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

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

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

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

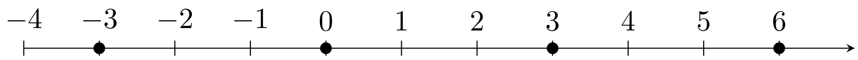
Definition 1.1: First element

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

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, for example

$$5 = 3 \times 1 + 2 \qquad 8 = 3 \times 2 + 2$$

We call the amount you walk to the right the remainder following division by 3.

Theorem 1.1: 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 $M \cap \mathbb{N} \neq \emptyset$, then 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 $M \cap \mathbb{N}$. $\square$

Definition 1.2: 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 1.3: 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 1.4: 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 1.1: 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). □

Proposition 1.2: 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. $\square$

1.4 Greatest common divisor

Definition 1.5: Divisor set

Let $\operatorname{div}(n) = \{d \in \mathbb{N} \mid d \mid n\}$ be the set of natural divisors of $n \in \mathbb{Z}$.

1.5 Euclidean algorithm

1.6 Chinese remainder theorem

2 Exercises