MATH403: Abstract Algebra

James Zhang*

September 10, 2024

These are my notes for UMD's MATH 403: *Abstract Algebra*. They are taken live during class. This course is taught by Dr. Jonathan Rosenberg.

Contents

1 August 26, 2024 **2**
1.1 Structures in Abstract Algebra . . . 2

2 August 28, 2024 **3**

3 August 30, 2024 **5**
3.1 Sets . . . 5
3.2 Equivalence relations . . . 6

4 September 4, 2024 **6**

5 September 6, 2024 **7**
5.1 Semigroups . . . 8
5.2 Monoids . . . 8
5.3 Groups . . . 8

6 September 9, 2024 **10**

7 September 11, 2024 **10**

*Email: jzhang72@terpmail.umd.edu

§1 August 26, 2024

We start today by reviewing the syllabus, what this course covers, the textbook (*Contemporary Abstract Algebra* by Jonathan Gallian).

§1.1 Structures in Abstract Algebra

There are two main algebraic objects: **groups** and **rings**. Within groups are **semigroups**; one more axiom gives a **monoid**, one more on top of that gives **groups**. We will primarily discuss groups.

Definition 1.1. A **semigroup** is a set S with a multiplication operation $x : S \times S \to S$, or $(x, y) \mapsto x \times y$.

Remark 1.2. The associative law holds for the semigroup multiplication operator, e.g. $(x \times y) \times z = x \times (y \times z)$. Also, the xyz for the triple product is unambiguous.

Definition 1.3. A **monoid** is a semigroup with a special element 1 (sometimes denoted by 0, or e) such that for every $x \in S$, $1 \cdot x = x \cdot 1 = x$.

Definition 1.4. A **group** is a monoid with an inversion operator $x \mapsto x^{-1}$ such that for every $x \in S$, $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

Remark 1.5. The inversion operator in groups makes it possible to do cancellation, so if $x \times y = x \times z$, then $x^{-1}(xy) = x^{-1}(xz)$ leads to $(x^{-1}x)y = (x^{-1}x)z \to y = z$.

Groups arise in practice from **symmetries**. The usual symbol of the ordinary integers if $\mathbb{Z}$. A subset of the integers are the natural numbers $\mathbb{N}$.

Remark 1.6. $\mathbb{Z}$ has an **order**, i.e. for any $a, b \in \mathbb{Z}$, one of the following holds:

$$\begin{cases} a < b \\ a > b \\ a = b \end{cases}$$

$\mathbb{Z}$ also has the **well-ordering property**: and nonempty subset of $\mathbb{N}$ has a unique smallest element. This is what makes it possible to do mathematical induction.

Definition 1.7. A **ring** is an algebraic system with two associative operations: addition and multiplication.

Remark 1.8. The distributive law holds for rings, e.g. $a(b + c) = ab + ac$.

Proposition 1.9

Suppose $a, b \in \mathbb{Z}$ with $b > 0$. Then there is a unique way to divide a by b and get a remainder r, e.g. $a = qb + r$, where $0 \leq r \leq b - 1$.

Definition 1.10. We say a **divides** b if $r = 0$.

§2 August 28, 2024

Recall last class, where we introduced Proposition 1.9. We will now introduce the **Division algorithm**:

Theorem 2.1 (Division algorithm)
If $a, b \in \mathbb{Z}$, where $b > 0$, one can write $a = qb + r$, where q, r are unique integers and $0 \leq r < b$. Here, r is called the **remainder** and q is called the **quotient**.

Definition 2.2. We say (for $b \neq 0$) that $b|a$ (said b divides a) if $a = qb$ for some $q \in \mathbb{Z}$.

Remark 2.3. If $a > 0$, all (positive) divisors of a are ≥ 1, $\leq a$.

Definition 2.4. We say that $a > 0$ is **prime** if $a \neq 1$ and its only positive divisors are 1 and a.

Theorem 2.5
Let $a, b \in \mathbb{Z} - \{a\}$. Then,

1. There exists a unique largest positive number that divides both a and b. This is called the **greatest common divisor** of a and b, denoted by $\gcd(a,\, b)$.
2. $\gcd(a, b) = \min\{t = ma + nb > 0 \mid m, n \in \mathbb{Z}\}$
3. Any common divisor of a and b divides $\gcd(a, b)$.

Proof. We will prove each part separately:

1. Note that the set of positive common divisors is nonempty (e.g. it contains 1) but lies in $\{1, 2, \ldots, |a|\}$. So this set is finite and has a maximum, proving the existence of the greatest common divisor.
2. We will prove 2. and 3. together. Let $S = \{t = ma + nb > 0 \mid m, n \in \mathbb{Z}\}$; note that S is a subset of $\mathbb{N}^+$. By the well-ordering principle, S has a unique smallest element t_0. By the division algorithm, $a = qb + r$ with $0 \leq r < t_0$. Since $t_0 = ma + nb$ for some m, n, we see that $r = a - qt_0 = a - qma - qnb = (1 - qm)a + (-qn)b$. Thus, either $r = 0$ or else $r \in S$; since $r < t_0$, we have $r \notin S$. By the same argument, $t_0|b$, so t_0 is a common divisor of a and b. Let d be any common divisor of a, b. So, $a = du$, $b = dv$ for some $u, v \in \mathbb{Z}$. But $t_0 = ma + nb$ for some m, n, so $t_0 = mdu + ndr = d(mu + nv)$ is a multiple of d, i.e. $d|t_0$. So if $d \leq t_0$, we have $t_0 = \gcd(a, d)$ and any common divisor of a, b divides $\gcd(a, b)$, as desired.

□

Corollary 2.6

If a, b have no common divisors except ± 1, then $1 = ma + nb$ for some $m, n \in \mathbb{Z}$.

There is an algorithm for finding teh m, n, called the **Euclidean algorithm**. We present an example below:

Example 2.7

Find m, n for $a = 13$ $b = 54$.

Solution. By the division algorithm, we have the following:

$$\begin{aligned} 54 &= 4 \cdot 13 + 2 \\ 13 &= 6 \cdot 2 + 1 \end{aligned}$$

Working backwards, we obtain the following:

$$\begin{aligned} 1 &= 13 - 6 \cdot 2 \\ &= 13 - 6 \cdot (54 - 4 \cdot 13) \\ &= 25 \cdot 13 - 6 \cdot 54 \end{aligned}$$

Thus, $m = 25$, $n = -6$. $\square$

Theorem 2.8

If p is prime and $p|ab$, then $p|a$ or $p|b$ or both.

Proof. If $p|a$, we're done. Assume $p \nmid a$. Let $t = \gcd(p, b)$. Since p is prime, $t = 1$ or p. If it's p, we're done. But if $t = 1 = mp + nb$, then $a = mpa + nba$. But $p|ab$, so p divides both terms on the right, and thus $p|a$, as desired. $\square$

Theorem 2.9 (Fundamental Theorem of Arithmetic)

Any positive integer can be written as a product of primes. The decomposition is unique except for the order of the factors.

Proof. Let $a > 0$. The set of positive divisors of a is either $\{1\}$, in which case $a = 1$, or else $S = \{d > 1 \, |||d|a\}$ is nonempty. In this case, S has a minimum by the well-ordering principle. This must be a prime; factor it and repeat, which gives a factorization into primes. To prove uniqueness, suppose $p_1 \cdots p_r = q_1 \cdots q_s$ with p_j, q_k primes (repetitions allowed). So $p_1 | q_1 \cdots q_s$, so by the a previous theorem, p_1 divides some q_k, hence $p_1 = q_k$. After re-indexing, we obtain $p_1 \cdots p_r = p_1 q_1 \cdots q_s$. Cancel p_1 and repeat, finishing the proof. $\square$

Remark 2.10. The convention we will use is that the produce of the empty set of primes is 1. A slogan we will use if $\mathbb{Z}$ is a **unique factorization domain**.

§3 August 30, 2024

Today, we will start discussing **sets**.

§3.1 Sets

A set S has objects x; we write x is an element of S as $x \in S$¿ A subset $A \subset S$ is a subcollection of S. Any set S has a **cardinality** ("size"), often denoted by $|S|$. A finite set S has cardinality in $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$. An infinite set can be characterized by a number of properties to follow.

Remark 3.1. Not all integer sets have the same cardinality, but omost in this course will have cardinality $\mathcal{X}_0 = |\mathbb{Z}| = |\mathbb{N}|$.

Remark 3.2. Another way of denoting cardinality of a set is as follows: if $\mathcal{X}_0$ is a set,

Fact 3.3. Saying a set is infinite is the same way of saying that it has the same cardinality as some proper subset.

Definition 3.4. A proper subset A of a set S is such that $A \subset S$ and $A \neq S$.

Definition 3.5. A function has a **graph** which is a subset of $X \times Y$. Note that not every subset of $X \times Y$ is the graph of a function.

Definition 3.6. If $S \subseteq X \times Y = \{(x, y) : x \in X, y \in Y\}$, S is the graph of a function $X \to Y$. This is the same as saying for every $x \in X$ there is a unique $y \in Y$ with $(x, y) \in s$

Definition 3.7. Given a function $f : X \to Y$, X is called the **domain** of the function and Y is called the **codomain** of the function. The **range** of f is the set of all $\{f(x) : x \in X\} \subseteq Y$.

Definition 3.8. A function is called **one-to-one** or **injective** if whenever $x_1 \neq x_2$, $f(x_1) \neq f(x_2) \in Y$. A function is called **onto** or **surjective** if for every $y \in Y$, there is *some* $x \in X$ with $f(x) = y$. A function is called **bijective** if it is both injective and surjective. This is equivalent to f being invertible, i.e. to there existing $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$, where $g \circ f = g(f(x))$.

Remark 3.9. Cantor defined cardinality by saying that $|S_1| = |S_2|$ if there is a bijective function $f : S_1 \to S_2$. He also defined a set S to be **infinite** if there is an injective function $f : S \to S$ which is not surjective.

We now present an example of the above.

Example 3.10

Consider $S = \mathbb{N} = \{0, 1, 2, \ldots\}$. Take $f(x) = x + 1$; this has range $\{1, 2, 3, \ldots\} \not\subset \mathbb{N}$.

For finite sets, the situation is different. On a finite set S, every injective function $S \to S$ is surjective.

Fact 3.11. If S is finite and $f : S \to S$ is surjective, then f is injective. Cantor also defined $|S_1| \leq |S_2|$ if there is an injective function $S_1 \to S_2$.

A non-obvious fact is that the above is equivalent to the existence of a surjective function $S_2 \to S_1$.

Theorem 3.12 (Pigeonhole Principle)
Suppose S_1 and S_2 are finite sets with $|S_1| < |S_2|$. Then for any function $f : S_2 \to S_1$, there exists $x \in S_1$ with $|\{y \in S_2 : f(y) = x\}| \geq 2|$, where $\{y \in S_2 : f(y) = x\} = f^{-1}(x)$. This is called the **Pigeonhole Principle**.

§3.2 Equivalence relations

Often we will have a set S and want to **partition** it into pieces. A partition is a family of disjoint subsets of S whose union is all of S. A partition is equivalent to defining $R \subset S \times S$ (where R is the **relation**) with the following properties:

1. $\forall x \in S, (x, x) \in \mathbb{R}$
2. $\forall x, y \in S, (x, y) \in \mathbb{R} \iff (y, x) \in \mathbb{R}$
3. $\forall x, y, z \in S$, $(x, y) \in \mathbb{R}$ and $(y, z) \in \mathbb{R} \implies (x, z) \in \mathbb{R}$

The above three properties are called the **reflexive**, **symmetric**, and **transitive** properties; the relationship is called an **equivalence relation**. We will continue with an example of an equivalence relation next lecture.

§4 September 4, 2024

Example 4.1
Fix $n > 0$ in $\mathbb{N}$ and let $X = \mathbb{Z}$. Say that $x \sim y$ if $x - y$ is divisible by n (this is often written as $x \equiv y \pmod{n}$). This is an equivalence relation since

1. $n|(x - x = 0)\ \forall x$
2. If $n|(x - y)$, then $n|(y - x)$
3. If $n|(x - y)$ and $n|(y - z)$, then $x - z = (x - y) + (y - z)$, which is divisible by n

The equivalence classes are denoted $\mathbb{Z}/n$. These equivalence classes can be labeled by $0, 1, \ldots, n - 1$ because of the division algorithm: $\forall x \in \mathbb{Z}$, $x = nq + r$ with $\in \{0, 1, \ldots, n - 1\}$ and this decomposition is unique.

Fact 4.2. The usual operations $+$, $\times$ on $\mathbb{Z}$ pass to equivalence classes, i.e. if $x \sim x'$, $y \sim y'$, $z \sim z'$, $x + y \sim x' + y'$, $x \times y \sim x' \times y'$. Why? Note that

$$\begin{aligned} x \times y - x' \times y' &= x \times y - x \times y' + x \times y' - x' \times y' \\ &= x \times (y - y') + (x - x') \cdot y' \end{aligned}$$

As $y - y'$ and $x - x'$ are both multiples, of n, we have that $x \times (y - y') + (x - x') \cdot y'$ is also a multiple of n.

So $\mathbb{Z}/n$ with addition is a group, denoted by Gallian as Z_n (Rosenberg prefers $\mathbb{Z}_n$). Note that $(\mathbb{Z}/n, x)$ is not a group, since 0 has no multiplicative inverse. But the invertible elements of $\mathbb{Z}/n$ form a group $(\mathbb{Z}/n)^x$, which Gallian denotes $U(n)$.

An equivalence relation R on a set X defines a partition of X into **equivalence classes** $\{x \in X : xRy\}$ for some fixed y.

The operations $+, \times$ on $\mathbb{Z}/n$ define **modular arithmetic** $\pmod n$. These satisfy all the usual rules of arithmetic (commutative, associate, distributive).

Example 4.3

Prove that if n is a positive integer, $n^3 + (n+1)^3 + (n+2)^3$ is a multiple of 9.

Proof. We work $\pmod 9$. Note that this repeats in cycles of 3, e.g. for $n \equiv \{0, 1, 2, 3, \ldots\} \pmod 9$, $n^3 \equiv \{0, 1, -1, 0, \ldots\} \pmod 9$. In all cases, the sum of 3 consecutive numbers is 0. $\square$

Example 4.4 (Symmetries of a polygon in $\mathbb{R}^2$)

Consider a regular polygon in $\mathbb{R}^2 = \mathbb{C}$ with n sides. If you don't like complex numbers, take the polygon P with vertices $\left(\cos \frac{2\pi k}{n}, \sin \frac{2\pi k}{n}\right)$, where $k = 0, 1, \ldots, n-1$. What are the **symmetries** of P? A **symmetry** means a distance-preserving map $\mathbb{R}^2 \to \mathbb{R}^2$ sending P to itself. The set of such is called D_n.

Fact 4.5. Each element of D_N is a rotation R_θ by an angle θ (a multiple of $\frac{2\pi}{n}$) or a **reflection** across an axis. The set of rotations is $\left\{R_0 = I, R_{\frac{2\pi}{n}}, R_{\frac{4\pi}{n}}, \ldots, R_{\frac{(n-1)\pi}{n}}\right\}$. There are exactly n of these.

How many reflections are there in D_n? n. If N is even we have the axes passing through 2 opposite vertices and axes passing midway through a pair of opposite sides. If n is odd, each reflection must have a fixed point. Again have n axes of reflection and N reflection operations. So $|D_n| = n + n = 2n$.

§5 September 6, 2024

We start by going over an example of a group from last lecture.

Example 5.1

Suppose we have a P regular polynomial with n sides $\{0, 1, \ldots, n-1\}$. The **dihedral group** D_N preserves distances. So if two vertices are adjacent, they stay adjacent.

§5.1 Semigroups

Definition 5.2. A **semigroup** S is a set with a multiplication operation $m : S \times S \to S$ satisfying the associative rule $m(m(a,b),c) = m(a, m(b,c))$. Usually we suppress the M and just write $(ab)c = a(bc)$.

Semigroups have very few good properties: usually cancellation fails, i.e. $ab = ab \not\to b = c$ and $ba = bc \not\to b = c$. If you fix an element e, $m(a,b) = e$ for all a, b satisfies the associative rule.

§5.2 Monoids

Definition 5.3. Better than semigroups is what is called a **semigroup with identity** or a **monoid**. We add the axiom that there is an element e such that $ae = ea = a$ for all $a \in S$.

Remark 5.4. e above is unique with this property, since if e' has the same property then $e = e'e = e'$.

Example 5.5

Examples of monoids are the following:

1. $\mathbb{N}$: the natural numbers with addition $+$, where the special identity element is 0: $0 + n = n + 0 = n$
2. $(\mathbb{Z}/n, \times)$; the identity element is 1

Now, we will start discussing groups, which we will stay on for half of the semester.

§5.3 Groups

Definition 5.6. A **group** G is a monoid with one more operation, $i : G \to T$ written $i(x) = x^{-1}$ with the property that for any $x \in G$, $x \cdot x^{-1} = x^{-1} \cdot x$.

In fact, it's enough to just require one-sided inverses $l : G \to G$ and $r : G \to G$ with $l(x)x = e$ and $xr(x) = e$. The reason is that

$$er(x) = (l(x)x)r(x) = l(x)(xr(x)) = l(x)e$$

We now present examples of groups with inversion:

Example 5.7

The below are examples of groups with inversion:

1. $(\mathbb{Z}/n, +)$. The identity element is 0. Inversion sends x to $-x$. If you identify $\mathbb{Z}/n$ with $\{0, 1, \ldots, n-1\}$, addition and inversion have to be computed $\pmod n$. For example for $n = 4$, we have $3 + 3 = 6 \equiv 2 \pmod 4$; thus, the "states" of i are as follows: 0 always returns to 2, 1 and 3 communicate, and 2 always remains at 2.

2. $((\mathbb{Z}/n)^x, x)$. The identity element is 1. This group sits inside the monoid $(\mathbb{Z}(m, x))$. What equivalence classes lie in $(\mathbb{Z}/n)^x$? They are the equivalence classes of integers x such that $\exists y, u$ with $yx = 1 + un$. This equation is equivalent to $yx - um = 1$, which is equivalent to saying $\gcd(x, n) = 1¿$ If $n = p$ is prime, $(\mathbb{Z}/p)^x = \{1, 2, \ldots, p-1\}$.

You can compute inverses in $(\mathbb{Z}/n)^x$ by using Euclid's algorithm:

Example 5.8

Consider $n = 13$, which is prime. What is the inverse of $6 \pmod{13}$? You need to solve for y so that $by = 1 + 13u$. But $6 \cdot 2 = 12 = 13 - 1$, so $6 \cdot -2 = -12 = 1 - 13$. But $\pmod{13}$, $-2 = 13 - 2 = 11$, so 11 is the multiplicative inverse of 6 $\pmod{13}$.

Definition 5.9. The **order** of a group G, denoted by $|G|$, is just its cardinality or number of elements.

Example 5.10

The below are examples of the order of a group:

- $|(\mathbb{Z}\ n, +)| = n$
- $|(\mathbb{Z}/n)^x, x)|$ is equal to the number of integers in $\{1, \ldots, n-1\}$ which have gcd 1 with $n = \phi(n)$ (which is Euler's phi function). For n prime, recall that $\phi(n) = n - 1$.

If $n = 8$, $(\mathbb{Z}/8)^x = \{1, 3, 5, 7\}$ so $|(\mathbb{Z}/8)^x| = 4$. IF $n = 12$, $(\mathbb{Z}/12)^x = \{1, 5, 7, 11\}$, so $|(\mathbb{Z}/x)^x| = 4$. Some more examples of computing the order of a group are below:

Example 5.11

The below are more examples of computing the order of a group:

- Consider the group D_n, where the operation is composition of symmetries. $|D_n| = 2n$.
- $\mathrm{GL}(2, \mathbb{Z}/p)$ is the group of invertible 2×2 matrices with entries in $\mathbb{Z}/o$. The group operation is matrix multiplication; inversion is in the sense of matrices, e.g. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}/p) \iff ad - bc! = 0 \pmod{p}$. This is because the inverse of the matrix can be computed via $\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ This is a noncommutative group. To find its order, note that $|\mathrm{GL}(2, \mathbb{Z}/p)| = (p^2 - 1)(p^2 - p) = p(p^2 - 1)(p - 1)$. If $p = 2$, this is equal to 6

§6 September 9, 2024

Recall last class, where we started discussing groups and some examples of groups.

Remark 6.1. In any group, inverses are unique. In fact, any one-sided inverse is automatically the two-sided inverse, i.e. if $xy = e$, then $yx = e$ comes for free. The reason for this is as follows: if $xy = e$, we can multiply by y on the left, giving $(yx)y = y$, implying yx must be the identity.

Remark 6.2. The group $\mathrm{GL}(2, \mathbb{Z}/2)$ has the same multiplication table as D_3. A multiplication table is a table that describes the structure of a (finite) group by arranging all the possible products of the group's elements (Wikipedia).

Definition 6.3. If G is a group and $H \subseteq G$, H is called a **subgroup** of G if H together with the group operations of G, is itself a group. This means $e \in H$ and $ab \in H$ for and $a, b, \in H$, and $a^{-1} \in H$ for all $a \in H$.

Remark 6.4. If G is a group and $a \in G$, we can form $\langle a \rangle = \{e, a, a^2, \ldots, a^{-1}, (a^{-1})^2 = a^{-2}, \ldots\}$. This is the smallest subgroup of G containing a; $|\langle a \rangle| = |a|$, the order of a. A subgroup of the form $< a >$, $a \in G$, is called **cyclic**.

Example 6.5

Another example of a subgroup is as follows: $G = \mathrm{GL}(2, \mathbb{Z}/3)$. This group has $(3^2 - 1)(3^2 - 3) = 48$ elements.

§7 September 11, 2024