Tying up Loose Ends

Math 4400, Summer 2017

These notes are meant to supplement the course text. They discuss some basic ring/group theory that is used later in the book, but not really discussed anywhere in detail.

1 Polynomial rings

Let R be a ring. For simplicity's sake, we'll assume always assume that R is commutative in these notes. We can use R to build a new ring, called the ***ring of polyonomials over*** R, and denoted $R[X]$. As a set, $R[X]$ is defined to be:

$$R[X] = \left\{ \sum_{i=0}^{n} a_i X^i \;\middle|\; n \in \mathbb{N}, \text{ and } a_i \in R \text{ for all } i \right\}$$

Addition and multiplication in $R[X]$ are defined in the usual way that we define addition and multiplication of polynomials: if $f = \sum_{i=0}^{n} a_i X^i$ and $g = \sum_{i=0}^{m} b_i X^i$, then

$$f + g = \sum_{i=0}^{\max(m,n)} (a_i + b_i) X^i \qquad f \cdot g = \sum_{i=0}^{m+n} \sum_{j=0}^{i} a_j b_{i-j} X^i$$

(we define $a_i = 0$ for $i > n$ and $b_i = 0$ for $i > m$)

If $f = \sum_{i=0}^{n} a_i X^i$ is an element of $R[X]$, then the ***degree*** of f is defined to be $\max\{i \in \mathbb{N} \mid a_i \neq 0\}$. If $a_i = 0$ for all i, then $f = 0_R$, and the degree of f is defined to be $-\infty$. The degree of f is denoted $\deg f$. If $n = \deg f \geq 0$, then a_n is called the ***leading coefficient*** of f.

Example. $\mathbb{Z}[X]$ is the set of polynomials with integer coefficients. Elements include $3X^5 - 6$ and $X + 1$. As usual,

$$(3X^5 - 6) + (X + 1) = 3X^5 + X - 5$$

and

$$(3X^5 - 6) \cdot (X + 1) = 3X^6 + 3X^5 - 6X - 6$$

□

Example. Let $R = \mathbb{Z}/5\mathbb{Z}$. Then $R[X]$ is the set of polynomials with coefficients in $\mathbb{Z}/5\mathbb{Z}$. For instance, $[1]X^2 + [2]$ and $[3]X^3 + [4]X^2 + [1]X$ are elements of $R[X]$. In this ring,

$$([1]X^2 + [2]) + ([3]X^3 + [4]X^2 + [1]X) = [3]X^3 + [5]X^2 + [1]X + [2]$$

But $[5] = [0]$ in $\mathbb{Z}/5\mathbb{Z}$, so

$$([1]X^2 + [2]) + ([3]X^3 + [4]X^2 + [1]X) = [3]X^3 + [0]X^2 + [1]X + [2]$$

It's a little silly to write things this way, though. Usually we omit the "$[0]X^2$" and the [1]s:

$$(X^2 + [2]) + ([3]X^3 + [4]X^2 + X) = [3]X^3 + X + [2]$$

Similarly,

$$\begin{aligned}([1]X^2+[2])\cdot([3]X^3+[4]X^2+[1]X) &= X^2\cdot([3]X^3+[4]X^2+X)+[2]\cdot([3]X^3+[4]X^2+X)\\ &= [3]X^5+[4]X^4+[7]X^3+[8]X^2+[2]X\\ &= [3]X^5+[4]X^4+[2]X^3+[3]X^2+[2]X\end{aligned}$$

□

Example. Let $R = \mathbb{Z}/2\mathbb{Z}$. Then $X + [1] \in \mathbb{R}/2\mathbb{Z}$ and

$$(X + [1])^2 = X^2 + [2]X + [1] = X^2 + [1]$$

□

Given a polynomial $f \in R[X]$, we can "plug in" elements of R into f as usual. More precisely, f defines a function $\widetilde{f} : R \to R$, defined as follows: if $f = \sum_{i=0}^{n} a_i X^i$ and $r \in R$, then $\widetilde{f}(r) = \sum_{i=0}^{n} a_i r^i \in R$. The ring element $\widetilde{f}(r)$ is called ***the evaluation of*** f ***at*** r

Remark. I don't think anyone else actually uses the notation $\widetilde{f}$. Usually, the function corresponding to a polynomial f is just denoted by f as well. I used the notation $\widetilde{f}$ to emphasize that polynomials and their corresponding functions are not the same thing. This is a confusing, but important point. In fact, it's worth repeating:

Caution. A polynomial $f \in R[X]$ and its corresponding function $\widetilde{f} : R \to R$ are different things. Moreover, **different polynomials can have the same corresponding function!** For example, let p be a prime number, and let $R = \mathbb{Z}/p\mathbb{Z}$. Then $f = X^p + [-1]X$ and $g = [0]$ are two different elements of $R[X]$. However, Fermat's little theorem tells us that $r^p = r$ for all $r \in \mathbb{Z}/p\mathbb{Z}$. Thus $\widetilde{f}(r) = r^p + [-1]r = r - r = [0]$ for all $r \in \mathbb{Z}/p\mathbb{Z}$. On the other hand $\widetilde{g}(r) = [0]$ for all $r \in \mathbb{Z}/p\mathbb{Z}$. So $\widetilde{f}$ and $\widetilde{g}$ are the same function, even though f and g are different polynomials!

Let R be a ring, and f a polynomial in $R[X]$. An element r of R is called a ***root*** of f if $\widetilde{f}(r) = 0_R$. Our next goal is to prove the following, very important theorem:

Theorem 1.1 (Important theorem!)**.** *Let k be a field, and let $f \in k[X]$. If $d = \deg f$, then f has at most d roots in k.*

To prove this, we start by noting that there's a division algorithm for polynomials over a field:

Lemma 1.2. *Let k be a field and let $f, g \in k[X]$ with $f, g \neq 0$. Then there exist unique $q, r \in k[X]$ such that $\deg r < \deg g$, and $f = qg + r$.*

The proof of this lemma is essentially the same as the proof of the division algorithm for integers, so I'll postpone it until the end of the section for those who are interested. We'll also need the following two lemmas:

Lemma 1.3. *Let $f \in k[X]$ and suppose α is a root of f. Then $f = g \cdot (X - \alpha)$ for some $g \in k[X]$*

Proof. By Lemma 1.2, there exist $g, r \in k[X]$ such that

$$f = g \cdot (X - \alpha) + r \tag{1}$$

and $\deg r < \deg(X - \alpha) = 1$. Thus $\deg r = 0$ or $\deg r = -\infty$. In either case, we know $r \in k$. Then, evaluating both sides of equation 1 at α, we get

$$f(\alpha) = g(\alpha)(\alpha - \alpha) + r(\alpha) = g(\alpha) \cdot 0 + r = r$$

But α is a root of f, so $f(\alpha) = 0$. Thus $r = 0$ and $f = g \cdot (X - \alpha)$. □

Lemma 1.4. *Let R be a commutative ring without zero divisors (e.g. R can be any field), and let $f, g \in R[X]$. Then* $\deg(f \cdot g) = \deg(f) + \deg(g)$.

Proof. We define $n \cdot -\infty = -\infty \cdot n$ for all $n \in \mathbb{N}$, and this takes care of the case that $f = 0$ or $g = 0$. So assume $f \neq 0$ and $g \neq 0$. So let $\deg f = n \geq 0$ and $\deg g = m \geq 0$. Then we can write $f = \sum_{i=0}^{n} a_i X^i$ and $g = \sum_{i=0}^{m} b_i X^i$ for some $a_i, b_i \in R$. Then $f \cdot g = \sum_{i=0}^{m+n} c_i X^i$, where

$$c_i = \sum_{j=0}^{i} a_j b_{i-j}$$

for all i. Thus $c_{n+m} = a_n b_m \neq 0$, since $a_n \neq 0$, $b_m \neq 0$, and R doesn't have zero-divisors. This proves the lemma. □

Caution. This lemma doesn't hold for polynomials over an arbitrary ring. For instance, let $R = \mathbb{Z}/6\mathbb{Z}$. If $f = 2X^2 + 1$ and $g = 3X$ are elements of $R[X]$, then $fg = 3X$, so $\deg(fg) = 1 < \deg f + \deg g$. In general, if R is any ring and f and g are any elements of $R[X]$, the most we can say is that $\deg(fg) \leq \deg f + \deg g$.

Proof of Theorem 1.1. We prove this by induction on the degree of f. If $\deg f = 0$, then f is some nonzero constant, so it has no roots. Now let $d \in \mathbb{N}$ and suppose the theorem is true for polynomials of degree d. Let f be a polynomial of degree $d + 1$. We wish to show that f has at most $d + 1$ roots. If f has no roots, then we're done since $0 \leq d + 1$. Otherwise, f has some root r. By Lemma 1.3, we can write $f = g \cdot (X - r)$ for some polynomial g. By Lemma 1.4, we have $\deg g + 1 = \deg f$, so $\deg g = d$. Now suppose that s is a root of f. That means $f(s) = g(s) \cdot (s - r) = 0$. Since k is a field, this means either $g(s) = 0$ or $s - r = 0$. In other words, either s is a root of g or $s = r$. Thus the set of all roots of f is $\{\text{roots of g}\} \cup \{r\}$. But, by the inductive hypothesis, g has at most d roots. Thus f has at most $d + 1$ roots □

1.1 Division algorithm

Here we prove the division algorithm for polynomials over a ring. Here is its most general guise:

Theorem 1.5 (Division algorithm for polynomials)**.** *Let R be a commutative ring without zero-divisors, and let $f, g \in R[X]$. If the leading coefficient of g has a multiplicative inverse in R, then there exist unique $q, r \in R[X]$ such that $f = gq + r$, and* $\deg r < \deg g$.

Proof. First we consider the issue of existence. If $f = gq$ for some $q \in R[X]$, then we're done, so we may assume that $f \neq gq$ for any $q \in R[X]$. Then consider the set $S = \{\deg(f - gh) \mid h \in R[X]\}$. This is a nonempty subset of the natural numbers. By the well-ordering principle, S must have a minimal element d. Let $h_0 \in R[X]$ be the polynomial such that $\deg(f - gh_0) = d$, and set $r = f - gh_0$. I claim that $\deg r < \deg g$. To see this, suppose otherwise. Set $n = \deg g$. Then $g = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ for some $a_0, \cdots, a_n \in R$. By assumption, a_n is invertible in R. Similarly, $r = b_d X^d + b_{d-1} X^{d-1} + \cdots + b_0$ for some $b_0, \cdots, b_d \in R$. Let $r' = r - a_n^{-1} b_d X^{d-n} g$. Then r' has degree at most d, even though $r' = f - g\left(h + a_n^{-1} b_d X^{d-n}\right)$ is of the form f minus something times g. This contradicts the minimality of $\deg r$ and proves existence.

As for uniqueness, suppose $q_1 g + r_1 = q_2 g + r_2$, with $\deg r_1, \deg r_2 < \deg g$. Then $g(q_1 - q_2) = r_1 - r_2$, so either $r_1 - r_2 = 0$ or $\deg(r_1 - r_2) \geq \deg g$. But $\deg(r_1 - r_2) \leq \max(\deg r_1, \deg r_2) < g$. Thus $r_1 = r_2$, and so $g(q_1 - q_2) = 0$. Since $\deg g > -\infty$, Lemma 1.4 tells us that $q_1 = q_2$. This proves uniqueness. □

Note that fields are commutative rings without zero-divisors, so the above theorem holds whenever R is a field. In that case, g can be any nonzero polynomial, and the hypotheses on g will be satisfied.

2 Groups, rings, and functions

Our next object of study is the set of functions between two groups. Consider the groups $(\mathbb{Z}/3\mathbb{Z}, +)$ and $(\mathbb{Z}/9\mathbb{Z}, +)$. There are many functions from one set to the other. For instance, we could define a function $f : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/9\mathbb{Z}$ by setting $f([0]_3) = [4]_9$, $f([1]_3) = [7]_9$, and $f([2]_3) = [2]_9$. However, most functions, like the one above, are not very interesting—they have nothing to do with the group structures on $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z}$! On the other hand, some functions are nice. For instance, the following function,

$$f : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/9\mathbb{Z},\ [n]_3 \mapsto [3n]_9$$

is a nice function: for instance, it satisfies

$$f(a + b) = f(a) + f(b)$$

for all $a, b \in \mathbb{Z}/3\mathbb{Z}$. We give a special name to such functions:

Definition 1. *Let $(G, \cdot)$ and $(H, *)$ be two groups. A* **group homomorphism** *from G to H is a function $f : G \to H$ satisfying*

$$f(g_1 \cdot g_2) = f(g_1) * f(g_2)$$

for all $g_1, g_2 \in G$.

A homomorphism is a lot like a linear transformation from linear algebra.

Example. The function $f : \mathbb{Z} \to \mathbb{Z}$, given by $f(x) = 3x$, is a homomorphism from $(\mathbb{Z}, +)$ to itself. Indeed,

$$f(a + b) = 3(a + b) = 3a + 3b = f(a) + f(b)$$

□

Example. The function $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(n) = n + 1$ is *not* a homomorphism, as $f(a+b) \neq f(a) + f(b)$. Indeed, for all $a, b \in \mathbb{Z}$, $f(a+b) = a+b+1$, whereas $f(a) + f(b) = a + 1 + b + 1 = a + b + 2$. □

Example. The set $P = \{x \in \mathbb{R} \mid x > 0\}$ forms a group under multiplication. The function $f : \mathbb{Z} \to P$ given by $f(n) = \exp(n)$ is a homomorphism, as $f(n+m) = \exp(n+m) = \exp(n) \cdot \exp(m)$ for all $n, m \in \mathbb{Z}$. □

Example. Let $(G, \cdot)$ and $(H, *)$ be two groups, and let e_H be the identity element of H. Then the function, $f : G \to H$ sending each element of G to e_H is a homomorphism. Indeed, for all $g_1, g_2 \in G$, $f(g_1 \cdot g_2) = e_H$ and $f(g_1) * f(g_2) = e_H * e_H = e_H$. Thus $f(g_1 \cdot g_2) = f(g_1) * f(g_2)$, so f is a homomorphism. □

Similarly, a "nice" function between two rings is also called a homomorphism. Rings have more structure than groups, however, so a function between two rings has to satisfy more requirements to be considered "nice":

Definition 2. *Let $(R, +_R, \cdot_R)$ and $(S, +_S, \cdot_S)$ be two rings. Then a function $f : R \to S$ is called a* **ring homomorphism** *if:*

- $f(r_1 +_R r_2) = f(r_1) +_S f(r_2)$
- $f(r_1 \cdot_R r_2) = f(r_1) \cdot_S f(r_2)$,
- $f(1_R) = 1_S$

Example. Let n be a positive integer. Then the function $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto [x]_n$ is a ring homomorphism. Indeed, $f(x+y) = [x+y]_n = [x]_n + [y]_n = f(x) + f(y)$, $f(x \cdot y) = [x \cdot y]_n = [x]_n \cdot [y]_n = f(x) \cdot f(y)$, and $f(1) = [1]_n$, which is indeed the multiplicative identity of $\mathbb{Z}/n\mathbb{Z}$. □

Example. Let k be a field of characteristic p. The frobenius map $\mathrm{Frob} : k \to k$, defined as $\mathrm{Frob}(x) = x^p$, is a ring homomorphism from k to itself. □

2.1 Isomorphisms

Sometimes two groups can really be the same, even if they look different. For instance, consider the following two groups: one group is $\mathbb{Z}/4\mathbb{Z}$ under addition, and the other is the set, $G = \{I, A, B, C\}$ under matrix multiplication, where

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, D = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Clearly, $\mathbb{Z}/4\mathbb{Z}$ and G are two different sets, so $\mathbb{Z}/4\mathbb{Z}$ and G are not literally the same group. However, they have quite a similar structure:

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\cdot$	I	A	B	C
I	I	A	B	C
A	A	B	C	I
B	B	C	I	A
C	C	I	A	B

These two tables are basically the same table but labeled differently: if you take the table on the left and replace each [0] with an I, each [1] with A, each [2] with B, and each [3] with C, then you get the table on the right. In this sense, the groups G and $\mathbb{Z}/4\mathbb{Z}$ have exactly the same "structure." This leads to the following deinitions:

Definition 3. *Let G and H be two groups. A function $f : G \to H$ is called a* **group isomorphism** *if:*

- *f is a group homomorphism, and*
- *f is a bijection*

We define ***ring isomorphisms*** in exactly the same way: just replace each instance of "group" in the definition above with "ring". Two groups/rings are said to be ***isomorphic*** if there exists an isomorphism from one to the other. This means they have the same structure.

Example. In the example above (right before the definition), the function $f : \mathbb{Z}/4\mathbb{Z} \to G$ defined by $f([0]) = I, f([1]) = A, f([2]) = B, f([3]) = C$ is an isomorphism: clearly, f a bijection, and our discussion above about the multiplication tables of $\mathbb{Z}/4\mathbb{Z}$ and G shows that f is a homomorphism. Thus, $\mathbb{Z}/4\mathbb{Z}$ and G are isomorphic. We usually use the symbol $\cong$ to mean "isomorphic". So we write $\mathbb{Z}/4\mathbb{Z} \cong G$. □

Example. Let $\mathbb{R}$ be the group of real numbers under addition, and let $\mathbb{R}^+$ be the group of positive real numbers under multiplication. Then the function $\exp : \mathbb{R} \to \mathbb{R}^+$ is an isomorphism. This function is a homomorphism, since $\exp(a + b) = \exp(a) \cdot \exp(b)$ for all $a, b \in \mathbb{R}$, so we just have to show exp is a bijection. In other words, given any $y \in \mathbb{R}^+$, we must show there exists a unique $x \in \mathbb{R}$ such that $\exp(x) = y$. This unique x is given by $\ln(y)$, so we're done. □