then*

(1) $f(e_H) = e_K$
(2) *for all $h \in H$, $f(h^{-1}) = f(h)^{-1}$*

Proof. We start by noting that $f(e_H) = f(e_H * e_H) = f(e_H)f(e_H)$, so $f(e_H) = e_K$ by exercise 3.

Let $h \in H$. We prove the second part by showing $f(h^{-1})$ does the job of an inverse. So we compute

$$f(h)f(h^{-1}) = f(hh^{-1}) = f(e_H) = e_K$$

and

$$f(h^{-1})f(h) = f(h^{-1}h) = f(e_H) = e_K\,.$$

So, $f(h^{-1}) = f(h)^{-1}$. □

Example. In linear algebra, one considers vector spaces and linear transformations between them. According to the definitions, every vector space is an abelian group for $+$, and every linear transformation is a homomorphism.

An important construction for homomorphsims is its kernel. In the linear algebra situation, this is the same as the kernel, which is also called the null space.

Definition 6.4. If $f : G \to K$ is a group homomorphism, the kernel of f is

$$\ker(f) = \{g \in G \mid f(g) = e_K\}.$$

Exercise 13: Suppose $f : G \to K$ is a homomorphism. Prove $\ker(f)$ is a subgroup of G.

An important family of examples of homomorphisms applies to any abelian group.

Example. Suppose G is an abelian group and $m \in \mathbb{Z}$. Then the *multiplication by m map* in additive notation is defined by

$$\begin{aligned}[m] : G &\to G\\ g &\mapsto mg\end{aligned}$$

If we are using multiplicative notation, $[m](g) = g^m$. This is a homomorphism whenever G is abelian.

Our main interest is the case when $m \in \mathbb{Z}^+$.

Exercise 14: Suppose G is an abelian group written multiplicatively and $m \in \mathbb{Z}^+$. Prove that the multiplication by m map is a homomorphism from G to G.

Note, if $m = 0$, then $[0](g) = g^0 = e$ for all $g \in G$. In other words, $[0]$ is the trivial map from G to G.

6.1. **Applications to $\mathbb{Z}_n$.** The multiplication by m map applies to all abelian groups. Since all finite abelian groups are built from cyclic groups, it helps to understand this map on $\mathbb{Z}_n$ in detail. Ultimately, this comes down to statements about congruences. We determine the kernel here, and study the image in Section 8.1.

Proposition 6.5. *If $n \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ and $d = \gcd(a, n)$, then for all $x \in \mathbb{Z}$,*

$$ax \equiv 0 \pmod{n} \iff dx \equiv 0 \pmod{n}.$$

Proof. ($\Rightarrow$) Suppose $ax \equiv 0 \pmod{n}$. By the Bezout property 17.4, there exists $r, s \in \mathbb{Z}$ such that $ra + sn = d$. Then

$$dx \equiv (ra + sn)x \equiv r(ax) + n(sx) \equiv r \cdot 0 + 0 \cdot (sx) \equiv 0 \pmod{n}.$$

($\Leftarrow$) Suppose $dx \equiv 0 \pmod{n}$. Since $d = \gcd(a, n)$, $a = dk$ for some integer k. Then

$$ax \equiv (dk)x \equiv k(dx) \equiv k \cdot 0 \equiv 0 \pmod{n}.$$

□

Corollary 6.6. *If $n \in \mathbb{Z}^+$, $m \in \mathbb{Z}$, and $d = \gcd(n, m)$, then as homomorphisms from $\mathbb{Z}_n$ to itself,* $\ker([m]) = \ker([d])$.

7. Cyclic groups

If G is a group and $g \in G$, then we use notation familiar notation for repeating the operation. For example,

$$g^2 = gg$$
$$g^3 = ggg$$

Working backwards, we also want $g^1 = g$, $g^0 = e$, g^{-1} to be the inverse of g (which is already our notation).

Definition 7.1. Let G be a group and $g \in G$. Then the cyclic subgroup generated by g is

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}.$$

If the group uses additive notation, then

$$\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}.$$

In either case, we should justify the name.

Proposition 7.2. *Let G be a group and $g \in G$. Then $\langle g \rangle$ is a subgroup of G.*

Proof. First note that $e = g^0 \in \langle g \rangle$, and if $g^n \in \langle g \rangle$, then $(g^n)^{-1} = g^{-n} \in \langle g \rangle$. Finally, if $g^n, g^m \in \langle g \rangle$, then $g^n \cdot g^m = g^{n+m} \in \langle g \rangle$. So, $\langle g \rangle$ is a subgroup of G. □

8. Order and torsion

Here we introduce two closely related notions for elements of a group, *order* and *torsion*.

Definition 8.1. If G is a group, $g \in G$, and $n \in \mathbb{Z}^+$, then we say that g *is n-torsion* if $g^n = e$.

In additive notation, g is n-torsion if $n \cdot g = 0$.

Definition 8.2. Let G be a group and $g \in G$.

(1) If $g^n \neq e$ for all $n \in \mathbb{Z}^+$, we say that g has *infinite order*.
(2) Otherwise, the *order of* g is the smallest positive integer n such that $g^n = e$.

In either case, we denote the order of g by $|g|$.

Example. In $\mathbb{C}^\times$, i (a root of $x^2 + 1$) satisfies $i^4 = 1$, but i, $i^2 = -1$, $i^3 = -i$ are all not equal to 1, so i has order 4. As far as torsion goes, we have $i^4 = i^8 = i^{12} = 1$, so i is 4-torsion, and also 8-torsion, and 12-torsion, and so on.

In this example, we can see a general phenominon, namely that an element of a group has only one order, but it can be m-torsion for many values of m.

Example. For $2 \in \mathbb{R}^\times$, $2^n \neq 1$ for any $n \in \mathbb{Z}^+$, so it is an element of infinite order. It is not n-torsion for any n.

We will see soon than an element in a finite group always has finite order, so that will be the case in which we are most interested.

Theorem 8.3. *Let G be a group and $g \in G$.*

(1) *If g has infinite order, then all g^i are distinct for $i \in \mathbb{Z}$. Moreover, $\mathbb{Z} \cong \langle g \rangle$ by the map $i \mapsto g^i$.*
(2) *If g has finite order n, then*
   (a) *$\langle g \rangle = \{g^0, \ldots, g^{n-1}\}$ which has order n*
   (b) *if $i \in \mathbb{Z}$, then $g^i = g^{i \bmod n}$*
   (c) *for all $i, j \in \mathbb{Z}$,*

$$g^i = g^j \iff i \equiv j \pmod{n}$$

   (d) *for all $i \in \mathbb{Z}$,*

$$g^i = e \iff n \mid i$$

   (e) *$\mathbb{Z}_n \cong \langle g \rangle$ by the map $[i]_n \mapsto g^i$.*

Proof. We separate the two basic cases by a different criteria, but we will quickly see that they divide as described in the theorem.

First suppose g^i are distinct for all $i \in \mathbb{Z}$. Then clearly g has infinite order. The map $f : \mathbb{Z} \to \langle g \rangle$ given by $f(i) = g^i$ is then a bijection, and for all $i, j \in \mathbb{Z}$,

$$f(i+j) = g^{i+j} = g^i g^j = f(i)f(j).$$

Thus, f is an isomorphism.

On the other hand, if they are not all distinct, then $g^i = g^j$ for some $i < j$. Multiplying by g^{-i} we get $g^i g^{-i} = g^j g^{-i}$ which implies $e = g^0 = g^{j-i}$. In other words,

$$g^i = g^j \implies g^{j-i} = e \tag{2}$$

Since $i < j$, $j - i \in \mathbb{Z}^+$, so g has finite order. Let $n = |g|$.

If $i \in \mathbb{Z}$, then by the Division algorithm 17.2, there exists $q, r \in \mathbb{Z}$ such that $i = nq + r$, $0 \leq r < n$. Then

$$g^i = g^{nq+r} = (g^n)^q g^r = e^q \cdot g^r = g^r.$$

Since $r = i \bmod n$, this gives (b) and that $\langle g \rangle = \{g^0, \ldots, g^{n-1}\}$. To show that this set has order n, we need to show that $g^0, \ldots, g^{n-1}$ are distinct.

Suppose not. Then there exist $i, j \in \mathbb{Z}$ such that $g^i = g^j$ and $0 \leq i < j < n$. But by implication 2 above, this implies $g^{j-i} = e$. The inequalities on i and j imply $0 < j - i < n$, contradicting that n is the order of g. This completes the proof of (a).

For part (c), note

$$\begin{aligned} g^i = g^j &\iff g^{i \bmod n} = g^{j \bmod n} \\ &\iff i \bmod n = j \bmod n \quad \text{since these powers are distinct} \\ &\iff i \equiv j \pmod{n} \end{aligned}$$

Part (d) follows from (c) letting $j = 0$.

Finally, for part (e) we note that the given map, $f : \mathbb{Z}_n \to \langle g \rangle$ given by $f([i]_n) = g^i$ is a bijection from (c) and the fact that $[i]_n = [j]_n$ iff $i \equiv j \pmod{n}$. To see that it is a homomorphism, we check

$$f([i]_n + [j]_n) = f([i+j]_n) = g^{i+j} = g^i g^j = f([i]_n) f([j]_n).$$

□

Corollary 8.4. *If G is a group and $g \in G$, then the order of g equals the order of the cyclic subgroup $\langle g \rangle$.*

Theorem 8.3 establishes the connection between the order of an element and for which m it is m-torsion.

Corollary 8.5. *If G is a group and $g \in G$ has order n, then g is m-torsion iff $n \mid m$.*

One of the reasons m-torsion elements are useful to work with is that they have an algebraic structure when G is abelian.

Definition 8.6. Let G be an abelian group and $m \in \mathbb{Z}^+$. We let

$$G[m] = \{g \in G \mid g^m = e\}.$$

This is refered to as the *m-torsion subgroup* of G.

Before going any farther, we should justify the terminology.

Exercise 15: Prove that if G is an abelian group, then for every $m \in \mathbb{Z}^+$, $G[m]$ is a subgroup of G.

We note that for non-abelian groups, the corresponding sets do not have to be subgroups.

The m-torsion subgroup contains all of the m-torsion elements. Note, the analogous construction for elements of order m is not a subgroup (unless $m = 1$), since the identity element always has order 1 and a subgroup must contain the identity.

8.1. **Back to $\mathbb{Z}_n$.** Here we analyze orders of elements in $\mathbb{Z}_n$.

Proposition 8.7. *Let $n \in \mathbb{Z}^+$, $a \in \mathbb{Z}_n$, and $d = \gcd(a, n)$. Then*

$$\langle a \rangle = \langle d \rangle.$$

Proof. Since $d \mid a$, $a = dk$ for some $k \in \mathbb{Z}$. Then $a \in \langle d \rangle$, so $\langle a \rangle = \langle d \rangle$.

On the other hand, from the Extended Euclidean algorithm, we have $d = ra + sn$ for some $r, s \in \mathbb{Z}$. So,

$$d \equiv ra \pmod{n} \implies d \in \langle a \rangle \text{ in } \mathbb{Z}_n.$$

□

Proposition 8.8. *If $n, d \in \mathbb{Z}^+$ and $d \mid n$, then $|\langle d \rangle| = \frac{n}{d}$.*

Proof. First note that for $k \in \{1, 2, \ldots, \frac{n}{d} - 1\}$, $1 \leq kd < n$, so these elements are non-zero in $\mathbb{Z}_n$. However

$$\frac{n}{d} d = n \equiv 0 \pmod{n}.$$

So, $|d| = \frac{n}{d}$, which in turn implies $|\langle d \rangle| = \frac{n}{d}$. □

A consequence of this proof is that when $d \mid n$, in $\mathbb{Z}_n$ we have

$$\langle d \rangle = \left\{0, d, 2d, \ldots, \left(\frac{n}{d} - 1\right) \cdot d\right\}.$$

Corollary 8.9. *If $n \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ and $d = \gcd(n, a)$, then in $\mathbb{Z}_n$, $|a| = \frac{n}{d}$.*

Proof. Combining prior results, $|a| = |\langle a \rangle| = |\langle d \rangle| = \frac{n}{d}$. □

We can reframe some of these results as statements about congruences.

Corollary 8.10. *If $n \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$, then the congruence*

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

has a solution if and only if $\gcd(a, n) \mid b$.

Proof. The existence of a solution is equivalent to $b \in \langle a \rangle$ in $\mathbb{Z}_n$, but $\langle a \rangle = \langle \gcd(a, n) \rangle$. □

We can connect this with the multiplication by m-map, $[m]$ on $\mathbb{Z}_n$.

Proposition 8.11. *Suppose $m, n \in \mathbb{Z}^+$. Let $d = \gcd(m, n)$. Then the maps $[m]$ and $[d]$ have the same kernel, $\langle n/d \rangle$ which has order d, and the same image $\langle d \rangle$, which has order n/d.*

Proof. The image of $[m]$ is $\{k[m]_n \mid k \in \mathbb{Z}\} = \langle m \rangle$. By Proposition 8.7, $\mathrm{Im}([m]) = \mathrm{Im}([d])$, and we get its order from Corollary 8.9.

That $\ker([m]) = \ker([d])$ follows from Corollary 6.6.

Since $[d](n/d) = n \equiv 0 \pmod{n}$, clearly $\frac{n}{d} \in \ker([d])$, and so $\langle n/d \rangle \subseteq \ker([d])$. Conversely, if $a \in \ker([d])$, then $da \equiv 0 \pmod{n}$. So $n \mid da$, which implies $da = nk$ for some $k \in \mathbb{Z}$. Thus $a = \frac{n}{d}k$, which implies $a \in \langle n/d \rangle$. Thus, $\ker([d]) = \langle n/d \rangle$. The order of this subgroup is $n/(n/d) = d$ by Corollary 8.9. □

8.2. **Products.** As seen in the Section 5.6, if $G_1, \ldots, G_n$ are groups, then we can construct a new group with the set $G_1 \times \cdots \times G_n$ with operations done coordinatewise. These groups are especially important for us since elliptic curves give rise to finite abelian groups, which are classified by the following theorem, which says that every finite abelian group is isomorphic to a product of cyclic groups.

Theorem 8.12 (Classification of finite abelian groups)**.** *If A is a finite abelian group of order greater than 1, then there exists a unique list of integers $n_1, \ldots, n_k$ with $1 < n_1$, $n_i \mid n_{i+1}$ for all $1 \leq i < k$ such that*

$$A \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}.$$

From the Theorem 11.1 below, the Chinese Remainder Theorem, we have isomorphisms

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n \quad \text{when } \gcd(m, n) = 1.$$

This allows for an alternate statement of the theorem where each cyclic group in the direct product has prime power order. Both versions are useful at different times.

We will defer the proof of Theorem 8.12 to a group theory course. Nonetheless, it tells us that if we can count torsion elements in a direct product of groups, then we can handle any finite abelian group.

Suppose $(g_1, \ldots, g_k) \in G_1 \times \cdots \times G_k$. Since operations are done coordinatewise, if $j \in \mathbb{Z}^+$, then

$$(g_1, \ldots, g_k)^j = (g_1^j, \ldots, g_k^j).$$

Thus,

$$\begin{aligned}(g_1, \ldots, g_k) \text{ is } m\text{-torsion} &\iff (g_1, \ldots, g_k)^m = (e_1, \ldots, e_k) \\ &\iff (g_1^m, \ldots, g_k^m) = (e_1, \ldots, e_k) \\ &\iff g_i^m = e_i \text{ for all } i \\ &\iff m \text{ is a multiple of } |g_i| \text{ for all } i\end{aligned}$$

This is the main part of the proof of the following.

Proposition 8.13. *If $G_1, \ldots, G_n$ are groups and $(g_1, \ldots, g_k) \in G_1 \times \cdots \times G_k$, then*

1. *$(g_1, \ldots, g_k)$ has finite order if and only if g_i has finite order for all i*
2. *if $(g_1, \ldots, g_k)$ has finite order, then*

$$|(g_1, \ldots, g_k)| = \operatorname*{lcm}_{1 \le i \le k} |g_i|$$

If we have a product of abelian groups, $H \times K$ and $m \in \mathbb{Z}^+$, then loosely the kernel of $[m]$ on $H \times K$ is the direct product of the map on each factor, and similarly for the image. To make a formal statement, we will use $[m]_G$ to denote the multiplication by m map on G.

Proposition 8.14. *If H and K are abelian groups and $m \in \mathbb{Z}^+$, then*

$$\ker([m]_{H \times K}) = \ker([m]_H) \times \ker([m]_K)$$

and

$$\operatorname{Im}([m]_{H \times K}) = \operatorname{Im}([m]_H) \times \operatorname{Im}([m]_K).$$

By induction, this extends to a product of finitely many abelian groups.

Exercise 16: Prove Proposition 8.14.

9. Rings

The definition of a ring applies to a couple of constructs we will need, and acts as a stepping stone to fields. However, there are only a couple of examples which will be relevant.

Definition 9.1. A set R with two binary operations $+$ and $\cdot$ is a *ring* if

(1) R is an abelian group for $+$
(2) $\cdot$ is associative for R
(3) the left and right distributative laws hold for multiplication over addition, i.e., for all $a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ and } (b + c) \cdot a = b \cdot a + c \cdot a.$$

Remark. The order of operations in a ring are the same as in arithmetic: multiplication is done first, and then addition.

All of our rings will satisfy the next property.

Definition 9.2. A ring R is a ring with one if R has an identity for multiplication.

Most of the our rings satisfy the next condition as well.

Definition 9.3. A ring is a commutative ring if multiplication is commutative.

Example. The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all commutative rings with one with their usual addition and multiplication.

Example. If $m \in \mathbb{Z}^+$, then $\mathbb{Z}_m$ is a commutative ring with 1.

Remark. If a ring has one, then the identity element is unique by Proposition 2.3. We denote the identity for addition by 0_R, or just 0 for simplicity, and the identity for multiplication (for a ring with one) by 1_R, or just 1.

Example. Let $n \in \mathbb{Z}^+$, then the set of $n \times n$ matrices $M_n(\mathbb{R})$ is a ring with one (the identity matrix is the identity element for multiplication). Note, it is *not* a commutative ring if $n > 1$.

More generally, if R is a ring, then $M_n(R)$ is also a ring. When adding and multiplying matrices, we just need to know how to add and multiply their entries, and one can check that the properties in the definition holds. So, for $n \in \mathbb{Z}^+$, $M_n(\mathbb{Z})$, $M_n(\mathbb{Q})$, $M_n(\mathbb{C})$, and $M_n(\mathbb{Z}_m)$ are all rings.

We prove one proposition about rings.

Proposition 9.4. *If R is a ring, then for all $a \in R$,*

$$0 \cdot a = a \cdot 0 = 0.$$

We note that the proposition gives a property under multiplication for the identity for addition. The only part of the definition of the axiom of ring which involves both operations is the distributive law, so that plays a key role in the proof. Of course, we also need to use that 0 is the identity for $+$, which comes via $0 + 0 = 0$.

Proof. Let $a \in R$. Then

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$

Adding $-(a \cdot 0)$ to both sides then gives

$$\begin{aligned} -(a \cdot 0) + a \cdot 0 = -(a \cdot 0) + a \cdot 0 + a \cdot 0 &\implies 0 = 0 + a \cdot 0 \\ &\implies 0 = a \cdot 0 \end{aligned}$$

The proof that $0 = 0 \cdot a$ is similar and left to the reader. □

Exercise 17: Complete the proof of Proposition 9.4 by proving $0 = 0 \cdot a$.

Example. Let $R = \{0\}$ as a subset of $\mathbb{Z}$. We note that this one element set is a ring with the usual addition and multiplication. It is called the trivial ring, and has the peculiar property that $0_R = 1_R$.

Exercise 18: Suppose R is a ring with one where $0_R = 1_R$. Prove $R = \{0_R\}$, i.e., that R is a copy of the trivial ring.

9.1. **Units.** We start with a definition.

Definition 9.5. Let R be a ring with one. An element $a \in$ which has an inverse under multiplication is called a unit.

By Proposition 2.5, the multiplicative inverse of a unit is unique. It is not hard to prove that the set of units forms a group under multiplication. In fact, the main thing to prove is that the product of two units is a unit.

Exercise 19: Prove that if R is a ring with one, then $R^\times$ is a group under multiplication.

Example. Several groups under multiplication we have encountered before are special cases of this construction. For example $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$, and $\mathbb{Z}_n^\times$ are all examples.

Note, $R^\times$ need not be all non-zero elements, for example, as seen in the case of $\mathbb{Z}_n^\times$.

Example. In a matrix ring such as $M_n(\mathbb{R})$, we let $M_n(\mathbb{R})^\times = \mathrm{GL}_n(\mathbb{R})$. This is simply the invertible matrices. More generally, if R is a ring with one,

$$\mathrm{GL}_n(R) = M_n(R)^\times = \{A \in M_n(R) \mid \exists B \in M_n(R) \text{ s.t. } AB = BA = I_n\}.$$

The point is that the inverse has to be in $M_n(R)$ as well.

If R is a commutative ring with one, then we can use determinants since they only involve ring operations. Then a consequence of results from linear algebra is that

$$\mathrm{GL}_n(R) = \{A \in M_n(R) \mid \det(A) \in R^\times\}.$$

Example. The two most relevant special cases here are

$$\mathrm{GL}_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det(A) = \pm 1\}$$

since $\mathbb{Z}^\times = \{1, -1\}$, and

$$\mathrm{GL}_n(\mathbb{Z}_m) = \{A \in M_n(\mathbb{Z}) \mid \det(A) \in \mathbb{Z}_m^\times\}.$$

This last group is used in the Hill cipher.

9.2. **Endomorphisms of groups.** Let A be an abelian group written additively.

Definition 9.6. An endomorphism of an abelian group A is a homomorphism $f : A \to A$. The set of all endomorphisms of A is denoted by $\mathrm{End}(A)$.

If $f, g \in \mathrm{End}(A)$, we can define their sum $(f+g) : A \to A$ by function addition. I.e., define $(f + g)(a) = f(a) + g(a)$ for all $a \in A$.

Exercise 20: Prove that if A is an abelian group and $f, g \in \mathrm{End}(A)$, then $f + g \in \mathrm{End}(A)$.

Similarly, we can define a multiplication on $\mathrm{End}(A)$ by composition. Then the identity map acts as identity for multiplication (i.e., compositition) and the trivial map which sends every element to 0 is the identity for addition.

Proposition 9.7. *If A is an abelian group, then* $\mathrm{End}(A)$ *is a ring with one.*

10. Fields

Definition 10.1. A field F is a commutative ring with one with $1_F \neq 0_F$, and every non-zero element is a unit.

Remark. As pointed out in problem 18, the condition $1_F \neq 0_F$ rules out the trivial ring from being considered a field.

Example. With their usual operations, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all fields, but $\mathbb{Z}$ is not because $2 \neq 0$ in $\mathbb{Z}$, but 2 has no multiplicative inverse in $\mathbb{Z}$.

One of our most important examples of fields come from the rings $\mathbb{Z}_n$.

Proposition 10.2. *Let $n \in \mathbb{Z}^+$. Then $\mathbb{Z}_n$ is a field if and only if n is prime.*

Proof. If n is prime and $a \in \mathbb{Z}_n - \{0\}$, then $n \nmid a$. Since n is prime, $\gcd(a, n) = 1$, so by the Bezout property (Thm. 17.4), there exists $r, s \in \mathbb{Z}$ such that $ra + sn = 1$, which implies $ra \equiv 1 \pmod{n}$. Thus, every non-zero element is a unit in a commutative ring with one (and $n > 1$ implies $0 \not\equiv 1 \pmod{n}$), and so $\mathbb{Z}_n$ is a field.

Conversely, if $\mathbb{Z}_n$ is a field we must have $n > 1$ (or else $0 \equiv 1 \pmod{n}$). If n is not prime, then it is composite, and has a non-trivial factorization $n = ab$ with $1 < a, b < n$. Since $a \not\equiv 0 \pmod{n}$, it would have to have a multiplicative inverse a' such that $aa' \equiv 1 \pmod{n}$. Multiplying by b we get

$$\begin{aligned} b &\equiv b(aa') \pmod{n} \\ &\equiv (ba)a' \pmod{n} \\ &\equiv 0 \cdot a' \pmod{n} \\ &\equiv 0 \pmod{n} \end{aligned}$$

But then $1 \equiv ab \equiv a \cdot 0 \equiv 0 \pmod{n}$, a contradiction. Thus, if n is not prime, then $\mathbb{Z}_n$ is not a field. □

We prove one small proposition for fields which forms the backbone of many results involving roots of polynomials over a field.

Proposition 10.3. *If F is a field, $a, b \in F$ and $ab = 0$, then $a = 0$ or $b = 0$.*

Proof. Suppose $ab = 0$ and $a \neq 0$. Then a has a multiplicative inverse; multiply by it to get

$$\begin{aligned} a^{-1}(ab) = a^{-1}0 &\implies (a^{-1}a)b = 0 \qquad \text{(by Prop. 9.4)} \\ &\implies 1 \cdot b = 0 \\ &\implies b = 0. \end{aligned}$$

□

Remark. The conclusion fails in some of the rings we have seen. For example, in $\mathbb{Z}_6$, $2 \cdot 3 \equiv 0 \pmod 6$, but $2 \not\equiv 0 \pmod 6$ and $3 \not\equiv 0 \pmod 6$. Similarly, in $M_2(\mathbb{R})$,

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

but neither matrix on the left-hand side is the zero-matrix.

10.1. **Characteristic.** The notion of characteristic can be applied to any ring, but will work in the context of rings with one.

Definition 10.4. Let R be a ring with one. If 1_R has infinite order in the additive group, we say R has characteristic zero. Otherwise, the characteristic of R is the order of 1_R under addition. We denote the characteristic of R by $\text{char}(R)$.

Recall that in a additive group, we defined $n \cdot a$ where $n \in \mathbb{Z}^+$ to be $a + \cdots + a$ (n times).

Exercise 21: Suppose R is a ring with one of characteristic $n > 0$. Prove that for all $a \in R$, $n \cdot a = 0_R$, and that n is the smallest positive integer with this property.

Example. Some of the most familiar rings have characteristic 0:

$$0 = \text{char}(\mathbb{Z}) = \text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = \text{char}(\mathbb{C}).$$

Example. If $n \in \mathbb{Z}^+$, then $\text{char}(\mathbb{Z}_n) = n$.

Suppose R and S are rings with one, R a subring of S with $1_R = 1_S$. Since the characteristic only depends the multiplicative identity, we immediately get

Proposition 10.5. *Suppose R and S are rings with one, R a subring of S with $1_R = 1_S$, then* $\text{char}(R) = \text{char}(S)$.

We will be mainly interested in fields, and the characteristic of a field is restricted.

Proposition 10.6. *If F is a field, then either* $\text{char}(F) = 0$ *or* $\text{char}(F) = p$ *for some prime p.*

Proof. Suppose F has finite characteristic n. If $n = 1$, then $1 \cdot 1_F = 0_F$, which implies $1_F = 0_F$ ↯. Thus, $n > 1$.

If n is not prime, then it is composite and $n = ab$ with $1 < a, b < n$. From the distributive law

$$0 = \underbrace{1 + \cdots + 1}_{n \text{ times}} = (\underbrace{1 + \cdots + 1}_{a \text{ times}})(\underbrace{1 + \cdots + 1}_{b \text{ times}})$$

But in a field, then implies $a \cdot 1 = 0$ or $b \cdot 1 = 0$. Either way, we get a contradiction to the fact that n is the additive order of 1 ↯. □

Remark. Proposition 10.6 is consistent with the example above and Proposition 10.2 since the latter two tell us $\text{char}(\mathbb{Z}_n) = n$, and $\mathbb{Z}_n$ is a field iff n is prime, so $\mathbb{Z}_n$ is a field iff $\text{char}(\mathbb{Z}_n)$ is prime.

11. Chinese remainder theorem

The Chinese remainder theorem is probably familiar from elementary number theory or cryptography. Here we phrase it in a way to highlight it connections to abstract algebra.

Theorem 11.1 (Chinese remainder theorem)**.** *Let $m, n \in \mathbb{Z}^+$ such that $\gcd(m, n) = 1$. Then the map*

$$\begin{aligned} \phi : \mathbb{Z}_{mn} &\to \mathbb{Z}_m \times \mathbb{Z}_n \\ [a]_{mn} &\mapsto ([a]_m, [a]_n) \end{aligned}$$

is a ring isomorphism.

Recall that being an isomorphism means that we can go back and forth between the two sides. Since it is an isomorphism of rings, the map respects addition and multiplication. A consequence of the latter is the multiplicative property of the Euler phi-function.

Corollary 11.2. *If $m, n \in \mathbb{Z}^+$ with $\gcd(m, n) = 1$, then*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Outline of proof of corollary: Filling in the steps is left to the reader. Recall that if R is a ring with one, then $R^\times$ denotes its set of units.

(1) If $\phi : R \to S$ is a ring isomorphism between rings with one, then it gives a bijection between $R^\times$ and $S^\times$.
(2) If R and S are commutative rings with 1, then $(R \times S)^\times = R^\times \times S^\times$.
(3) Deduce $|\mathbb{Z}_{mn}^\times| = |\mathbb{Z}_m^\times| \cdot |\mathbb{Z}_n^\times|$.
(4) Use that $|\mathbb{Z}_n^\times| = \varphi(n)$.

□

Proof of CRT. We sketch the proof.

(1) Show that the map ϕ is well-defined by proving that if $a, b \in \mathbb{Z}$, $a \equiv b \pmod{mn}$, then $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$.
(2) Show that ϕ respects addition (this is mainly invoking a the definition of addition in $\mathbb{Z}_n$).
(3) Show that ϕ respects multiplication (this is mainly invoking a definition of multiplication in $\mathbb{Z}_n$).
(4) Show that the map is one-to-one by showing $\ker(\phi) = \{[0]_{mn}\}$.
(5) Deduce that ϕ is surjective by counting (and using that it is injective).

□

Exercise 22:

(a) Fill in the details of the proof of Theorem 11.1.
(b) Which step(s) use the hypothesis that $\gcd(m, n) = 1$?

The traditional version of the Chinese Remainder Theorem states that if $a, b \in \mathbb{Z}$, $m, n \in \mathbb{Z}^+$ with $\gcd(m, n) = 1$, then the system of congruences

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

has a unique solution modulo mn. The existence of this solution is equivalent to the statement that the map ϕ in Theorem 11.1 is surjective, and the uniqueness is then equivalent to the statement that ϕ is injective. However, the the traditional version does not draw out the algebraic nature of the correspondence – that ϕ is a ring homomorphism – which is to many applications.

12. Curves

We work in the realm of algebraic geometry. This means that some of our basic objects come as the set of solutions to systems of polynomial equations.

In linear algebra, one studies these objects in the case when all of the equations are linear. If we have n linear equations in m unknowns with $n \leq m$, then in general we get a solution set with $m-n$ free parameters. It is an $m - n$ dimensional set (a translate of an $m - n$ dimensional vector space). However, that is not the only possible outcome: one might end up with more free parameters, or no solutions at all.

We will work with non-linear equations, but make an important simplifying assumption: we virtually always work with one equation in two unknowns. In the linear case, this resolves the ambiguity and the solution set is a line. In the non-linear case, we generally end up with

something one-dimensional. There are two degenerate situations we largely avoid because they are distractions from our main interest.

Example. The solution set for $x^2 + y^2 = -1$ over $\mathbb{R}$ is empty.

Example. The solution set for $x^2 = y^2$ over $\mathbb{R}$ is the union of two lines. If we move everything to one side of the equation, it factors: $(x + y)(x - y) = 0$. In a case like this, we say the solution set is reducible. If the corresponding polynomial does not factor, we say that the solution set is irreducible.

Again, we are not interested in these degenerate cases. In practice, the solution set to the equations we work with will be one dimensional and irreducible. The result is then called a *curve*.

13. Projective space

13.1. **Geometry.** When studying functions in calculus and high school algebra, we consider their graphs in the plane. Here the two axes play different roles, and sometimes particular points in the plane are special. For example, one might consider the graph of a polynomial, and places where it hits the x-axis are special because they correspond to roots.

In these courses, analytic geometry refers to using a coordinatized plane to study geometric ideas. A geometric figure is just a subset of the plane, and an essential notion of when two geometric figures are the same is if they are congruent. In particular, sets are congruent to their images under rotation, reflection, or translation (shift); there is no special direction, and the origin is just another point.

We will take the geometric point of view of the plane. As in calculus, we may consider higher dimensional space as well. We will work over a field K, and define *affine n-space* to be K^n as a generalization of $\mathbb{R}^n$.

13.2. **Slopes in the plane.** Consider lines in $\mathbb{R}^2$. An essential invariant is slope. From the geometric point of view, vertical lines are as good as any other line, so the set of possible slopes is almost given by $\mathbb{R}$, but we need one more "slope" to account for vertical lines. Nothing changes algebraically if we generalize to K^2 where K is a field, so we do just that.

We can approach this another way. Every slope is represented by a single line through the origin, the set of lines through the origin could be used as the set of slopes. Each such line is completely determined by a point it goes through $(a, b) \neq (0, 0)$. We define a relation on these points based on when they determine the same line:

$$(a, b) \sim (c, d) \iff (a, b) = \lambda(c, d) \quad \text{for some } \lambda \in K. \tag{3}$$

Here $\lambda(c,d) = (\lambda c, \lambda d)$ as in scalar multiplication from linear algebra.

Exercise 23: Prove $\sim$ in equation (3) defines an equivalence relation.

Since this is an equivalence relation, we want to consider the equivalence classes and write $[a : b]$ for the equivalence class of (a, b). We define $\mathbb{P}^1(K)$ to be the set of equivalence classes. Then the lines through the origin are in one-to-one correspondence with these equivalence classes.

Naturally, we can connect this point of view with the original one, that the set of slopes should be K plus one more element for vertical lines.

Proposition 13.1. *If K is a field, the elements of $\mathbb{P}^1(K)$ are in one-to-one correspondence with*

$$\{[1 : m] \mid m \in K\} \cup \{[0 : 1]\}.$$

The proof is straightforward if one breaks it into cases for $[a : b]$ based on whether or not $a = 0$.

Exercise 24: Prove Proposition 13.1.

13.3. $\mathbb{P}^n(K)$**.** We now generalize the construction from the previous section. Points in $\mathbb{P}^n(K)$ to correspond to lines through the origin in K^{n+1}. Let

$$S = K^{n+1} - \{(0, \ldots, 0)\}.$$

As above, we define a relation

$$\vec{u} \sim \vec{v} \iff \vec{u} = \lambda \vec{v} \text{ for some } \lambda \in K^\times$$

where if $\vec{u} = (x_0, \ldots, x_n)$, then $\lambda \vec{u} = (\lambda x_0, \ldots, \lambda x_n)$. We then let $\mathbb{P}^n(K) = S/\sim$.

As above, we let $[x_0 : \cdots : x_n]$ denote the equivalence class of $(x_0, \ldots, x_n)$.

13.4. **Affine points and points at infinity.** We can partition the points of $\mathbb{P}^n(K)$ into two sets in a natural way. Fix $i \in \{0, \ldots, n\}$. The two sets are

$$\{[x_0 : \cdots : x_n] \mid x_i \neq 0\} \text{ and } \{[x_0 : \cdots : x_n] \mid x_i = 0\}.$$

Although the coordinates of $[x_0 : \cdots : x_n]$ are only well-defined up to a non-zero scalar, the condition $x_i = 0$ makes sense.

If $[x_0 : \cdots : x_n]$ is in the first set, we can normalize the scaling by multiplying through by $\frac{1}{x_i}$. This makes the ith coordinate 1, and there is only one way to represent such a point with $x_i = 1$. There are n

coordinates x_j with $j \neq i$, so there is a natural bijection between the first set and K^n, i.e., a copy of affine n-space.

Points in the second set have $x_i = 0$. There are n remaining coordinates, and they

(1) cannot all be zero
(2) give the same point in projective space if they differ by multiplication by a non-zero element of K

But, these two conditions describe projective $n-1$ dimensional space. In other words, dropping x_i (which equals 0) from the list gives a natural bijection between the second set and $\mathbb{P}^{n-1}(K)$.

So, we can break $\mathbb{P}^n(K)$ into a disjoint union:

$$\mathbb{P}^n(K) = K^n \cup \mathbb{P}^{n-1}(K).$$

The K^n are called the affine points, and the $\mathbb{P}^{n-1}(K)$ are the points at infinity. Note, we initially picked $i \in \{0, \ldots, n\}$, so there are $n+1$ choices for i, and each gives a different decomposition. A given point $[x_0 : \cdots : x_n]$ ends up being an affine point in the decomposition for i if $x_i \neq 0$, and is a point at infinity where $x_i = 0$.

On one hand, a point like $[1 : 2 : 3] \in \mathbb{P}^2(\mathbb{R})$ is an affine point in all three of the decompositions, the point $[1 : 0 : 2]$ is an affine point in two decompositions and gives a point at infinity for the third (when $i = 1$). Importantly, every point $[x_0 : \cdots : x_n] \in \mathbb{P}^n(K)$ has some $x_i \neq 0$ (from the original construction), so every point is an affine point for at least one of the decompositions.

13.5. **Homogenization and dehomogenization.** Here we look at the process of switching between affine and projective coordinates. An elliptic curve lives in projective space, so we need to use projective coordinates sometimes. However, any individual point lives in at least one affine subset of projective space, so we can switch to affine coordinates when dealing with that point.

We illustrate the process with $\mathbb{P}^2(\mathbb{R})$. For projective coordinates, we will use capital letters: $[X : Y : Z]$. There are three affine spaces covering $\mathbb{P}^2(\mathbb{R})$, but our favorite will be the set where $Z \neq 0$. On this set, the transition between affine and projective coordinates is

$$(x, y) \leftrightarrow \left[\frac{X}{Z} : \frac{Y}{Z} : 1\right].$$

In other words, $x = X/Z$ and $y = Y/Z$.

13.5.1. *Homogenization.* Suppose we start with the affine equation

$$x^2 + 3y^2 = 1, \tag{4}$$

and want to convert it to projective coordinates. We simply make the substitutions above, and clear denominators. This is what it looks like.

$$\left(\frac{X}{Z}\right)^2 + 3\left(\frac{Y}{Z}\right)^2 = 1 \iff X^2 + 3Y^2 = Z^2. \tag{5}$$

The end result is a *homogeneous equation* in that every term has total degree 2 (the *total degree* of a monomial is the sum of the powers of all of its variables). Because of this the process of going from affine to projective coordinates is called homogenization.

Note that if $f(X, Y, Z) = 0$ is homogeneous of degree d, then every monomial has total degree d, so $f(\lambda X, \lambda Y, \lambda Z) = \lambda^d f(X, Y, Z)$. So, if one representative of $[a : b : c]$ is a solution to $f(X, Y, Z) = 0$, then so is every representative $(\lambda a, \lambda b, \lambda c)$. So it is fitting to use homogeneous equations when using projective coordinates.

Example. Here we find the projective equation for $x^3+xy+2x-3 = y^2$:

$$\left(\frac{X}{Z}\right)^3 + \left(\frac{X}{Z}\right)\left(\frac{Y}{Z}\right) + 2\left(\frac{X}{Z}\right) - 3 = \left(\frac{Y}{Z}\right)^2$$

which, after clearing denominators gives

$$X^3 + XYZ + 2XZ^2 - 3Z^3 = Y^2Z$$

There is a slightly faster way to homogenize. Suppose an equation has total degree d (i.e., the maximum of the degrees of monomials is d). For a term with degree k, the substitution introduces Z^k to its denominator. To clear all denominators, we multiply by Z^d, so the degree k term is multiplied by Z^{d-K}. So, the term is multiplied by the power of Z to bring it to the maximum degree.

The process is essentially the same with more variables, except that we may go back to $X_0, \ldots, X_n$.

Example. To find the projective equation for $x_1^7 - 3x_2x_3^2 = 4x_1^3x_4^5 - 11$, we use the faster method: capitalize all of the variables and mulitply each term by a power of X_0 so that its degree matches the largest degree, which is 8 (from the $4x_1^3x_4^5$ term):

$$X_0X_1^7 - 3X_0^5X_2X_3^2 = 4X_1^3X_4^5 - 11X_0^8.$$

13.5.2. *Dehomogenization.* Dehomogenization is simple. If we want to dehomogenize with respect to the variable x_i, we use the correspondence

$$(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \leftrightarrow [X_0 : \cdots : X_{i-1} : 1 : X_{i+1} : \cdots : X_n].$$

So, we replace X_i with 1, and convert the other variables accordingly.

Example. To dehomogenize $X_0X_1^7 - 3X_0^5X_2X_3^2 = 4X_1^3X_4^5 - 11X_0^8$ with respect to X_2, we apply the process to get

$$x_0x_1^7 - 3x_0^5x_3^2 = 4x_1^3x_4^5 - 11x_0^8.$$

There is a danger when homogenizing and dehomogenizing equations. In the examples above, we started with $x_1^7 - 3x_2x_3^2 = 4x_1^3x_4^5 - 11$, homogenized and dehomogenized to get $x_0x_1^7 - 3x_0^5x_3^2 = 4x_1^3x_4^5 - 11x_0^8$. However, variables in these two equations represent different things. In the first equation, $x_1 = X_1/X_0$ and in the second equation $x_1 = X_1/X_2$. The projective coordinates are consistent, but not the two sets of affine coordinates. For this reason, we will usually use different variable names for different dehomogenizations.

Usually, we work in $\mathbb{P}^2$ with coordinates $[X : Y : Z]$. The affine coordinates with $Z = 1$ will be (x, y), which means we need to pick other letters for the other dehomogenizations.

Example. Dehomogenize $X^3+XYZ+2XZ^2-3Z^3 = Y^2Z$ with respect to Y. Here we will use $u = X/Y$ and $v = Z/Y$. The process is to set $Y = 1$, replace X with u, and replace Z with v, which gives $u^3 + uv + 2uv^2 - 3v^3 = v$.

13.5.3. *Points at infinity.* Here, we will work in $\mathbb{P}^2$. As a first example, consider the line $y = mx + b$. It has homogenization is $Y = mX + bZ$.

Points at infinity are points which satisfy the homogenized equation in projective space which do not come from solutions to the original equation, i.e., they have $Z = 0$. So, we set $Z = 0$ which gives $Y = mX$. Note, if one point is a solution to this equation, then all of its scalar multiples are solutions, but these multiples are all representatives of the same projective point. So, we are only interested in solutions up to scalar multiplication. In this case, we get one point: $[1 : m : 0]$.

Note, any two lines with slope m hit the same point at infinity. If we consider vertical lines, then a similar computation shows that they have one point at infinity, namely $[0 : 1 : 0]$.

Exercise 25: Show that the line $x = c$ has one point at infinity, namely $[0 : 1 : 0]$.

This points out part of the appeal of working in projective space.

- In the affine plane, two distinct lines intersect in 0 or 1 point.
- In the projective plane, two distinct lines always intersect in 1 point.

Moreover, there we see that the points at infinity are in $1 - 1$ correspondence with slopes of lines (including the infinite slope).

Next we consider $x^2 - y^2 = 1$, a hyperbola with asymptotes $y = \pm x$. Intuitively, we expect the points at infinity to match those of its asymptotes, and that is exactly what happens.

The homogenization of the equation is $X^2 - Y^2 = Z^2$. Setting $Z = 0$ gives

$$X^2 - Y^2 = 0 \iff Y = \pm X.$$

Up to scalar multiplication, this gives get two projective points: $[1 : 1 : 0]$, and $[1 : -1 : 0]$. These match the points at infinity for the two asymptotes.

As a final example, consider the equation $x^2 + 3y^2 = 1$. We saw earlier that its homogenization is $X^2 + 3Y^2 = Z^2$. Setting $Z = 0$ and solving gives

$$X^2 + 3Y^2 = 0 \iff X^2 = -3Y^2.$$

To deal with the fact that this is a homogeneous equation with projective solutions, we can dehomogenize. We just need to be careful to not miss any solutions in the process.

We already have $Z = 0$ so we do not get a projective point from the obvious solution $X = Y = 0$. Note that if $Y = 0$, then $X = 0$ ↯, so $Y \neq 0$. We can then dehomogenize with respect to Y to get the equation $u^2 = -3$ (with $u = X/Y$).

Over $\mathbb{R}$, we get no solutions, so there are no points at infinity in $\mathbb{P}^2(\mathbb{R})$. However, over $\mathbb{C}$ there are solutions, $u = \pm i\sqrt{3}$. Going back to projective coordinates, this gives two points $[\sqrt{3}i : 1 : 0]$ and $[-\sqrt{3}i : 1 : 0]$.

13.5.4. *Quadratic curves.* By a quadratic curve, we mean (in affine coordinates) the solutions to a quadratic equation in two variables. In analytic geometry, one learns how to make coordinate changes to shift a central point to the origin, and then to rotate the graph until it takes one of three forms: parabola, hyperbola, or ellipse[2]. If we allow scaling of variables, then every quadratic equation can be transformed into one of three specific equations.

We considered the projective equation $X^2 + Y^2 = Z^2$.

- If we dehomogenize with respect to Z, we get $x^2 + y^2 = 1$, an ellipse
- If we dehomogenize with respect to Y, we get $u^2 + 1 = v^2 \iff u^2 - v^2 = 1$, a hyperbola

The affine curves are parts of a single curve which may be missing points. Here, the ellipse and the hyperbola are just two views of the same curve. For points over $\mathbb{R}$, the ellipse has no points at infinity, but

[2]We are ignoring the degenerate cases here, like $x^2 = y^2$.

the hyperbola has two points at infinity. We think of those points as connecting the branches of the hyperbola.

The next problem shows that a curve can have one affine part be a parabola, and another be a hyperbola.

Exercise 26: Start with $y = x^2$.

(1) Find its homogeneous equation.
(2) Show that it has one point at infinity (over any field).
(3) Dehomogenize with respect to X.

From the examples above, we have seen that a parabola and a hyperbola can both be affine parts of the same curve. Similarly, an ellipse and a hyperbola can be affine parts of the same curve. There are three affine parts to every projective curve, and in fact, one can find equations of curves where these three affine parts hit all three types! In projective space, the situation is very simple: there is only one type of (smooth) quadratic equation. From the projective curves point of view, when you look at any affine piece, you see most of the curve, but not all of it.

The situation is analgous to holding a spherical object and trying to see it. No matter how you hold it, you do not see all of the surface of the sphere. You can, however, turn the sphere and get different views. Every point is visible from some view, but no one view lets you see all of the points at once.

Similarly with a curve in projective space (of any degree), the affine parts let us see parts (most) of the curve, and every point is in part of some affine piece, but no affine part contains all of the points (technically, we should add the condition "over an algebraically closed field").

14. More about group homomorphisms

For general functions between sets, the inverse image of an element can have various sizes. For group homomorphisms, it is much more restrictive. Suppose $f : H \to K$ is a group homomorphism. If $k \in K$ but $k \notin \mathrm{Im}(f)$, then clearly $f^{-1}(k) = \emptyset$. If $k \in \mathrm{Im}(f)$, then $k = f(a)$ for some $a \in H$. We focus on these elements.

Proposition 14.1. *Suppose $f : G_1 \to G_2$ is a homomorphism of groups. Then for all $k \in \mathrm{Im}(f)$, the sets $f^{-1}(k)$ have the same number of elements as $\ker(f)$.*

We will prove this in two steps: we show that the inverse image of a point (from the image) is always a left coset, and then we show that all left cosets (of a given subgroup) have the same number of elements. First, we should define left coset.

Definition 14.2. If G is a group, H is a subgroup of G, and $a \in G$, then the left coset of a, denoted aH is the set

$$aH = \{ah \mid h \in H\}.$$

Recall that if $f : G_1 \to G_2$ is a homomorphism, then $\ker(f)$, the kernel of f, is a subgroup of G_1. Moreover, $\ker(f) = f^{-1}(e)$, so it is the inverse image of a particular point.

Lemma 14.3. *Suppose $f : G_1 \to G_2$ is a homomorphism of groups and $a \in G_1$. Then*

$$a\ker(f) = f^{-1}(f(a)).$$

Proof. Suppose $x \in a\ker(f)$. Then $x = ah$ for some $h \in \ker(f)$. Note $f(h) = e$. So,

$$f(x) = f(ah) = f(a)f(h) \implies f(x) = f(a) \cdot e \implies f(x) = f(a).$$

This implies $x \in f^{-1}(f(a))$.

Now suppose $x \in f^{-1}(f(a))$. Then $f(x) = f(a)$, which implies

$$e = f(x)f(a)^{-1} = f(x)f(a^{-1}) = f(xa^{-1}).$$

Thus,

$$xa^{-1} \in \ker(f) \implies xa^{-1} = h \text{ for some } h \in \ker(f).$$

Therefore, $x = ah \in a\ker(f)$. □

Lemma 14.4. *If H is a subgroup of a group G, then for all $g \in G$, $|gH| = |H|$.*

We show that these sets have the same number of elements by constructing a bijection between them.[3]

Proof. Let $g \in G$. Define

$$\begin{aligned} f : H &\to gH \\ h &\mapsto gh \end{aligned}$$

It is clear from the definition of gH that this function is surjective. To see that it is injective, note that for all $a, b \in H$,

$$f(a) = f(b) \implies ga = gb \implies a = b$$

by left-cancellation (or multiplication on the left by g^{-1}. Thus f is also injective, hence bijective, and we get $|H| = |gH|$. □

[3]This works in the situation we are interested in, namely when H is finite, but applies to cardinalities of infinite sets.

15. More about fields

15.1. **Extension fields.** We stipulate the following as a fact from abstract algebra.

Proposition 15.1. *If K is a field, then there is a field $\overline{K}$ called the* algebraic closure of K *with the following two properties:*

1. *every $\alpha \in \overline{K}$ is the root of a non-constant polynomial with coefficients in K*
2. *every non-constant polynomial with coefficients in K factors as a product of degree 1 polynomials over $\overline{K}$.*

The theorem covers not only the existence of this large field containing all roots of all polynomials from K, but also that every element of this field is the root of a polynomial. In particular, if α and β are both roots of polynomials in $K[x]$, then so is $\alpha + \beta$ and $\alpha\beta$.

Example. If $K = \mathbb{R}$, then $\overline{K} = \mathbb{C}$.

When considering roots of polynomials, we can multiply by a non-zero constant. So, we normally deal with monic polynomials, i.e., ones whose highest degree coefficient is 1.

Similarly, when considering the factorization of monic polynomials, we can adjust constant factors to make each factor monic as well.

Example. The polynomial $x^2 - 4$ factors over $\mathbb{Q}$ as $(2x - 4)(\frac{1}{2}x + 1)$, but we can multiply the first factor by $\frac{1}{2}$ and the second by 2 to obtain $x^2 - 4 = (x - 2)(x + 2)$.

Proposition 15.2. *Let K be a field and $\alpha \in \overline{K}$. Let $f(x)$ be a monic polynomial with coefficients in K of minimal degree such that $f(\alpha) = 0$. Then*

1. *$f(x)$ is irreducible over K*
2. *if $\deg(f) = n$, then the elements $a_{n-1}\alpha^{n-1} + \cdots + a_0$ with $a_i \in K$ are distinct.*

Proof. For the first part, suppose not. Then we have a non-trivial factorization $f(x) = g(x)h(x)$, and can assume $g(x)$ and $h(x)$ are both monic with coefficients in K. Since the factorization is non-trivial, both $g(x)$ and $h(x)$ have degree smaller than the degree of $f(x)$. Evaluating at α we get

$$0 = f(\alpha) = g(\alpha)h(\alpha) \tag{6}$$

and so $g(\alpha) = 0$ or $h(\alpha) = 0$ (since equation (6) takes place in the field $\overline{K}$). This contradicts the minimality of the degree of $f(x)$ ↯.

For the second part, suppose

$$a_{n-1}\alpha^{n-1} + \cdots + a_0 = a'_{n-1}\alpha^{n-1} + \cdots + a'_0$$

for some $a_i, a'_i \in K$. Subtracting, we get

$$(a_{n-1} - a'_{n-1})\alpha^{n-1} + \cdots + (a_0 - a'_0) = 0.$$

By the minimality of the degree of $f(x)$, α cannot be the root of a polynomial of degree less than n over K, so $(a_{n-1} - a'_{n-1})x^{n-1} + \cdots + (a_0 - a'_0)$ must be the 0-polynomial, i.e., all of its coefficients are zero. Thus, $a_i = a'_i$ for all i. □

It is not hard to show that the polynomial $f(x)$ in the previous proposition is unique for α (lowest degree monic polynomial over K with α as a root), and is called the *monic irreducible polynomial of* α.

Another result from algebra:

Proposition 15.3. *If K is a field, $\gamma \in \overline{K}$, and n the degree of the monic irreducible polynomial for γ. Then*

$$K[\gamma] = \{a_{n-1}\gamma^{n-1} + \cdots + a_0 \mid a_i \in K\}$$

is a subring of $\overline{K}$ which is a field.

Proof. Let $\alpha = \sum_{i=0}^{n-1} a_i\gamma^i, \beta = \sum_{i=0}^{n-1} b_i\gamma^i \in K[\gamma]$. Then

$$\alpha + \beta = \sum_{i=0}^{n-1} a_i\gamma^i + \sum_{i=0}^{n-1} b_i\gamma^i = \sum_{i=0}^{n-1}(a_i + b_i)\gamma^i \in K[\gamma].$$

Similarly,

$$-\left(\sum_{i=0}^{n-1} a_i\gamma^i\right) = \sum_{i=0}^{n-1}(-a_i)\gamma^i \in K[\gamma],$$

and clearly $0 = \sum_{i=0}^{n-1} 0 \cdot \gamma^i \in K[\gamma]$. To see that $K[\gamma]$ is a subring of $\overline{K}$, all that is left is to show that it is closed under multiplication.

From the distributative law,

$$\alpha \cdot \beta = \sum_{i=0}^{2n-2} c_i\gamma^i \tag{7}$$

for some $c_i \in K$. We can reduce this to an element of the right form as follows. Note $f(x) = x^n + d_{n-1}x^{n-1} + \cdots + d_0$ for some $d_i \in K$, so $f(\gamma) = 0$ implies

$$\gamma^n = -d_0 - d_1\gamma - \cdots - d_{n-1}\gamma^{n-1},$$

and multiplying by γ^k:

$$\gamma^{n+k} = -d_0\gamma^k - d_1\gamma^{k+1} - \cdots - d_{n-1}\gamma^{n+k-1}. \tag{8}$$

In a sum such as the right-hand side of equation (7), we can reduce the "degree in γ" by repeatedly making a substitution from equation (8) until the degree is less than n.

To complete the proof, we would need to show that every non-zero element of $K[\gamma]$ has a multiplicative inverse of the same form. We leave the proof to a course in abstract algebra.[4] □

Now suppose K is a field, $\alpha \in \overline{K}$, and $f(x)$ is the monic irreducible polynomial for α over K. By Prop. 15.3, we get a field $K[\alpha]$. It is pretty easy to see that elements of that form are closed under addition and additive inverse. When multiplying two elements of that form, we typically get powers of α as high as α^{2n-2}.

15.2. **Finite fields.** A *finite field* is simply a field K which is a finite set. The most familiar examples are $\mathbb{Z}_p$ with p prime. In general, one can prove

- if K is a finite field, then it has characteristic p for some prime p
- if K is a finite field of characteristic p, then it has order p^n for some $n \in \mathbb{Z}^+$
- for every prime p and positive integer n, there exists a unique subfield of $\overline{\mathbb{F}}_p$ which is finite of order p^n.

Given this, we will write $\mathbb{F}_{p^n}$ for the field of order p^n. Since $\mathbb{Z}_p$ is a field of order p, we have $\mathbb{Z}_p = \mathbb{F}_p$. We will use the $\mathbb{F}_p$ notation when we want to emphasize that we are talking about $\mathbb{Z}_p$ as a field, and $\mathbb{Z}_p$ if we want to emphasize that we are dealing with integers modulo p, or that we have a cyclic group of order p.

15.3. **Characteristic p.** Let F be a field with prime characteristic p. In particular, this applies to any finite field. Our goal here is to prove the following proposition, and see some of its consequences.

Proposition 15.4 (Freshman Dream)**.** *If* $\mathrm{char}(F) = p$ *and* $a, b \in F$*, then*

$$(a+b)^p = a^p + b^p.$$

Proof. We will use the binomial theorem, that

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

[4] One could either prove and use an analogue of the Bezout property for polynomials, or linear algebra.

where the coefficients

$$\binom{n}{i} = \frac{n(n-1)(n-2)\cdots(n-i+1)}{i!}.$$

It can be proven by induction in any commutative ring. Moreover, one can show that the coefficients $\binom{m}{i}$ are integers by induction.

In the case where $n = p$ and $1 \leq i \leq p-1$, there is a factor of p in the numerator, but all factors in the denominator are relatively prime to p (they are less than p since p is prime). So, the coefficient is a multiple of p making that term 0 in characteristic p. □

With this in hand, we can define Frobenius maps.

Proposition 15.5. *If F is a field with characteristic p prime, then*

$$\mathcal{F}_p : F \to F$$

given by $\mathcal{F}_p(a) = a^p$ is a ring homomorphism.

Proof. We need to check that $\mathcal{F}_p$ respects both addition and multiplication. For all $a, b \in F$,

$$\mathcal{F}_p(ab) = (ab)^p = a^p b^p = \mathcal{F}_p(a)\mathcal{F}(b)$$

since multiplication is commutative, and

$$\mathcal{F}_p(a+b) = (a+b)^p = a^p + b^p = \mathcal{F}_p(a) + \mathcal{F}_p(b)$$

where the key middle step follows from Prop. 15.4. □

Since a ring homomorphism is a group homomorphsim for addition, we get

Corollary 15.6. *If F is a field of characteristic p, then $\mathcal{F}_p : F \to F$ is injective.*

Proof. By Proposition 14.1, it suffices to show that the kernel is trivial. But

$$\begin{aligned} a \in \ker(\mathcal{F}_p) &\iff \mathcal{F}_p(a) = 0 \\ &\iff a^p = 0 \\ &\iff a = 0 \end{aligned}$$

since in a field, if a product of elements is zero, then one of the factors must be zero. □

If we compose $\mathcal{F}_p$ with itself, we get the function

$$\mathcal{F}_p \circ \mathcal{F}_p(a) = \mathcal{F}_p(\mathcal{F}_p(a)) = \mathcal{F}_p(a^p) = (a^p)^p = a^{p^2},$$

and similarly

$$\mathcal{F}_p \circ \mathcal{F}_p(a) \circ \mathcal{F}_p = \mathcal{F}_p(a^{p^2}) = (a^{p^2})^p = a^{p^3}.$$

By induction, we see that we compose $\mathcal{F}_p$ with itself n times, we get the function we denote $\mathcal{F}_{p^n}(a) = a^{p^n}$. Since the composition of two injective homomorphisms is an injective homomorphism, we have that $\mathcal{F}_{p^n} : F \to F$ is an injective ring homomorphism for all $n \in \mathbb{Z}^+$. To simplify notation, we let $q = p^n$ and write $\mathcal{F}_q$.

The field $\overline{\mathbb{F}}_p$ is a field of characteristic p, so we can consider $\mathcal{F}_q$ on $\overline{\mathbb{F}}_p$ (where $q = p^n$). The question is, what are its fixed points.

Proposition 15.7. *If p is prime, $n \in \mathbb{Z}^+$, and $q = p^n$, then*

$$\{a \in \overline{\mathbb{F}}_p \mid \mathcal{F}_q(a) = a\} = \mathbb{F}_q.$$

The right-hand side of the equation is the unique field of order q.

Proof. We first note that if $a \in \overline{\mathbb{F}}_p$ and $\mathcal{F}_q(a) = a$, the $a^q = a$, i.e., a is a root of $f(x) = x^q - x$. This polynomial has exactly q roots in $\overline{\mathbb{F}}_p$. Note, $f'(x) = qx^{q-1} - 1 = -1$ ($q = p^n = 0$ as a multiplier in characteristic p), so $f(x)$ and $f'(x)$ have no common roots. Hence, there are exactly q distinct roots of $x^q - x$ in $\overline{\mathbb{F}}_p$.

Now if $b \in \mathbb{F}_q$, we consider two cases. If $b = 0$, then $b^q - b = 0^q - 0$, so b is a root of $x^q - x$. If $b \neq 0$, then b is an element of the group $\mathbb{F}_q^\times$, which is a finite group of order $q - 1$. Hence $b^{q-1} = 1$, Multiplying by b, we get $b^q = b$, and so b is a root of $x^q - x$.

Comparing the results of the two paragraphs, the field $\mathbb{F}_q$ provides q fixed points for $\mathcal{F}_q$, and there are exactly q fixed points, so the two sets are equal. □

Note, the second half of this proof is often used to prove Fermat's Little Theorem. In abstract algebra, the material is usually arranged a bit differently, and this argument is part of the proof of the existence and uniqueness of the field $\mathbb{F}_q$.

16. Group algorithms

Here we present three algorithms which apply to any group. Particular instances of these may be familiar from other classes.

16.1. **Square and multiply.** The name for this algorithm applies when the group is written multiplicatively. Of course, it is useful in additive groups, like the group of an elliptic curve.

Given a group G, an element $g \in G$, and $n \in \mathbb{Z}^+$, the goal is to compute g^n efficiently. If we use the "naive algorithm" of repeated multiplication, this takes $n - 1$ steps.

There are two ideas involved. For the first, suppose n is a power of 2, such as $n = 16 = 2^4$. Then, we can compute g^{16} with just 4 multiplications:

$$\begin{aligned} g^2 &= g \cdot g \\ g^4 &= (g^2) \cdot (g^2) \\ g^8 &= (g^4) \cdot (g^4) \\ g^{16} &= (g^8) \cdot (g^8) \end{aligned} \tag{9}$$

In short, this uses basic exponent rules: $(g^{2^j})^2 = g^{2 \cdot 2^j} = g^{2^{j+1}}$.

Now if the exponent is not a power of 2, we write it as a sum of distinct powers of 2. This is always possible, and is equivalent to writting the number in base 2. We compute the powers as above, and then multiply together what we need.

Example. Suppose we want to compute g^{19}. We first write

$$19 = 2^0 + 2^1 + 2^4$$

One way to find this is to start with the largest power of 2 which is ≤ 19, subtract it from 19, and repeat.

Next we compute squarings exactly as in equation (9) (four steps), saving all of the results. Then we compute

$$g^{19} = g^{2^0+2^1+2^4} = g^{2^0} \cdot g^{2^1} \cdot g^{2^4} = g \cdot g^2 \cdot g^{16}$$

and each of these three values have already been computed. There are two more multiplications needed in the final expression. The result is computed with 4 squarings and 2 multiplications, so 6 operations as oposed to 18 with the naive algorithm.

Historically, this is one of the oldest recorded algorithms when applied to the problem of multiplying two positive integers, which can be viewed as "repeated addition" in the additive group $\mathbb{Z}$, and is also known as Russian Peasant Multiplication.

16.2. **Order of an element with a multiplicative bound.** Let G be a group and $g \in G$. The question is: if we know $|g|$ is a divisor of m for some $m \in \mathbb{Z}^+$, then how do we efficiently find $|g|$. We give an algorithm which runs in polynomial time provided we can somehow factor m.

The algorithm is based on the following proposition.

Proposition 16.1. *Suppose G is a group, $g \in G$, and $m \in \mathbb{Z}^+$, such that $g^m = e$, and p a prime dividing m. If $g^{m/p} \neq e$, then the exponent of p in the factorization of m equals the exponent of p in the factorization of $|g|$.*

Proof. Let $m = p_1^{a_1} \cdots p_k^{a_k}$ be the prime power factorization of m. Reordering the factors, we can assume $p = p_1$. Let $n = |g|$. Since $g^m = e$, $n \mid m$, and so we can factor n over the same set of primes $n = p_1^{b_1} \cdots p_k^{b_k}$ with $0 \leq b_i \leq a_i$ for all i. We want to show $b_1 = a_1$.

So, suppose $b_1 < a_1$. Then $n \mid (m/p)$ (recall $p = p_1$), which implies $g^{m/p} = e$ ↯. Thus, $b_1 = a_1$. □

If we apply the proposition to every prime dividing m, we get the following corollary which gives a criterion for checking if a value m is the order of g.

Corollary 16.2. *Suppose G is a group, $g \in G$, and $m \in \mathbb{Z}^+$ such that*

- $g^m = e$
- $g^{m/p} \neq e$ *for every prime* $p \mid m$

Them m is the order of g.

For the algorithm, suppose G is a group, $g \in G$, $m \in \mathbb{Z}^+$ and $g^m = e$. We then

(1) Factor $m = p_1^{a_1} \cdots p_k^{a_k}$.
(2) Loop over the primes p_i. For each i,
   (a) If $g^{m/p_i} = e$, replace a_i with $a_i - 1$. If now $a_i = 0$, move to the next prime. If a_i is still positive, repeat this step with the same prime p_i.
   (b) If $g^{m/p_i} \neq e$, move to the next prime p_i.

Example. Let $p = 7129$, which is prime. We want to find the order of 3467 modulo p, i.e., in $\mathbb{Z}_{7129}^\times$. By Fermat's Little Theorem, we know $3467^{7128} \equiv 1 \pmod{7129}$, so we have a starting value of m. We then factor $7128 = 2^3 3^4 11$, so we have three primes to check.

$$3467^{7128/2} \equiv 7128 \not\equiv 1 \pmod{7129}$$
$$3467^{7128/3} \equiv 1 \pmod{7129}$$

So, we revise of value of m to $(2^3 3^4 11)/3 = 2376$ and check

$$3467^{2376/3} \equiv 1 \pmod{7129}$$

So, we revise again to $m = (2^3 3^3 11)/3 = 792$ and check

$$3476^{792/3} \equiv 5879 \not\equiv 1 \pmod{7129}$$
$$3476^{792/11} \equiv 5899 \not\equiv 1 \pmod{7129}$$

So, the order of 3476 in $\mathbb{Z}_{7129}^\times$ is 729. Note, we did not have to recheck the exponent on 2.

There are lots of powers to compute in the example. They can be computed by square and multiply, and even that can be sped up since we are always computing powers of 3476 modulo 7129. So, we would only need to do the series of squarings once. Then for each power, we just have to do the "multiply" stage.

16.2.1. *Primality proving.* For some cryptosystems, it is important to have large prime numbers. A test like Rabin-Miller is effective in finding composite numbers, but does not prove that an input is prime. Corollary 16.2 is the basis of a primality proving algorithm called the Pocklington-Lehmer test. The algorithm we present here is a slight simplification of the test, but the difference in practice is negligible.

Suppose we have $m \in \mathbb{Z}^+$ we think is prime and want to prove it is prime. If we can find an integer a which has order $m-1$, then $\varphi(m) = m-1$ since

$$m - 1 \geq \varphi(m) = |\mathbb{Z}_m^\times| \geq |a| = m - 1,$$

so we have equality all the way across. But, $\varphi(m) = m-1$ means all of the numbers $1, 2, \ldots, m-1$ are relatively prime to m. In particular, m has no non-trivial divisors, so m is prime.

So, how can we find this value of a, just try $a = 2, 3, 4, \ldots$ until we find a winner. If m really is prime, such values must exist (existence of primitive roots modulo p), and their proportion cannot be too small. For each a, we apply Corollary 16.2 to see if it has order $m-1$.

The slowest part of this primality proving algorithm is that we must factor $m-1$. So, it is not useful in all cases, but can be used to prove primality of numbers of special forms (where $m-1$ is easy to factor).

16.3. **Order of an element given an archimedian bound.** Let G be a group and $g \in G$. The question is: if we know $|g| \leq B$ for some bound B, then how do we efficiently find $|g|$. Algorithms for this are given in the text. Baby-step Giant-step is a deterministic algorithm (with $O(\sqrt{B})$ steps and $O(\sqrt{B})$ storage), and Pollard's rho is a probabilistic algorithm (with $O(\sqrt{B})$ steps and constant storage).

17. Number theory background

We start with a definition.

Definition 17.1. If $a, b \in \mathbb{Z}$, then we say that a divides b and write $a \mid b$ if there exists an integer c such that $ac = b$.

Theorem 17.2 (Division algorithm)**.** *If $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$, then there exists a unique pair of integers q and r such that $a = bq + r$ and $0 \leq r < b$.*

With a, b, q, r as above, we write $r = a \bmod b$. Note, $r = 0$ if and only if $b \mid a$.

Definition 17.3. If $a, b \in \mathbb{Z}$, then

- if $a = b = 0$, then we define $\gcd(a, b) = 0$,
- if $a \neq 0$ or $b \neq 0$, then we define $\gcd(a, b)$ to be the largest integer d such that $d \mid a$ and $d \mid b$.

The next theorem is also refered to as the Extended Euclidean Algorithm since values for r and s can be computed from the Euclidean algorithm plus a little more work.

Theorem 17.4 (Bezout property)**.** *If $a, b \in \mathbb{Z}$, then there exist integers r and s such that*

$$ra + sb = \gcd(a, b).$$

The next proposition is often proven as a step towards proving unique factorization in $\mathbb{Z}$. The name comes from ring theory where one distinguishes prime elements from irreducible elements of a ring (the point here is that they are the same in $\mathbb{Z}$).

Proposition 17.5 (Prime property)**.** *Let $n \in \mathbb{Z}$, $n > 1$. Then n is prime if and only if*

$$\forall a, b \in \mathbb{Z}, n \mid ab \implies n \mid a \text{ or } n \mid b.$$

Proof. ($\Rightarrow$) Suppose $n \nmid a$. Since $\gcd(a, n)$ divides n and n is prime $\gcd(a, n) = 1$ or n. But $n \nmid a$, so $\gcd(n, a) = 1$. Then by the Bezout property (Thm. 17.4), there exists $r, s \in \mathbb{Z}$ such that $ra + sn = 1$. Multiplying by b we get $r(ab) + snb = b$. Both terms on the left side are multiples of n, so n divides the right side, i.e., $n \mid b$.

($\Leftarrow$) Suppose not. Since $n > 1$ and is not prime, $n = ab$ for some $1 < a \leq b < n$. Thus $n \mid ab$, and so $n \mid a$ or $n \mid b$, which contradicts the inequalities on a and b ↯. □

Proposition 17.6. *If $n \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$ such that $\gcd(a, n) = \gcd(b, n) = 1$, then $\gcd(ab, n) = 1$.*

Proof. Suppose not. Then there exists some prime p such that $p \mid \gcd(ab, n)$. But then $p \mid ab$ and $p \mid n$. By the Prime Property (Prop. 17.5), $p \mid a$ or $p \mid b$. Thus, $1 < p \leq \gcd(a, n)$ or $1 < p \leq \gcd(b, n)$ ↯. □

18. Crypto 101

Here we provide the basic set up and notation we use for basic cryptography. We have a set of possible messages, $\mathcal{P}$, called the plaintexts.

It might be the set of 26 letters, or the set of all 4-letter strings, or anything. A cryptosystem has a set of keys $\mathcal{K}$, and a set of encoded texts $\mathcal{C}$ called ciphertexts. The cryptosystem provides encryption and decryption functions depending on the key being used. That is, for each $K \in \mathcal{K}$, we have functions

$$e_K : \mathcal{P} \to \mathcal{C} \quad \text{and} \quad d_K : \mathcal{C} \to \mathcal{P}$$

so that encryption followed by decryption returns the original message:

$$d_K \circ e_K = I_{\mathcal{P}}$$

(the right hand side denotes the identity function on the set of plaintexts).

Many cryptosystems encode one letter at a time, so $\mathcal{P}$ may be the set of single letters (e.g., shift and affine ciphers), but others work naturally on blocks of several letters at a time (e.g., the Hill and Vigenère ciphers). In those cases, we let $\mathcal{A}$ be the set of letters (i.e., our alphabet), and generally $\mathcal{P} = \mathcal{C} = \mathcal{A}^n$, the set of n-letter strings for some fixed $n \in \mathbb{Z}^+$.

19. Lagrange's theorem

We make frequent use of Lagrange's theorem from group theory.

Theorem 19.1 (Lagrange's theorem)**.** *If G is a finite group and H is a subgroup of G, then $|G|$ is a multiple of H.*

Most of the ingredients are already established. In Section 14, we defined cosets of a subgroup and proved that all cosets of H have $|H|$ elements. To prove Lagrange's theorem, we need just one more lemma.

Lemma 19.2. *If H is a subgroup of a group G, then the left cosets of H partition G.*

Proof. For all $g \in G$, $g = ge \in gH$, so every element of G is in at least one coset. What remains is to prove that if two cosets have non-trivial intersection, then they are the same set.

Suppose $a, b \in G$ and $aH \cap bH \neq \emptyset$. Now, there exists $x \in aH \cap bH$. So, there exists $h, k \in H$ such that $x = ah$ and $x = bk$. Thus $ah = bk$, which implies $a = bkh^{-1}$.

Let $y \in aH$. Then $y = at$ for some $t \in H$. Substituting, we get

$$y = at = (bkh^{-1})t = b(kh^{-1}t) \in bH.$$

The final step follows because H is a subgroup, and $h, k, t \in H$. Thus, $aH \subseteq bH$. The reverse inclusion now follows by reversing the roles of a and b, so $aH = bH$. □

Proof of Lagrange's theorem. We count the elements of G by counting them by coset. Each coset has the same number of elements and they partition G, so

$$|G| = |H| \cdot \text{ the number of cosets of } H.$$

Therefore, $|G|$ is a multiple of $|H|$. □

To see how this works, it helps to see some examples of cosets.

Example. Let $G = \mathbb{Z}_7^*$, and $H = \{1, 6\}$. To find the left coset of say 2, we just compute

$$2H = \{2 \cdot 1, 2 \cdot 6\} = \{2, 5\}$$

where we do the computation modulo 7. Now all of the cosets are

$$1H = \{1, 6\}$$
$$2H = \{2, 5\}$$
$$3H = \{3, 4\}$$
$$4H = \{4, 3\}$$
$$5H = \{5, 5\}$$
$$6H = \{6, 1\}$$

We have 6 elements in all, and each generates a left coset, but there is duplication: $1H = 6H$, $2H = 5H$, and $3H = 4H$. So, there are only 3 distinct left cosets, they are pairwise disjoint, and each has 2 elements. The count for Lagrange's theorem is then 3 cosets with 2 elements each for a total of $3 \cdot 2 = 6$ elements.

Exercise 27: Repeat the computation in the example using $G = \mathbb{Z}_7^*$ and $H = \{1, 2, 4\}$.

20. LFSRs

Suppose we have a plaintext which has been converted to binary form, i.e., a sequence of 0s and 1s. The optimal encryption would be a *one-time pad*, where a random binary sequence is generated, and xor'ed (i.e., added modulo 2) to the plaintext to produce the cipher text. This encryption has *perfect secrecy* – looking at the ciphertext, the probability that it came from any given plaintext is the same as it was without knowing the ciphertext. In essence, the ciphertext adds no information.

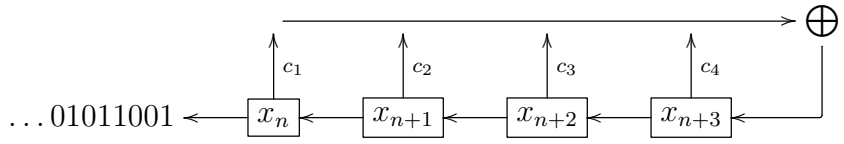
One-time pads are generally impractical, in part because the encryption key is as long as the plaintext and must also be communicated to the reader. In a stream cipher, one generates a long binary sequence

which looks random, but which can be generated from a much smaller amount of information.

Linear feedback shift registers, or LFSRs, are stream ciphers which can be implemented in hardware and which run extremely quickly, so they can be used to encrypt large amounts of data. One of the historical uses was in military field telephones. A small amount of key information was input to the phone, and then it would be able to encrypt/decrypt audio in real time.

Let $n \in \mathbb{Z}^+$. In an n-stage LFSR, we have n memory locations which each holds a bit, i.e., a 0 or a 1. We visualize these as n boxes in a row. When we run the LFSR by one step forward, the bits shift one box to the left. The bit in the leftmost box comes out, and is the next bit of the key stream. The only thing remaining is to fill the rightmost box. For that, we use a fixed linear combination of the bits in the registers taken modulo 2.

We can picture an 4-stage LFSR as follows



Here, sequence of bits which is output by the LFSR is denoted x_1, x_2, x_3, ... The linear combination used to fill the rightmost box is

$$x_{n+4} = c_4 x_{n+3} + c_3 x_{n+2} + c_2 x_{n+1} + c_1 x_n \mod 2 \tag{10}$$

$$= \sum_{j=1}^{4} c_j x_{n+j-1} \mod 2 \tag{11}$$

The values $c_1, \ldots, c_4 \in \{0, 1\}$ are called the taps. To get things started, we also need the initial contents of the boxes $(x_1, \ldots, x_4)$.

LFSRs have been used in cases where one needs to encrypt large amounts of data quickly, such as digitized audio in military phones used in the field. The bit operations can be implemented fairly easily in hardware, making them fast.

Mathematically, we can view this as simply a sequence defined by a linear recursion, namely equation (10). In general, a linear recursive

sequence can be thought of as coming from matrix multiplication:

$$C \begin{pmatrix} x_i \\ x_{i+1} \\ \vdots \\ x_{i+n-1} \end{pmatrix} = \begin{pmatrix} x_{i+1} \\ x_{i+2} \\ \vdots \\ x_{i+n} \end{pmatrix}$$

where (for a 4-stage LFSR)

$$C = \begin{pmatrix} 0 & 0 & 0 & -c_1 \\ 1 & 0 & 0 & -c_2 \\ 0 & 1 & 0 & -c_3 \\ 0 & 0 & 1 & -c_4 \end{pmatrix}$$

Shifting the LFSR one time corresponds to multiplying by C once, running it 2-steps corresponds to multiplying by C twice, or equivalently by C^2, and so on. In fact,

$$C^{j-1} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_j \\ x_{j+1} \\ \vdots \\ x_{j+n=1} \end{pmatrix}$$

So, understanding the behavior of the LFSR comes by understanding powers of C.

A standard convention for LFSRs is to assume $c_1 = 1$; otherwise, the exact same stream of bits could be generated by a shorter LFSR. With this assumption, the matrix C above has non-zero determinant (modulo 2), so is invertible. In other words, $C \in \mathrm{GL}_n(\mathbb{Z}_2)$, and we would need to analyze the powers of this group element.

Some of the basic results on LFSRs are as follows. Here we fix the taps, or equivalently, fix the matrix C. By the state of the LFSR we mean the contents of the n memory locations.

(1) From any time forward, all future states are determined by the current loading of the LFSR.
(2) The output stream is ultimately periodic with period of at most 2^n (by the Pidgeon hold principle, there has to be a repeat in the state of the LFSR after at most 2^n steps).
(3) With the convention $c_1 = 1$, the process is reversible (the matrix C is invertible). So, the output is a purely periodic sequence.
(4) If the state has all 0s, then it remains that way going forward. Similarly, if it ever reaches a state of all 0s, then the previous, hence all previous, state was all 0s.

(5) So, if the initial load is not all 0s, then output is a purely periodic sequence with period of at most $2^n - 1$.

Using linear algebra to analyze this further, one can prove that for each n, there is a set of taps so that one can achieve a period of $2^n - 1$.