MATH403: Abstract Algebra

James Zhang*

August 29, 2024

These are my notes for UMD's MATH403: Abstract Algebra. These notes are taken live in class ("live-TEX"-ed). This course is taught by Professor Qendrim Gashi, qgashi@umd.edu. The textbook for the class is *Contemporary Abstract Algebra* by Joseph A. Gallian. 10*th Edition*.

Contents

*Email: jzhang72@terpmail.umd.edu

§1 Preliminaries

Definition 1.1 (Well-Ordering Principle)**.** If $\emptyset \neq S \subseteq \mathbb{N} \implies S$ has a smallest element,

Theorem 1.2 (Division Algorithm)
Suppose $a, b \in \mathbb{Z},$ s.t. $a < b \implies \exists!\ q, r \in \mathbb{Z}, 0 \leq r < b$ such that $a = bq + r$.

Proof.
Define a set $\{a - bk \mid k \in \mathbb{Z}, a - bk \geq 0\} \neq \emptyset$. By the Well-Ordering Principle, it has a smallest element which we will denote by r, and $r = a - bq\ \forall\ q \in \mathbb{Z}$. Assume $r \geq b$. Therefore,

$$0 \leq r - b = a * bq - b = a - b(q + 1) \in S$$

which is a contradiction since r is the smallest element. If there exists $q!, r!$ of the same type of q, r then

$$bq + r = bq! + r! \implies b(q - q!) = r! - r$$

We can assume that $r! > r$, so $b \mid r! - r$, therefore $r! = r!$ and $q! = q!$. □

Lemma 1.3 (Bezout's Lemma)
Let $a, b \in \mathbb{Z} \backslash \{0\}$ then $\exists\ s, t \in \mathbb{Z}$ such that $GCD(a, b) = as + bt$ and $GCD(a, b)$ is the least (positive) integer expressed in such a linear combination.

Proof.
Define the set $S = \{am + bn \mid m, n \in \mathbb{Z}, am + bn > 0\} \neq \emptyset$. By the Well-Ordering Principle, let $d = \min S$, which by definition of the set, must have a form $d = as + bt$ for some $s, t \in \mathbb{Z}$. Now we have to prove that d is a division of a, b and that it is the greatest division.
Claim 1: d is a divisor of a, b. By the Division Algorithm, $a = qd + r$ for some $q, r \in \mathbb{Z}, 0 \leq r < d$. If $r > 0$, then

$$r = a - qd = a - q(as + bt) = a(1 - qs) + b(-qt) \in S$$

which is a contradiction because $r \in S$ but $r < d$ and d is the smallest element in the set, so r cannot be in the set.
Claim 2: Any common divisor of a and b divides d. Assume d is such a divisor. Therefore, we write $a = d'h, b = d'k$. Therefore,

$$d = as + bt = s(d'h) + t(d'k) = d'(hs + kt)$$

and so we get that $d' \leq d$ and so $d = GCD(a, b)$.

□

Corollary 1.4

If a, b are relatively prime $\iff \exists\ s, t \in \mathbb{Z}$ s.t. $as + bt = 1$

Note 1.5. Define the GCD operator $GCD(a, b) = (a, b)$ for two integers $a, b \in \mathbb{Z}$.

Example 1.6

Let $n \in \mathbb{N}$ and consider $(n^2 + n + 1, n + 1)$. Note that

$$(n^2 + n + 1) + (n + 1)(-n) = 1 \overset{\text{Corollary}}{\implies} (n^2 + n + 1, n + 1) = 1$$

Theorem 1.7 (Fundamental Theorem of Arithmetic)

Given $n \in \mathbb{N}$, $\exists!\ p_i$ primes and $t_i \in \mathbb{N}, i, \ldots, k$ such that

$$n = \prod_{i=1}^{k} p_i^{t_i}$$

where $p_i \neq p_j$ and uniqueness is up to reordering.

Proof. Base case: for $n = 2$ this is true. Inductive hypothesis: assume this is true for $n \leq m$. Inductive case: now consider $n = m+1$. If this number is prime, then we are done. If it is not a prime, then by definition of not prime, then $m + 1 = m_1 \cdot m_n, m_1, m_2 \in \mathbb{N}$ such that $1 < m_1, m_2 < m + 1$. By assumption in our inductive hypothesis,

$$m_1 = \prod_{i=1}^{k_1} p_i^{t_i} \qquad m_2 = \prod_{i=1}^{k_2} (p_i')^{k_i'} \implies m_1 m_2 = \left(\prod_{i=1}^{k_1} p_i^{t_i}\right)\left(\prod_{i=1}^{k_2} (p_i')^{k_i'}\right)$$

and thus we have proved existence. To prove uniqueness, we will use Euclid's Lemma

Lemma 1.8 (Euclid's Lemma)

If you p prime, $a, b \in \mathbb{N}$ then $p|(ab) \implies p|a \vee p|b$

Proof. □

Suppose there are two expressions where p_i, q_j are prime and distinct

$$n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k} = q_1^{s_1} q_2^{s_2} \cdots q_c^{s_c}$$

Since $p_1 \mid (q_1^{s_1}, \ldots, q_c^{s_c}) \implies\ \exists\ j, p_i \mid q_j \implies p_i = q_j$. By repeating this process, $k = c$, and p_i's are just reordering of q_j's and the powers agree. □

§1.1 Relations

Definition 1.9 (Relation)**.** Suppose $A, B \neq \emptyset$, define $R \subset A \times B$, so R is a **relation** between A and B. If $A = B$, they say R is a relation on $A \implies R \subset A \times A$.

Note 1.10 (Functions are Relations)**.** Suppose $f : A \times B$, then $f \subset A \times B = \{(fa, f(a)) : a \in A\}$. Similarly, for a $m \times n$ matrix that is a linear transformation, then $f : [m] \times [n] \to \mathbb{R}, m = \{1, 2, \ldots, m\}$ and $n = \{1, 2, \ldots, n\}$.

Definition 1.11 (Equivalence Relations)**.** Suppose $R \subset A \times A$ then it must satisfy three properties

1. R is reflexive, which means that $(a, a) \in \mathbb{R} \ \forall \ a \in A$.
2. R is symmetric, which means $(a, b) \in \mathbb{R} \implies (b, a) \in \mathbb{R} \ \forall \ a, b \in \mathbb{R}$
3. R is transitive, which means $(a, b) \in R \ \wedge \ (a, c) \in R \implies (a, c) \in R$

Note 1.12. Instead of writing $(a, b) \in R$, let us write aRb.

Example 1.13

Let $R \subset \mathbb{R} \times \mathbb{R}$, and so $a = a \ \forall \ a \in \mathbb{R}$ and $a = b \implies b = a \ \forall \ a, b \in \mathbb{R}$ and $(a = b \ \wedge \ b = c) \implies a = c \ \forall \ a, b \in \mathbb{R}$

Definition 1.14 (Equivalence Class)**.** Let $R \subset A \times A$ be an equivalence relation, then for any $x \in A$ we call $C_x := \{a \in A \mid xRa\}$

Note 1.15. Note that $x \in C_x$ by reflexivity and so $C_x \neq \emptyset$

Note 1.16. If $x, y \in A$ then $C_x = C_y$ or $C_x \cap C_y = \emptyset$ and this naturally leads to the ideas of partitions, since $A = \cup_{x \in A} C_x$ where all of the C_x's are disjoint of equal.

Definition 1.17 (Modular Arithmetic)**.** Fix $m \in N$, usually $m > 1$. Consider residues when dividing any integer by $m = 3$.

$$\begin{pmatrix} 6 & 7 & 8 \\ 3 & 4 & 5 \\ 0 & 1 & 2 \\ -3 & -2 & -1 \\ \vdots & \vdots & \vdots \end{pmatrix}$$

where the columns of this matrix are equivalence classes C_0, C_1, C_2. Denote $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\} = \{0, 1, \ldots, n-1\}$ where each of these are the equivalence classes corresponding to these integers. In this way (lol), $1 + 2 = 0$ where addition does not depend on the equivalence class; this just means we don't have to stay in the same row when performing the addition.

Note 1.18. Let $[n] = \{1, 2, \ldots, n\}$ and denote by S_n the set of all bijective maps $[n] \to [n]$. If $f, g \in S_n$ then $f \circ g \in S_n$, and so $(S_n, \circ)$ is known as the **permutation group**. This composition of maps is the first algebraic operation that gives way to groups.

§2 Groups