Algebra - MATH310

Jacopo “quartztz” Moretti

January 2024

Preface

Helo! I'm Jack :3.

I'm a student that need sto type out courses in order to make sure they properly understand them. So I put them out into the world! They might help you more than they help me :D. They are given as they are, with no guarantee of quality but guarantee of goodwill, bla bla bla. You know the gist of it.

Contents

Chapter 1

Introduction

Week 1

Algebra rests on 3 basic principles, which are equivalent in nature.

1. **Induction:** Let $S \subset \mathbb{N}$ such that $0 \in S$ and $n \in S \Rightarrow n+1 \in S$. Then, $S = \mathbb{N}$.
2. **Well-ordering principle:** For any non-empty $A \subset \mathbb{N}$, there exists an element $a : \forall b \in A, a \leqslant b$.
3. **Strong induction:** Let $S \subset \mathbb{N}$ such that $0 \in S$ and $\{0, ..., n\} \in S \Rightarrow n+1 \in S$. Then, $S = \mathbb{N}$.

It is well-established that these three principles are equivalent. Let us prove it.

Theorem 1.1. ***I*** $\Rightarrow$ ***WOP*** $\Rightarrow$ ***SI*** $\Rightarrow$ ***I***.

Proof. We will prove each induction separately.

1. 1. $\Rightarrow$ 3. Let S be the construction from the strong induction definition, and let us consider $P(n) = \{0, 1, ..., n\} \subset S$. We can prove it by induction:

   Base: $0 \in S$ by construction $\Rightarrow \{0\} \subset S$.

   Induction: Let us prove that $P(k) \Rightarrow P(k+1)$ for some k.

   $$\begin{aligned} \{0,1,...,k\} \subset S \text{ [by IH]} &\Rightarrow k \in S && \text{[by construction]} \\ &\Rightarrow k+1 \in S && \text{[by definition]} \\ &\Rightarrow \{0,1,...,k,k+1\} \in S \end{aligned}$$

   Since it is hereditary and true for 0, it is true $\forall n \in \mathbb{N}$ by the induction principle.

   Since $\{0, 1, ..., n\} \subset \mathbb{N}\ \forall n$, then $S = \mathbb{N}$.

2. $2 \Rightarrow 1$. Suppose $S \subset \mathbb{N}$ such that $0 \in S$ and $n \in S \Rightarrow n+1 \in S$. Consider $S' = \mathbb{N} \setminus S$, which we assume to be nonempty by absurd. By the well-ordering principle, we can pick a least element in $k \in S'$, which is by definition not in S. k cannot be zero, since $0 \in S$ by definition, but it can also not be non-zero, since $k \neq 0 \Rightarrow k = m+1$ for some $m < k$ (therefore not in S'). $m \in S$, so by construction, $m+1 = k \in S$ as well, which is a contradiction. S' has to be empty, so $S = \mathbb{N}$.
3. $3 \Rightarrow 2$. Done in a Problem Set, found in appendix A.

$\square$

Chapter 2

Primes

2.1 Divisors and primes

Definition 2.1. *Let $a, b \in \mathbb{Z}$. We say that a divides b (notate: $a|b$) if there exists $k \in \mathbb{Z}$ such that $b = ka$.*

Definition 2.2. *A number $p \in \mathbb{Z}$ is prime if $p > 1$ and the only numbers that divide it are itself and 1.*

Theorem 2.3. *Any $n > 1$ has a prime divisor.*

Proof. Let $S = \{n \in \mathbb{N} : n > 1 \wedge n \text{ has no prime divisors}\}$. We suppose S to be nonempty, meaning it contains a least element $k \in S$. k cannot be prime, since $k|k \ \forall k$. Therefore, it has to be true that $k = ab$ for $a, b < k \in \mathbb{N}$. Since k was the lest element, then, $a \notin S$, meaning that there exists a prime p such that $a = pt$ for $tin\mathbb{N}$. Therefore, $k = ab = ptb \Rightarrow p|k$, contradicting our construction of S. Therefore, S must be empty. $\square$

Theorem 2.4. *Any $n > 1$ can be expressed by the product of primes.*

> This proof was done in an exercise set, and can be found in the appendix.

Theorem 2.5. *The prime number factorization of a number is unique.*

Proof. Let $k = \prod^n p_i = \prod^m q_j$ two distinct prime sets. Suppose without loss of generality that $q_1 > p_1$ and let $t = (q_1 - p_1)q_2...q_m > 0$. Then:

$$\begin{aligned} t &= (q_1 - p_1)q_2...q_m \\ &= q_1 q_2...q_m - p_1 q_2...q_m \\ &= k - p_1 q_2...q_m > 0 \Rightarrow p_1|t \end{aligned}$$

We know that $p_1 \neq q_j$ for all j, so we focus on the only “weird” term:

$$\begin{aligned} (q_1 - p_1) &= sp_1 \\ \Rightarrow q_1 &= (s+1)p_1 \end{aligned}$$

Which is a contradiction because q_1 is supposed to be prime. Therefore, the prime factorization is unique. $\square$

2.2 Integer arithmetic

Definition 2.6 (Euclidian division)**.** *Let $n \in \mathbb{Z}, d \in \mathbb{Z}^*$. There exists a unique pair $q, r \in \mathbb{Z}$ such that $n = qd + r$ with $0 < r < d$.*

Proof. **Existence.** Consider the set of all numbers $S = \{n - kd\}_{k \in \mathbb{Z}} \cap \mathbb{N} = \{n - kd, kd \leqslant n\}_{k \in \mathbb{Z}}$.

We know that S is not empty, because:

- ▷ if $n >= 0$, then we set $k = 0$, meaning $n \in S$
- ▷ if $n < 0$, then we set $k = |n| + 1$, meaning $kd > |n|$ and $n + kd \in S$.

Since it's never empty, we can pick the least element of S by means of the well-ordering principle. Let's call it r. Therefore, we have $r = n - kd$ for some k. To prove $r < d$, we assume towards absurdity that $r >= d$, meaning that

$$n - (k+1)d = n - kd - d = r - d >= 0$$

meaning r wasn't minimal, which is a contradiction.

Uniqueness. Suppose $n = q_1 d + r_1 = q_2 d + r_2$. Without loss of generality, assume $q_1 > q_2$. Then:

$$(q_1 - q_2)d + r_1 = r_2 \geqslant d$$

Since r_1 and $q_1 - q_2$ are positive. This contradicts the definition of r_2, and is therefore absurd. □

Definition 2.7. *Let $a, b \in \mathbb{Z}$. We define the greatest common divisor (*gcd*) of two numbers as*

$$\gcd(a, b) = \max\{x \in \mathbb{Z} : x|a \wedge x|b\}$$

Theorem 2.8. *For $n, q \in \mathbb{Z}, d \in \mathbb{Z}^*$, such that $n = qd + r$, it is always the case that:*

$$\gcd(n, d) = \gcd(d, r)$$

Proof. By inspection of the relationship $n = qd + r$, it's clear that if $x|n \wedge x|d$ then $x|r$, and if $x|d \wedge x|r$ then $x|n$. □

> *Method* This induces a special algorithm to compute the gcd of two numbers! Let $d_1, d_2 \in \mathbb{Z}$. Then:
>
> $$\begin{aligned} d_1 &= q_1 d_2 + d_3 \\ d_2 &= q_2 d_3 + d_4 \\ &\ldots \\ d_k &= q_k d_{k+1} + 0 \end{aligned}$$
>
> The relationship $\gcd(d_{i-1}, d_i) = \gcd(d_i, d_{i+1})$ holds down the tree, meaning that by the end
>
> $$\gcd(d_1, d_2) = d_{k+1}$$
>
> Additionally, we have:

Corollary 2.9. *For any $a, b \in \mathbb{Z}^+$, there exist $x, y \in \mathbb{Z}$ such that*

$$\gcd(a, b) = xa + yb$$

This is obtained by running Euclid "up the tree".

Example 1. *TODO*

Special consequence of corollary 2.9 is the following

Corollary 2.10. *If $a, b \in \mathbb{Z}^+$ are such that $d = \gcd(a, b)$, then the equation:*

$$c = ax + by$$

has solutions (x, y) if and only if $\exists\ k > 0 : c = kd$, and they can be found as the solutions in corollary 2.9 multiplied by k.

Final consequence of these facts is the well-known Bézout's theorem.

Theorem 2.11. *Two numbers $a, b \in \mathbb{Z}^+$ are relatively prime if and only if the equation*

$$1 = ax + by$$

has integer solutions.

Definition 2.12. *For any $n \in \mathbb{Z}^+$, Euler's totient function is defined as:*

$$\varphi(n) = \left|\left\{k \in \{1, ..., n\} : \gcd(k, n) = 1\right\}\right|$$

meaning the number of positive integers less than n that are coprime to it.

Properties Properties of the totient function include:

- ▷ $\varphi(p) = p - 1$ for any prime p.
- ▷ $\varphi(pq) = (p - 1)(q - 1)$ for any pair of distinct primes p, q.
- ▷ More generally, $\varphi(mn) = \varphi(m)\varphi(n)$ for any m, n coprime.

Chapter 3

Groups

Week 2

3.1 Base definitions

Definition 3.1. *A group is a set G with a binary operation $\cdot : G \times G \to G$, satisfying the following axioms:*

- $\cdot$ *is associative:* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- *There exists a neutral element e such that $a \cdot e = e \cdot a = a \ \forall a \in G$.*
- *For any $a \in G$ there exists an inverse a^{-1} such that $a^{-1} \cdot a = a \cdot a^{-1} = e$.*

We say that G is a finite group if $|G| < \infty$. In that case, we say that G is of order $|G|$. We say that G is abelian (or commutative) if $a \cdot b = b \cdot a \ \forall a, b \in G$.

Definition 3.2. *$H \subset G$ is a subgroup if it contains the neutral element e_G and if it is closed with respect to $\cdot_G$, meaning that for every $a, b \in H$, $a \cdot b \in H$, and to inverses.*

We can note that any group has a subgroup generated by a single element:

$$\langle g \rangle = \{e, g^1, g^2, \dots, g^{-1}, g^{-2}, \dots\}$$

Since $g^i \cdot g^j = g^{i+j}$ by definition of the group operation, this set is closed under it, meaning it is a subgroup.

Definition 3.3. *If it exists, the minimal $n \in \mathbb{N}^*$ such that $g^n = e$ is called the order of g. It is finite for every element in a finite group.*

3.2 Cosets

Definition 3.4. *Let $H \subset G$ be a subgroup of G. The left coset of g with respect to H, denoted gH, is the following set:*

$$gH = \{gh, h \in H\}$$

Theorem 3.5. *Let $H \subset G$ finite. Then:*

1. *Two left-cosets xH, yH are either disjoint ($xH \cap yH = \emptyset$) or equal.*

2. *For any element $g \in G$ there exists a left coset of H such that $g \in H$.*

3. $|xH| = |H| \; \forall x \in G$

Proof. We will prove each part separately:

1. Suppose xH, yH are such that $xH \cap yH \neq \emptyset$. This means that there exist h_1, h_2 such that $xh_1 = yh_2$. Therefore,

$$x = yh_2h_1^{-1} = yh_3 \in yH \Rightarrow xh = yh_3h \; \forall h \in H$$

This means that if there exists an element of xH that is in yH, then every element in xH can be written as an element in yH, meaning they are equal.

2. For any $g \in G$, one can construct $gH = \{e, g, g^2, ...\}$, which naturally contains g.

3. The mapping

$$\begin{aligned} f(h) : H &\to xH \\ h &\mapsto xh \end{aligned}$$

is surjective, by definition of $xH = \{xh, h \in H\}$, and it is also injective, since $xh_1 = yh_2 \Leftrightarrow h_1 = h_2$. This means it defines a bijection between H and xH, indicating they have the same cardinality.

> *Example* Let $G = (\mathbb{Z}, +, 0), H = 3\mathbb{Z} \subset \mathbb{Z}$. The left coset of 0 with respect to H is :
> $$\{0 + 3k\}_{k\in\mathbb{Z}} = H = \{3 + 3k\}_{k\in\mathbb{Z}}$$
> The left coset of 1 is
> $$\{1 + 3k\}_{k\in\mathbb{Z}} = \{1, 4, 7, -2, ...\}$$

□

Theorem 3.6 (Lagrange)**.** *Let G be a finite group, $H \subset G$ a subgroup. Then, $|H|$ divides $|G|$.*

Proof. Each $g \in G$ belongs to a left coset of H, which are either disjoint or equal. This means:

$$\begin{aligned} G &= \bigcup_{i=0}^{r} x_iH && \text{[disjoint union of finitely many sets]} \\ \Rightarrow |G| &= \sum_{i=0}^{r} |x_iH| \\ \Rightarrow |G| &= \sum_{i=0}^{r} |H| && \text{[since } |xH| = |H|\text{]} \\ \Rightarrow |G| &= r|H| \end{aligned}$$

with $r \in \mathbb{N}$, meaning that $|H|$ divides $|G|$. □

Definition 3.7. *The number of left cosets of H of G is called the index of G:*

$$[G : H] = |G|/|H| \in \mathbb{N}^*$$

This means that the order of any element $g \in G$ (notated $\mathrm{ord}(g)$) divides the order of the group $|G|$, since every element generates a subgroup $\langle g \rangle$. Additionally, it implies

Corollary 3.8. $g^{|G|} = (g^{\mathrm{ord}(g)})^k = e^k = e$ *for some* k*.*

3.3 RSA

Theorem 3.9 (Euler's theorem)**.** *Let* $a, n \in \mathbb{Z}^+$*. such that* $\gcd(a, n) = 1$*. Then,*

$$a^{\varphi(n)} \equiv 1 \mod n$$

Proof. Consider $G = (\mathbb{Z}/n\mathbb{Z}, \cdot, 1)$. Then,

$$a^{\varphi(n)} = a^{|G|} \overset{3.8}{=} 1$$

□

Theorem 3.10 (Fermat's little theorem)**.** *Let* $a \in \mathbb{Z}^+$*,* p *prime such that* p *does not divide* a*. Then,* $a^{p-1} = 1$*.*

Proof. Consider $G = (\mathbb{Z}/p\mathbb{Z}, \cdot, 1)$. Then, $|G| = \varphi(p) = p - 1$. By Euler's theorem,

$$a^{\varphi(p)} = a^{(p-1)} = 1$$

□

> *RSA* The RSA cryptosystem for message transmission works as follows:
>
> 1. Choose two distinct large primes p, q.
> 2. Compute $m = pq \Rightarrow \varphi(m) = (p - 1)(q - 1)$.
> 3. Choose $e \leqslant m$ an encryption key such that $\gcd(e, \varphi(m)) = 1$.
> 4. Use Euclid's algorithm to determine d such that $ed - k\varphi(m) = 1$ for some integer k.
> 5. The encoding key is the pair (m, e), and it can be published. To decode, you use the decoding key (m, d) which is to be kept private.
>
> To send a message x to someone, you need their public pair (m, e). You first compute $c \equiv x^e \bmod m$, which can be sent publicly. To decode, the person will use their private pair (m, d), computing $x \equiv c^d \bmod m \equiv x^{ed} \bmod m$.

Why is it the case that $x^{ed} \equiv x \bmod m$? Well...

Theorem 3.11. *Let* p, q *be two distinct primes, and* $m = pq$*. Let* $e : \gcd(e, \varphi(m)) = 1$*, and let* $d \in \mathbb{Z} : ed - k\varphi(m) = 1$ *for some* $k \in \mathbb{Z}$*. Then,*

$$x^{ed} \equiv x \bmod m$$

for all $x \in \{1, ..., m\}$*.*

Appendix A

Proofs from exercise sets

This barely needs such pompous titles but oh well. It's fun.

A.1 Theorem 1.1

Theorem. *Strong Induction $\Rightarrow$ Well-ordering principle.*

Proof. We can prove this by induction. Suppose there exists a subset $Y \subset \mathbb{N}$ such that it contains no least element. Consider $P(n) =$ "$n \notin Y$".

> **Base:** If 0 was in Y, then it would be its least element, since there are no smaller elements of $\mathbb{N}$. As such, it cannot be that $0 \in Y$, meaning $P(0)$ is true.
>
> **Induction:** Assume $P(k)$ is true for any $k \in \{0, 1, ..., n\}$. Then, if it was in Y, $n + 1$ would be its smallest element, since every smaller element is not in Y. As such, $P(n + 1)$ holds as well. Since P is hereditary and true for 0, it is true for any $n \in \mathbb{N}$.

$\square$

A.2 Theorem 2.4

Theorem A.1. *Any $n > 1$ can be expressed by the product of primes.*

Proof. Consider $S = \{n \in \mathbb{N} : n > 1 \land n \text{ does not have a prime factorization}\}$. Then, we take the smallest element in this set, k. k cannot be a prime, so there exists $a, b < k$ such that $k = ab$. However, a and b cannot be in S, since they are smaller than k. This means that $a = \prod {p_{a,k}}^{a_k}, b = \prod {p_{b,k}}^{b_k}$, meaning that their product is the product of primes. Therefore, k cannot be in S, so S has to be empty. $\square$