ALGEBRA 1

Concrete Abstract Algebra: From Numbers to Gröbner Bases

Niels Lauritzen

Contents

1 Numbers

1.1 Natural numbers and integers

In order to constract abstract algebra, we define the natural numbers, $\mathbb{N}$, and the integers, $\mathbb{Z}$, where

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, \ldots\}$$
$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

Making $\mathbb{N}$ a subset of $\mathbb{Z}$, $\mathbb{N} \subset \mathbb{Z}$. In order to construct these as ordered sets, we define the greater than- or equal and greater than operator, let $X, Y \in \mathbb{Z}$ then we define

$$X \leq Y \iff X - Y \in \mathbb{N} \quad \text{and} \quad X < Y \iff X \neq Y \vee X \leq Y$$

Giving us the usual number ordering

$$\cdots < -3 < -2 < -1 < 0 < 1 < 2 < 3 < \cdots$$

Definition 1.1.1: First element

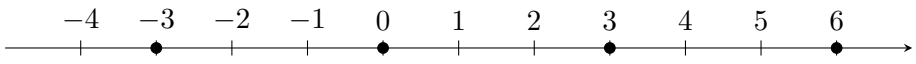
Let $s \in S$ where $S \subseteq \mathbb{Z}$, then s is the unique first element in S if $\forall x \in S, s \leq x$.

Example 1.1.1 Suppose that $S = \{1, 2, 3, 4, \ldots\}$, then $\forall x \in S, 1 \leq x$, making 1 the first element of the set.

It is immediately obvious that every nonempty subset of $\mathbb{N}$ must have a first element (due to it having a concrete lower bound), we call this property being well-ordered.

1.2 Modular arithmetic

Imagine that every multiple of 3 is marked on the axis of integers



then any integer can be expressed by the closest left multiple of 3 and the amount of you have to travel right to reach it. We call the amount you walk to the right the remainder following division by 3.

Example 1.2.1 Suppose we are observing multiples of 3, then

$$5 = 3 \times 1 + 2 \qquad 7 = 3 \times 2 + 1$$

As such 5 has remainder 2 with respect to 3 and and 7 has remainder 1 with respect to 3.

Theorem 1.2.1: Uniqueness of remainder

Let $d \in \mathbb{Z}$ where $d > 0$, then $\forall x \in \mathbb{Z}$ there exists a unique remainder $r \in \mathbb{N}$ such that

$$x = qd + r$$

where $q \in \mathbb{Z}$ and $0 \leq r < d$.

Proof. Assume that $x = q_1 d + r_1$ and $n = q_2 d + r_2$ where $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ and $0 \leq r_1, r_2 < d$ then

$$\begin{aligned} q_1 d + r_1 = q_2 d + r_2 &\implies q_1 d - q_2 d = r_2 - r_1 \\ &\implies d(q_1 - q_2) = r_2 - r_1 \end{aligned}$$

as we are assuming that $r_1 \neq r_2$, we let r_2 be larger than r_1, which implies that $r_2 - r_1 = md$ where $m = q_1 - q_2$, but this contradicts that $r_2 - r_1 \leq r_2 < d$. To prove the existence of r, we let $M = \{x - qd \mid q \in \mathbb{Z}\}$, then $M \cap \mathbb{N} \neq \emptyset$, whereby r must be the first element in $M \cap \mathbb{N}$, as such $\exists q, r = x - qd$, where $0 \leq r < d$. If $r \geq d$ then $r > r - d \geq 0$ and $r - d = x - (q+1)d \in M \cap \mathbb{N}$, contradicting that r is the first element in $M \cap \mathbb{N}$. □

Definition 1.2.1: Divisor

Suppose that $a = bc$ where $a, b, c \in \mathbb{Z}$, then we call c a divisor of a, which we write as $c \mid a$.

Definition 1.2.2: Remainder

If $x, d \in \mathbb{Z}$ where $d > 0$ we let $[x]_d$ be the unique remainder from Theorem 1.1.

1.3 Congruences

Definition 1.3.1: Congruence

Let $a, b, c \in \mathbb{Z}$ then a, b are called congruent modulo c if $c \mid b - a$, denoted $a \equiv b \mod c$, which can be simply stated as them having the same remainder when divided by c.

Proposition 1.3.1: Congruence

Let $c \in \mathbb{Z}$ where $c > 0$ then:

(i) $a \equiv [a]_c \mod c$

(ii) $a \equiv b \mod c \iff [a]_c = [b]_c$

for $a, b \in \mathbb{Z}$.

Proof. We know that $\exists q \in \mathbb{Z}, a = qc + [a]_c$ by Theorem 1.1, whereby

$$\begin{aligned} a = qc + [a]_c &\implies a - [a]_c = qc \\ &\implies c \mid a - [a]_c = qc \end{aligned}$$

proving (i). We now define $b = q'c + [b]_c$ for some $q' \in \mathbb{Z}$, then

$$a - b = (q - q')c + [a]_c - [b]_c$$

whereby $c \mid a - b \iff c \mid [a]_c - [b]_c$ which as $0 < [a]_c, [b]_c < c \implies [a]_c = [b]_c$ proving (ii). □

Example 1.3.1 The integers 29 and 14 can be written as $29 = 5 \times 5 + 4$ and $14 = 5 \times 2 + 4$, as they both have the same remainder

$$[29]_5 = [24]_5 = 4 \iff 24 \equiv 14 \mod 5$$

Proposition 1.3.2: Congruence of sum and product

Suppose that $x_1 \equiv x_2 \mod d$ and $y_1 \equiv y_2 \mod d$ then:

(i) $x_1 + y_1 \equiv x_2 + y_2 \mod d$

(ii) $x_1 y_1 \equiv x_2 y_2 \mod d$

for $x_1, x_2, y_1, y_2 \in \mathbb{Z}$.

Proof. Since d divides $x_1 - x_2$ and $y_1 - y_2$, it must also divide the sum of the two

$$d \mid x_1 - x_2 + y_1 - y_2 \implies d \mid x_1 + y_1 - (x_2 + y_2)$$

proving (i). Similarly we recognize that

$$x_1 y_1 - x_2 y_2 = x_1(y_1 - y_2) + y_2(x_1 - x_2)$$

And as x_1, y_2 are factors of terms we know to be divisible by d, so must their products be, and by (i) also their sum, proving (ii). □

Example 1.3.2 We wish to determine the remainder of 12^{11} divided by 21. We split the exponent using binary expansion

$$11 = 2^3 + 2^1 + 2^0 = 2^3 + 2 + 1$$

From this it follows that $\left[12^{11}\right] = \left[\left[12^{2^3}\right]\left[12^2\right][12]\right]$. As such we compute

$$\begin{aligned}
\left[12^1\right] &= 12 \\
\left[12^2\right] &= 18 \\
\left[12^{2^2}\right] = \left[(12^2)^2\right] &= \left[12^2\left[12^2\right]\right] = [18 \times 18] = 9 \\
\left[12^{2^3}\right] = \left[\left(12^{2^2}\right)^2\right] &= \left[\left[12^{2^2}\right]\left[12^{2^2}\right]\right] = [9 \times 9] = 18
\end{aligned}$$

Which lets us compute the remainder as

$$\left[12^{11}\right] = [18 \times 18 \times 12] = 3$$

1.4 Greatest common divisor

Definition 1.4.1: Divisor set

Let $D = \{d \in \mathbb{N} \mid d \mid n\}$ be the set of natural divisors of $n \in \mathbb{Z}$, we call D the divisor set of n and denote it $\operatorname{div}(n)$.

Example 1.4.1 A few example are listed:

$$\operatorname{div}(12) = \{1, 2, 3, 4, 6, 12\}$$
$$\operatorname{div}(28) = \{1, 2, 4, 14, 28\}$$
$$\operatorname{div}(32) = \{1, 2, 4, 8, 16, 32\}$$

Here an interesting pattern emerges when we determine the intersection of divisor sets:

$$\operatorname{div}(12) \cap \operatorname{div}(28) = \{1, 2\} = \operatorname{div}(2)$$
$$\operatorname{div}(28) \cap \operatorname{div}(32) = \{1, 2, 4\} = \operatorname{div}(4)$$

Indicating that the intersection of divisor sets for some $m, n \in \mathbb{Z}$ form a divisor set for a third number $d \in \mathbb{N}$.

Lemma 1.4.1: Euclid

Let $m, n \in \mathbb{Z}$, then there exists a unique natural number $d \in \mathbb{N}$ such that

$$\operatorname{div}(m) \cap \operatorname{div}(n) = \operatorname{div}(d)$$

Proof. Uniqueness follows from the fact that no two distinct natural numbers have the same divisior sets as it always contains itself. To prove existence of d we assume that $m, n \in \mathbb{N}$, since $\operatorname{div}(x) = \operatorname{div}(-x)$ for $x \in \mathbb{Z}$. We use induction on $\min(m, n)$ where

$$\min(m, n) = m \implies m \leq n \text{ and } \min(m, n) = n \implies m > n.$$

If $\min(m, n) = 0$, we can assume that $n = 0$ whereby $\operatorname{div}(m) \cap \operatorname{div}(n) = \operatorname{div}(m)$ as all numbers divide zero whereby $\operatorname{div}(m) \subset \operatorname{div}(0)$. We now assume that $\operatorname{div}(m) \cap \operatorname{div}(n) = \operatorname{div}(d)$ holds for every $m, n \in \mathbb{N}$ where $\min(m, n) < N$ with $N > 0$.

Using induction, we suppose that $m, n \in \mathbb{N}$ where $\min(m, n) = N$ with $m \geq n = N$. Then we have that $\exists q \in \mathbb{Z}, m = qn + r$ where $0 \leq r < n$ by Theorem 1.2.1, then

$$\operatorname{div}(m) \cap \operatorname{div}(n) = \operatorname{div}(m - qn) \cap \operatorname{div}(n) = \operatorname{div}(r) \cap \operatorname{div}(n)$$

as a number divides m, n if and only if it also divides $m - qn$. By induction we know that $\operatorname{div}(r) \cap \operatorname{div}(n) = \operatorname{div}(d)$ for some $d \in \mathbb{N}$ since $\min(r, n) = r < n = N$. □

Definition 1.4.2: Greatest common divisor

The unique number $d \in \mathbb{N}$ discussed above is called the greatest common divisor of m, n denoted $d = \gcd(m, n)$.

1.5 Euclidean algorithm

Proposition 1.5.1: Euclid's algorithm

Let $m, n \in \mathbb{N}$, then:

(i) $\gcd(m, 0) = m$ if $m \in \mathbb{N}$.

(ii) $\gcd(m, n) = \gcd(m - qn, n)$ for every $q \in \mathbb{Z}$.

Proof. As $\operatorname{div}(0) = \mathbb{Z} \implies \gcd(m, 0) = \operatorname{div}(m) \cap \operatorname{div}(\mathbb{Z}) = \operatorname{div}(m)$, proving (i). We arrive at (ii) from the fact that

$$\operatorname{div}(d) = \operatorname{div}(m) \cap \operatorname{div}(n) = \operatorname{div}(m - qn) \cap \operatorname{div}(n)$$

being an alternative way to express that $d \mid m, n \iff d \mid m - qn, n$, such that $\gcd(m, n) = \gcd(m - qn, n)$. □

Example 1.5.1 Let $m = 24$ and $n = 14$, then

$$\gcd(24, 14) = \gcd(14, 10) = \gcd(10, 4) = \gcd(4, 2) = \gcd(2, 0) = 2$$

For a more general case with $m \leq n \leq 0$, we let $r_{-1} = m$ and $r_0 = n$, if $r_0 = 0$ then $\gcd(r_{-1}, r_0) = r_{-1}$, if this is not the case however then we define $r_1 = [r_{-1}]_{r_0} \implies \exists q_1, r_1 = r_{-1} - q_1 r_0$, wherby we let $\gcd(r_{-1}, r_0) = \gcd(r_0, r_1)$, repeating until $r_N = 0$ whereby we have that $\gcd(m, n) = r_{N-1}$.

Since m, n share a common factor, it must be possible to construct a linear combination of m, n resulting in said factor.

Example 1.5.2 We wish to determine $\lambda, \mu \in \mathbb{Z}$ such that $\lambda \times 24 + \mu \times 14 = 2$, we do this by determining λ, μ for the remainder in each step of the algorithm

$$\begin{aligned}
24 &= 1 \times 24 + 0 \times 14 \\
14 &= 0 \times 24 + 1 \times 14 \\
10 &= 24 - 14 = 1 \times 24 - 1 \times 14 \\
4 &= 14 - 10 = -1 \times 24 + 2 \times 14 \\
2 &= 10 - 2 \times 4 = 24 - 14 = 2 \times 24 - 3 \times 14
\end{aligned}$$

Whereby $2 \times 24 - 3 \times 14 = \gcd(n, m)$.

Definition 1.5.1: Extended Euclidean algorithm

The Euclidean algorithm with the addition demonstrated above for computing λ, μ is called the extended Euclidean algorithm.

Lemma 1.5.1: Linear combination exists

Let $m, n \in \mathbb{Z}$, then there exist $\lambda, \mu \in \mathbb{Z}$ such that

$$\lambda m + \mu n = \gcd(m, n).$$

Proof. Let $m, n \in \mathbb{N}$ and $d = \gcd(m, n)$, then the extended Euclidean algorithm will give $\lambda, \mu \in \mathbb{Z}$ such that $\lambda m + \mu n = d$, we now show that

$$(-\lambda)(-m) + \mu n = \lambda m + (-\mu)(-n) = (-\lambda)(-m) + (-\mu)(-n) = d$$

Showing that λ, μ exist for all m, n. □

Definition 1.5.2: Coprime integers

Two integers $a, b \in \mathbb{Z}$ are called relatively prime (or coprime) if

$$\gcd(a, b) = 1.$$

Corollary 1.5.1: Divisor of product of relative prime

Suppose that $a \mid bc$ where $a, b, c \in \mathbb{Z}$ where $\gcd(a, b) = 1$, then $a \mid c$.

Proof. By Lemma 1.5.1 there exists a linear combination $\lambda a + \mu b = 1$, multiplying by c then gives $\lambda ac + \mu bc = c \implies a \mid c$ as a obviously divides the first term and bc by the proposition. □

Corollary 1.5.2: Properties of relative primes

Let $a, b, c \in \mathbb{Z}$ then:

(i) If $\gcd(a, b) = 1$, $a \mid c$ and $b \mid c$ then $ab \mid c$.

(ii) If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$ then $\gcd(a, bc) = 1$.

Proof. By Lemma 1.5.1 there exists a linear combination $\lambda a + \mu b = 1$, since $a, b \mid c$ we can write c as $c = ax = by$ for some $x, y \in \mathbb{Z}$, as such we multiply

the linear combination by c, giving

$$c = \lambda ac + \mu bc = \lambda aby + \mu bax = ab(\lambda y + \mu x)$$

proving (i). To prove (ii) we again use Lemma 1.5.7, whereby we get two identities $\lambda_1 a + \mu_1 b = 1$ and $\lambda_2 a + \mu_2 c = 1$ for some $\lambda_1, \mu_1, \lambda_2, \mu_2 \in \mathbb{Z}$, multiplying the two together we have that

$$1 = (\lambda_1 a + \mu_1 b)(\lambda_2 a + \mu_2 c) = (\lambda_1 \lambda_2 a + \lambda_1 \mu_2 c + \mu_1 b \lambda_2)a + (\mu_1 \mu_2)bc$$

Showing that $\gcd(a, bc) = 1$ whereby they are relative primes. □

1.6 Chinese remainder theorem

Example 1.6.1 Consider a number $x < 30$, let a, b, c be rows numbered upwards from zero in the following three tables where the number is located

0	2	4	6	8	10	12	14	16	18	20	22	24	26	28
1	3	5	7	9	11	13	15	17	19	21	23	25	27	29

0	3	6	9	12	15	18	21	24	27
1	4	7	10	13	16	19	22	25	28
2	5	8	11	14	17	20	23	26	29

0	5	10	15	20	25
1	6	11	16	21	26
2	7	12	17	22	27
3	8	13	18	23	28
4	9	14	19	24	29

Take for example $x = 27$, then we find $a = 1, b = 0, c = 2$, in fact, these numbers are all you need to know in order to determine x, this is called the 30-riddle.

Definition 1.6.1: Remainder map

Define

$$\mathbb{Z}/N = \{X \in \mathbb{N} \mid 0 \leq X < N\}$$

For $N \in \mathbb{N}$. If $N = n_1 \times n_2 \times \ldots \times n_t \neq 0$ then we let

$$r : \mathbb{Z}/N \to \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_t$$

By the map given by $r(X) = ([X]_{n_1}, \ldots, [X]_{n_t})$. We call this the remainder map.

Example 1.6.2 Suppose that $N = 2 \times 3 \times 5 = 30$ and $x = 27$, then we have that

$$r(27) = ([27]_2, [27]_3, [27]_5) = (1, 0, 2)$$

We recognize this tuple as the values a, b, c for $x = 27$ in the 30-riddle.

Lemma 1.6.1: Bijective remainder map

Suppose that $N = n_1 \times n_2 \times \cdots \times n_t$ where $n_1, n_2 \ldots, n_t \in \mathbb{N} \setminus \{0\}$ and $\gcd(n_i, n_j) = 1$ if $i \neq j$ then

$$r : \mathbb{Z}/N \to \mathbb{Z}/n_1 \times n_2 \times \cdots \times n_t$$

is bijective.

Proof. If $r(X) = r(Y)$ then $[X]_{n_i} = [Y]_{n_i}$ for all $i \in \{1, 2, \ldots, t\}$, implying that $X \equiv Y \mod n_i$ whereby $n_i \mid X - Y$. From Corollary 1.5.2 we know that if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$ then $\gcd(a, bc) = 1$, meaning that if a number is divisible by several coprimes, it is also divisible by their products, and as such $N \mid X - Y$. Similarly we recognize that $0 \leq X, Y < N$, whereby it is only possible for N to divide $X - Y$ if their sum is equal 0, and as such $X = Y$, implying that each mapping is unique and r is therewfore injective, this implies that r is also surjective as the codomain and domain have the same number of elements, making r injective. □

Theorem 1.6.1: Chinese remainder theorem

Suppose that $N = n_1 \times n_2 \times \cdots \times n_t$ where $n_1, n_2, \ldots, n_t \in \mathbb{Z} \setminus \{0\}$ and $\gcd(n_i, n_j) = 1$ for $i \neq j$. Consider the system of congruences

$$\begin{aligned} X &\equiv a_1 \mod n_1 \\ X &\equiv a_2 \mod n_2 \\ &\vdots \\ X &\equiv a_t \mod n_t \end{aligned}$$

for $a_1, a_2, \ldots, a_t \in \mathbb{Z}$. Then:

(i) The system has a solution $X \in \mathbb{Z}$.

(ii) If $X, Y \in \mathbb{Z}$ are solutions of the system then $X \equiv Y \mod N$. If X is a solution and $Y \equiv X \mod N$ then Y is a solution.

Proof. If X, Y are solutions then by Lemma 1.6.1 $N \mid X - Y$ and $X \equiv Y \mod N$, the same applies in reverse where $Y \equiv X \mod N$ and $N \mid Y - X$, proving (ii) by showing theyre both solutions. As we know n_i and N/n_j must be relatively prime (N/n_j contains the product of the other coprime

terms without n_j) there must exist integers λ_j, μ_j such that

$$\begin{aligned}\lambda_1 n_1 + \mu_1 N/n_1 &= 1\\ \lambda_2 n_2 + \mu_2 N/n_2 &= 1\\ &\vdots\\ \lambda_t n_t + \mu_t N/n_t &= 1\end{aligned}$$

We let $A_j = \mu_j N/n_j$ for $j = \{1, 2, \ldots, t\}$ noticing that $A_j \mod n_j = 1$ and $A_j \mod n_i = 0$ for $i \neq j$, we build a solution from these as

$$X = a_1 A_1 + a_2 A_2 + \cdots + a_t A_t$$

Where we can ignore the first term it is equal 1 when the other term is equal 0 and vice versa, whereby the equation. □

Example 1.6.3 Applying the above on the 30-riddle we have that $n_1 = 2, n_2 = 3, n_3 = 5$, we find $\lambda_i, mu_i \in \mathbb{Z}$ that satisfy

$$\begin{aligned}\lambda_1 n_1 + \mu_1 N/n_1 &= 2\lambda_1 + (2 \times 3 \times 5)/2\mu_1 = 2\lambda_1 + 15\mu_1 = 1\\ \lambda_2 n_2 + \mu_2 N/n_2 &= 3\lambda_2 + (2 \times 3 \times 5)/3\mu_2 = 3\lambda_2 + 10\mu_2 = 1\\ \lambda_3 n_3 + \mu_3 N/n_3 &= 5\lambda_3 + (2 \times 3 \times 5)/5\mu_3 = 5\lambda_3 + 6\mu_3 = 1\end{aligned}$$

Which has solution $\lambda_1 = -7, \mu_1 = 1, \lambda_2 = -3, \mu_2 = 1, \lambda_3 = -1, \lambda_3 = 1$, giving us $A_1 = 15, A_2 = 10, A_3 = 6$ whereby

$$X = 15a_1 + 10a_2 + 6a_3$$

Is a solution to the system of congruences

$$X \equiv a_1 \mod 2X \qquad \equiv a_2 \mod 3X \equiv a_3 \mod 5$$

And as such we can determine our original number using a_1, a_2, a_3, for $a_1 = 1, a_2 = 0, a_3 = 2$ we find that $X = 15 + 0 + 12 = 27$, and determine the remainder following division by 30 $[X]_{30} = [27]_{30} = 27$, which is also the number we used in the first example.

---

2 Exercises

2.1 Chapter 1

Exercise 2

Exercise 3

Exercise 4

Exercise 6

Exercise 8

Exercise 12

Exercise 13

Exercise 17

Exercise 18