MATH403: Abstract Algebra

James Zhang*

August 27, 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. 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

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

Theorem 1.7 (Fundamental Theorem of Mathematics)

Given $a \in \mathbb{N}$, $\exists!\ p_i$ prime, $i \in 1, \ldots, b$ and $t_i \in \mathbb{Z}$ such that

$$a = \prod_{i=1}^{b} p_i^{t_i}$$

§2 Groups