Monday: Division in $\mathbb{Z}_n$

The cancellation laws in $\mathbb{Z}_n$

Recall that in $\mathbb{Z}$ we have two cancellation laws: $a + c = b + c$ implies $a = b$, and $ac = bc$ implies $a = b$ for $c \neq 0$. The first of these laws carries over to $\mathbb{Z}_n$, because we can use the same argument as we did for $\mathbb{Z}$: the element $\overline{a}$ has an additive inverse $\overline{-a}$. However, the cancellation law for $\cdot_n$ does not always work. For example, fix $n = 12$. Then we have $\overline{3} \cdot_{12} \overline{4} = \overline{12} = \overline{0}$, and $\overline{6} \cdot_{12} \overline{4} = \overline{24} = \overline{0}$, so $\overline{3} \cdot_{12} \overline{4} = \overline{6} \cdot_{12} \overline{4}$, but $\overline{3} \neq \overline{6}$.

The problem is that we cannot divide both sides of the equation $\overline{3} \cdot_{12} \overline{4} = \overline{6} \cdot_{12} \overline{4}$ by $\overline{4}$. What would division mean? When might division work? What should $\dfrac{\overline{a}}{\overline{b}}$ mean when $\overline{a}, \overline{b} \in \mathbb{Z}_n$?

In $\mathbb{Q}$, the fraction $\frac{a}{b}$ is the unique solution x of the equation $a = bx$. So the problem becomes the question of whether the equation $\overline{a} = \overline{b} \cdot_n \overline{x}$ has a unique solution $\overline{x}$. In general, this equation could have no solutions, a unique solution, or more than one solution.

Example 1. *Consider the equation $\overline{6} = \overline{4} \cdot_n \overline{x}$. Show that this equation has*

- *no solutions when $n = 8$*
- *two solutions when $n = 10$*
- *a unique solution when $n = 15$.*

Now, if $\overline{a} = \overline{b} \cdot \overline{x}$ has a solution $\overline{x}$, then $a \equiv bx \pmod{n}$, so $a = bx + ny$ for some $y \in \mathbb{Z}$. From our discussion of Diophantine equations, we know this happens if and only if $\gcd(b, n) \mid a$. In particular, if $\gcd(b, n) = 1$, then this equation has a solution for all a. Further, the solution will be unique:

Theorem 2. *Let $a, b \in \mathbb{Z}$, $x \in \mathbb{N}$. If b and n are relatively prime then the equation $\overline{a} = \overline{b} \cdot_n \overline{x}$ has a unique solution $\overline{x} \in \mathbb{Z}_n$.*

Corollary 3. *If p is a prime number then for every $b \not\equiv 0 \pmod{p}$ the equation $\overline{a} = \overline{b} \cdot_p \overline{x}$ has a unique solution in $\mathbb{Z}_p$.*

Thus, division works in $\mathbb{Z}_p$ just the same as it does in $\mathbb{Q}$ and $\mathbb{R}$. We will return to this example, which is an example of a *field*, when we discuss the axioms for the real numbers in Chapter 8.

Tuesday: Polynomials

Definition. *A* polynomial in x over $\mathbb{R}$ *(or, more briefly, a* polynomial*) is an expression of the form*

$$a(x) = a_0 + a_1 x + \cdots + a_n x^n$$

where $a_0, a_1, \ldots, a_n \in \mathbb{R}$. We may change the order of the terms, and omit the terms where $a_i = 0$. The numbers $a_0, a_1, \ldots, a_n$ are called the coefficients.

The set of all such polynomials is denoted by $\mathbb{R}[x]$*.*

Definition. *The* degree *of the term* $a_i x^i$ *is* i*. The degree of the polynomial* $a_0 + a_1 x + \cdots + a_n x^n$ *is the greatest* i *such that* $a_i \neq 0$*. If there is no such* i *(i.e.* $a(x) = 0$*), then the degree is* $-\infty$*. We denote the degree of* $a(x)$ *by* $\deg a(x)$*.*

We can also consider polynomials over other sets of numbers, such as $\mathbb{Z}[x]$ (polynomials with integer coefficients), $\mathbb{Q}[x]$ (polynomials with rational coefficients) and so on.

We usually just think of a polynomial over $\mathbb{R}$ as being a function from $\mathbb{R}$ to $\mathbb{R}$. However, we must be careful when considering polynomials over $\mathbb{Z}_n$: there are infinitely many polynomials, and only finitely many functions from $\mathbb{Z}_n$ to $\mathbb{Z}_n$, so sometimes different polynomials give the same function. For example, we have $\bar{a}^n - \bar{a} = 0$ for all $\bar{a} \in \mathbb{Z}_n$, but the polynomials $x^n - x$ and 0 are not equal.

Addition of polynomials

Now that we have our set $\mathbb{R}[x]$, we will define operations of addition and multiplication on $\mathbb{R}[x]$. First, we consider addition. To add together two polynomials, we just collect together the terms with the same degree. In other words, we have

$$(a_0 + a_1 x + \cdots + a_n x^n) + (b_0 + b_1 x + \cdots + b_n x^n) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n.$$

If the two polynomials had different degrees, we have to "padd out" the one with the lower degree with terms $0x^i$. To put this another way, we have

$$(a_0 + a_1 x + \cdots + a_n x^n) + (b_0 + b_1 x + \cdots + b_m x^m) = c_0 + c_1 x + \cdots + c_N x^N,$$

where $N = \max(n, m)$, and for $0 \leq k \leq N$ we have $c_k = a_k + b_k$. [In this definition, if $i > n$ then $a_i = 0$ and if $i > m$ then $b_i = 0$.]

Exercise 4. *Suppose* $a(x)$ *and* $b(x)$ *are polynomials of degree* n *and* m *respectively. What is the degree of* $a(x) + b(x)$*?*

Multiplication of polynomials

What happens when we multiply together the polynomials $a_0 + a_1 x$ and $b_0 + b_1 x + b_2 x^2$? If we multiply out the brackets and collect terms together we get

$$\begin{aligned}(a_0 + a_1 x)(b_0 + b_1 x + b_2 x^2) &= a_0 b_0 + a_0 b_1 x + a_0 b_2 x^2 + a_1 b_0 x + a_1 b_1 x^2 + a_1 b_2 x^3 \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1)x^2 + a_1 b_2 x^3\end{aligned}$$

In general, we have

$$(a_0 + a_1 x + \cdots + a_n x^n)(b_0 + b_1 x + \cdots + b_m x^m) = c_0 + c_1 x + \cdots + c_{n+m} x^{n+m},$$

where for $0 \leq k \leq n + m$, $c_k = \sum_{i=0}^{k} a_i b_{k-i}$. [As before, we take $a_i = b_j = 0$ for any $i > n$, $j > m$.]

Exercise 5. *Suppose* $a(x)$ *and* $b(x)$ *are polynomials of degree* n *and* m *respectively. What is the degree of* $a(x)b(x)$*?*

Multiplication in $\mathbb{R}[x]$ is rather like multiplication in $\mathbb{Z}$. As in $\mathbb{Z}$, we define a notion of "divisibility": we write $a(x) \mid b(x)$ if there is some $c(x)$ such that $b(x) = a(x)c(x)$. Like $\mathbb{Z}$, and unlike $\mathbb{N}$, this relation in **not** antisymmetric. In $\mathbb{Z}$ we have that if $a \mid b$ and $b \mid a$ then $a = \pm b$. In $\mathbb{R}[x]$, we have that if $a(x) \mid b(x)$ and $b(x) \mid a(x)$ then $a(x) = cb(x)$ for some $c \neq 0$.

Thursday: The Euclidean Algorithm in $\mathbb{R}[x]$

In $\mathbb{Z}$ we use the Euclidean Algorithm to find greatest common divisors. What makes this possible is the Division Algorithm.

Since we also have the Division Algorithm in $\mathbb{R}[x]$, we can use a similar process to find greatest common divisors in $\mathbb{R}[x]$.

Example 6. *Find the greatest common divisor of* $a(x) = 2x^3 + x^2 - 2x - 1$ *and* $b(x) = x^3 - x^2 + 2x - 2$.

Solution. We use the Euclidean Algorithm: first divide $b(x)$ into $a(x)$, then divide the remainder into $b(x)$, then divide this new remainder into the first one, and so on. The last non-zero remainder is the greatest common divisor.

We have

$$\begin{aligned} 2x^3 + x^2 - 2x - 1 &= 2(x^3 - x^2 + 2x - 2) + (3x^2 - 6x + 3) \\ x^3 - x^2 + 2x - 2 &= (\tfrac{1}{3}x + \tfrac{1}{3})(3x^2 - 6x + 3) + (3x - 3) \\ 3x^2 - 6x + 3 &= (x - 1)(3x - 3) \end{aligned}$$

So the last non-zero remainder is $d(x) = 3x - 3$. □

Theorem 7 (The Factor Theorem). *Let* $p(x) \in \mathbb{R}[x]$*, and let* $a \in \mathbb{R}$*. Then* $(x - a) \mid p(x)$ *if and only if* $p(a) = 0$*.*

Proof. Suppose first that $(x - a) \mid p(x)$. Then there is some $q(x)$ such that $p(x) = q(x)(x - a)$. But then $p(a) = q(a)(a - a) = 0$.

Conversely, suppose that $p(a) = 0$. By the Division Algorithm in $\mathbb{R}[x]$, we can find polynomials $q(x)$ and $r(x)$ with $\deg r(x) < 1$ such that $p(x) = q(x)(x - a) + r(x)$. Now, since $\deg r(x) < 1$, $r(x)$ is a constant. Also, we have $p(a) = q(a)(a - a) + r(a)$, in other words $0 = q(a) \cdot 0 + r(a)$, so $r(a) = 0$. Hence $r(x) = 0$, so we have $p(x) = q(x)(x - a)$, so $(x - a) \mid p(x)$. □

Irreducible polynomials in $\mathbb{R}[x]$

Definition. *A polynomial* $p(x) \in \mathbb{R}[x]$ *is* reducible *in* $\mathbb{R}[x]$ *if it can be factorised as* $p(x) = a(x)b(x)$*, where* $a(x), b(x) \in \mathbb{R}[x]$ *with* $\deg a(x) < \deg p(x)$ *and* $\deg b(x) < \deg p(x)$*. It is* irreducible *in* $\mathbb{R}[x]$ *if it is not reducible in* $\mathbb{R}[x]$*.*

When we say that a polynomial is irreducible, we must specify over what field of coefficients. For example, the polynomial $x^2 + 1$ is irreducible in $\mathbb{R}[x]$, but it can be factorised as $(x - i)(x + i)$ in $\mathbb{C}[x]$.

Exercise 8. *Show that every linear polynomial* $ax + b$ *(with* $a \neq 0$*) is irreducible.*

The irreducible polynomials in $\mathbb{R}[x]$ play the same rôle in $\mathbb{R}[x]$ that the primes play in $\mathbb{Z}$: every polynomial of degree greater than 0 can be written as a product of (one or more) irreducible polynomials. Moreover, as with uniqueness of prime factorisations in $\mathbb{Z}$, the factorisation of a polynomial as a product of irreducibles is unique (up to the order of the elements, and multiplication by constants).

Friday: Groups

Definition. *Let $*$ be a binary operation on a set A with identity element e. Let $a \in A$. Then b is an* inverse *of a if $a * b = b * a = e$.*

Example 9. *The inverse of a real number x under the operation $+$ is the number $-x$: we have $x+(-x) = (-x) + x = 0$.*

Definition. *A* group *is a pair $(G, *)$ where $*$ is a binary operation on G such that*

- *for any $a, b, c \in G$, $a * (b * c) = (a * b) * c$;*
- *there is some $e \in G$ such that, for every $a \in G$, $a * e = e * a = a$; and*
- *for any $a \in G$ there is some $b \in G$ with $a * b = b * a = e$.*

We often abuse notation and refer to "the group G" instead of "the group $(G, *)$".

Example 10. *The integers form a group under addition, in other words $(\mathbb{Z}, +)$ is a group. The non-zero real numbers for a group under multiplication, in other words $(\mathbb{R} \setminus \{0\}, \cdot)$ is a group.*

Proposition 11. *The inverse of a is unique. In other words, if $a * b = b * a = e$ and $a * c = c * a = e$ then $b = c$.*

Because of this uniqueness, we can denote the inverse of an element a by a^{-1}.

Proposition 12. *If $(G, *)$ is a group and $a, b, c \in G$ with $a * b = a * c$ then $b = c$.*

This is sometimes called the *cancellation law*.

Cayley tables

If $*$ is a binary operation on a finite set, we can write down a "multiplication table" for $*$. For example, we can define an operation $*$ on the set $G = \{e, a, b, c\}$ by the following table:

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

We call this the *Cayley table* of the operation.

Exercise 13. *Show that if $*$ is defined by the above table then $(G, *)$ is a group.*

Proposition 14. *Each element of G occurs exactly once in each row and each column of the Cayley table of a group operation.*

Proposition 15. *Let $(G, *)$ be a group with identity element e.*

1. *If $x \in G$ satisfies $x * x = x$, then $x = e$.*
2. *If $x, y \in G$ satisfy $x * y = y$, then $x = e$. [Put another way, if $x * y = y$ for* some *$y \in G$ then $x * y = y$ for* every *$y \in G$.]*

Exercise 16. *Given that $\oplus$ is a group operation on the set $G = \{p, q, r, s\}$, complete the following Cayley table:*

$\oplus$	p	q	r	s
p	r			
q		q		
r				
s				