

# FIELDS AND POLYNOMIALS

MATH 372. FALL 2005. INSTRUCTOR: PROFESSOR AITKEN

## 1. FIELDS

In class, the definitions of *commutative ring* and *Abelian group* were given. Examples of commutative rings, which you have seen before this class, include the set of integers  $\mathbb{Z}$ , the set of rational numbers  $\mathbb{Q}$ , the set of real numbers  $\mathbb{R}$ , and the set of complex numbers  $\mathbb{C}$ . New examples, taught in this class, are the sets  $\mathbb{Z}_m$  of integers modulo  $m$  where  $m \geq 1$ . (If  $m = 1$  then  $\mathbb{Z}_m$  is called the *trivial ring* because  $\bar{0} = \bar{1}$ .)

**Definition 1.** A *field*  $F$  is a commutative ring with the following properties: (i)  $F$  is not trivial in the sense that  $0 \neq 1$ , and (ii) every non-zero element of  $F$  has a multiplicative inverse in  $F$ . In other words, the unit group consists of exactly the non-zero elements of  $F$ .

Examples of fields include  $\mathbb{Q}$ ,  $\mathbb{R}$ , and  $\mathbb{C}$ . Note that  $\mathbb{Z}$  is not a field since there are integers, for example  $3 \in \mathbb{Z}$ , whose multiplicative inverse, for example  $1/3 \in \mathbb{Q}$ , is not in  $\mathbb{Z}$ . Another example is  $\mathbb{Z}_p$ :

**Theorem 1.** *If  $p$  is a prime, then  $\mathbb{Z}_p$  is a field. If  $m \geq 1$  is not a prime, then  $\mathbb{Z}_m$  is not a field.*

*Proof.* Let  $p$  be a prime. Since  $p > 1$ , we have that  $\bar{1} \neq \bar{0}$  in  $\mathbb{Z}_p$  (since  $p$  does not divide 1). We now show that every non-zero element has an inverse. Suppose  $\bar{a} \neq \bar{0}$ , in other words suppose  $p$  does not divide  $a$ . Then the only possible common divisor of  $p$  and  $a$  is 1. Thus  $1 = (p, a)$ . From an earlier theorem, this implies that  $\bar{a}$  has an inverse. Since  $\mathbb{Z}_p$  is not the trivial ring and since every non-zero element is invertible, it is a field.

Suppose that  $m \geq 1$  is not a prime. If  $m = 1$  then  $\bar{1} = \bar{0}$  since  $m \mid 1$ . Thus  $\mathbb{Z}_m$  is the trivial ring, which is not considered a field. If  $m > 1$  is not a prime, it must have a divisor  $d$  such that  $1 < d < m$ . Obviously  $(m, d) = d > 1$ . So  $\bar{d}$  is a non-zero element without an inverse (this follows from an earlier theorem). Thus  $\mathbb{Z}_m$  is not a field.  $\square$

*Remark.* If  $p$  is a prime, then  $\mathbb{Z}_p$  is often written  $\mathbb{F}_p$  to emphasize that it is a field.

## 2. POLYNOMIAL RINGS

Let  $R$  be a commutative ring. Then  $R[x]$  signifies the set of polynomials  $a_n x^n + \dots + a_1 x + a_0$  with coefficients  $a_i \in R$ . For example,  $7x^3 - 3x^2 + 11$  is in  $\mathbb{Z}[x]$ , which is also in  $\mathbb{Q}[x]$ , in  $\mathbb{R}[x]$ , and in  $\mathbb{C}[x]$  since  $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ . Observe that  $\frac{7}{11}x^3 - 3x^2 + 11$  is in  $\mathbb{Q}[x]$  but not in  $\mathbb{Z}[x]$ . Observe that  $7x^3 - \sqrt{2}x^2 + x - 11$  is in  $\mathbb{R}[x]$  but not in  $\mathbb{Q}[x]$ .

If  $a_n x^n + \dots + a_1 x + a_0$  is a polynomial with coefficients  $a_i$ , we adopt the convention that  $a_i = 0$  for all values of  $i$  not occurring in the expression  $a_n x^n + \dots + a_1 x + a_0$ . For example, when writing  $7x^3 + x - 11$  as  $a_n x^n + \dots + a_1 x + a_0$ , then we consider  $a_2 = 0$  and  $a_4 = 0$ , but

$a_3 = 7$  and  $a_0 = 11$ , etc. Two polynomials  $a_n x^n + \dots + a_1 x + a_0$  and  $b_k x^k + \dots + b_1 x + b_0$  are defined to be equal if  $a_i = b_i$  for all  $i \geq 0$ .

For example,  $\bar{6}x^3 + \bar{2}x^2 - x + \bar{1} = -x^2 + \bar{2}x + \bar{1}$  in  $\mathbb{Z}_3[x]$ .

Among the polynomials in  $R[x]$  are the *constant* polynomials  $a_0$ . In other words,  $a_0 \in R$  it can be thought of as both an element of  $R$  and as a constant polynomial in  $R[x]$ . Thus  $R \subset R[x]$ .

We define multiplication and addition of polynomials in the usual way. (I will skip the details of the definition since these procedures are so familiar). Both operations are closed on  $R[x]$ . For example, in  $\mathbb{Z}_6[x]$  the product of  $\bar{2}x^2 + \bar{3}x + \bar{1}$  with  $\bar{3}x^2 + \bar{2}$  can be computed as follows

$$(\bar{2}x^2 + \bar{3}x + \bar{1})(\bar{3}x^2 + \bar{2}) = \bar{6}x^4 + \bar{4}x^2 + \bar{9}x^3 + \bar{6}x + \bar{3}x^2 + \bar{2} = \bar{3}x^3 + x^2 + \bar{2}.$$

As an exercise, try multiplying  $\bar{2}x^2 + \bar{3}x + \bar{1}$  by  $\bar{3}x^2 + \bar{x} - \bar{2}$  in  $\mathbb{Z}_5[x]$ .

Now, multiplication and addition are defined on  $R[x]$  and are closed in the sense that the result is in  $R[x]$ . So  $+$  and  $\times$  give two binary operations. These operations are associative and commutative (we skip the proofs). The distributive law holds between them. The constant polynomials  $0$  and  $1$ , given by  $0, 1 \in R$ , are respectively the additive and multiplicative identities. Given a polynomial  $f$ , when we multiply each coefficient by  $-1$  we get another polynomial  $-f$  such that  $f + (-f) = 0$ . These properties taken together give us the following:

**Theorem 2.** *Let  $R$  be a commutative ring. Then the set  $R[x]$  is a commutative ring under the usual addition and multiplication.*

If  $f \in R[x]$  then  $f(a)$  denotes what we get when we substitute  $a$  for  $x$  in  $f$ . It is defined whenever the substitution makes sense. For example,  $f(x)$  is just  $f$  itself since when we replace  $x$  with  $x$  we get what we started with. So some authors write  $f(x)$  while others write  $f$ . I will write  $f(x)$  whenever I want to remind you that  $f$  is a polynomial in  $x$ . Another example, if  $f = x^2 + \bar{1}$  in  $\mathbb{Z}_8[x]$  then  $f(\bar{3}) = \bar{2}$ . Another example, if  $f = x^3$  in  $\mathbb{Z}_{12}[x]$  then  $f(x + \bar{2}) = (x + \bar{2})^3 = x^3 + \bar{6}x^2 + \bar{8}$ . (Did you see what happened to the linear term?). If  $f \in R[x]$ , and  $y$  is another variable, then  $f(y)$  is in  $R[y]$  and has the same coefficients. However, if  $x$  and  $y$  are different variables, then  $f(x)$  is not considered to be equal to  $f(y)$  (although if  $f$  is a constant polynomial, you can consider them to be equal in the common subring  $R$ ). If  $f = c$  is a constant polynomial, then  $f(a) = c$  for all  $a \in R$ . Observe that if  $a \in R$  and  $f \in R[x]$  then  $f(a) \in R$ . Addition and multiplication were defined in such a way to make the following true:  $(f + g)(a) = f(a) + g(a)$  and  $(f \cdot g)(a) = f(a) \cdot g(a)$  for all  $a \in R$ .

Here is an amusing example. Let  $f = x^3 - x \in \mathbb{Z}_3[x]$ . Then  $f(\bar{0}) = \bar{0}$ ,  $f(\bar{1}) = \bar{0}$ , and  $f(\bar{2}) = \bar{0}$ . So  $f(a) = \bar{0}$  for all  $a \in \mathbb{Z}_3$  but  $f \neq \bar{0}$ . So polynomials cannot be treated as functions when  $R$  is finite: two distinct polynomials, for example,  $f$  and  $\bar{0}$  above, can have identical values. This cannot happen for functions.

**Definition 2.** An element  $a \in R$  is called a *root* of  $f \in R[x]$  if  $f(a) = 0$ . The above example is amusing: every element of  $\mathbb{Z}_3$  is a root of  $x^3 - x \in \mathbb{Z}_3[x]$ .

### 3. THE QUOTIENT-REMAINDER THEOREM FOR POLYNOMIALS

If  $F$  is a field, then  $F[x]$  shares some properties with  $\mathbb{Z}$ . For example, the Quotient-Remainder Theorem. To state this theorem we need to discuss a notion of size for  $F[x]$  traditionally called the *degree*:

**Definition 3.** Let  $f \in R[x]$  where  $R$  is a commutative ring. If  $f = a_n x^n + \dots + a_1 x + a_0$  with  $a_n \neq 0$  then the *degree* of  $f$  is defined to be  $n$  and the *leading coefficient* is defined to be  $a_n$ . If  $f = 0$  then the degree of  $f$  is not defined as an integer (some authors define it to be  $-\infty$ ).

Be careful when using this definition modulo  $m$ . For example,  $\bar{6}x^3 + \bar{2}x^2 - x + \bar{1}$  only has degree 2 when interpreted as an element in  $\mathbb{Z}_3[x]$ , and only has degree 1 when interpreted as an element in  $\mathbb{Z}_2[x]$ . It has degree 3 when interpreted as an element in  $\mathbb{Z}_5$ .

You would hope that the degree of  $fg$  would be the sum of the degrees of  $f$  and  $g$  individually. However, examples such as  $(\bar{2}x^2 + \bar{3}x + \bar{1})(\bar{3}x^2 + \bar{2}) = \bar{3}x^3 + x^2 + \bar{2}$  in  $\mathbb{Z}_6[x]$  spoil our optimism. However, if the coefficients are in a field  $F$  then it works.

**Proposition 1.** *If  $f, g \in F[x]$  are non-zero polynomials where  $F$  is a field, then*

$$\deg(fg) = \deg f + \deg g.$$

*Proof.* I won't give the proof (now), but will let you think about it. It is not hard. □

*Remark.* This equation also holds for polynomials whose coefficients are not in a field as long as the leading coefficients are not zero divisors.

As mentioned above, the degree of a polynomial is a measure of size. When we divide we want the size of the remainder to be smaller than the size of the quotient. This leads to the following:

**Theorem 3** (Quotient-Remainder Theorem for Polynomials). *Let  $f, g \in F[x]$  be polynomials where  $F$  is a field. Assume  $g$  is not zero. Then there are unique polynomials  $q(x)$  and  $r(x)$  such that (i)  $f(x) = q(x)g(x) + r(x)$ , and (ii) the polynomial  $r(x)$  either the zero polynomial or has degree strictly smaller than  $g(x)$ .*

*Remark.* The polynomial  $q(x)$  in the above is called the *quotient* and the polynomial  $r(x)$  is called the *remainder*.

*Remark.* This theorem actually holds for polynomials in  $R[x]$  where  $R$  is a commutative ring that is not a field, as long as we add the extra assumption that the leading coefficient of  $g$  is a unit in  $R$ .

*Remark.* We can use this theorem to prove theorems about GCD's and unique factorization in  $F[x]$  just as we did for  $\mathbb{Z}$ .

As an important special case, consider  $g(x) = x - a$  where  $a \in R$ . Then  $r(x)$  must be zero, or have degree zero. So  $r = r(x)$  is a constant:  $r \in R$ . What is this constant? Well  $f(x) = q(x)(x - a) + r$  so when we substitute  $x = a$  we get

$$f(a) = q(a)(a - a) + r = 0 + r = r.$$

In other words,  $r = f(a)$ . This gives the following:

**Corollary 1.** *Let  $a \in F$  where  $F$  is a field, and let  $f \in F[x]$ . Then there is a  $q \in F[x]$  such that*

$$f(x) = (x - a)q(x) + f(a).$$

*Remark.* This actually works for commutative rings as well as for fields  $F$  since the leading coefficient of  $g(x) = x - a$  is 1 which is always a unit.

#### 4. A THEOREM OF LAGRANGE

As you learned long ago, a polynomial  $f$  with coefficients in  $\mathbb{R}$  (or  $\mathbb{Q}$  or  $\mathbb{C}$ ) has at most  $\deg f$  roots. You probably do not remember the proof which we give now.

**Theorem 4.** *Let  $f \in F[x]$  be a non-zero polynomial with coefficients in a field  $F$ . Then  $f$  has at most  $\deg f$  roots in  $F$ .*

*Proof.* This is proved by induction. The induction statement is as follows: *if  $f$  has degree  $n$  then  $f$  has at most  $n$  roots in  $F$ .* The case  $n = 0$  is easy. In this case  $f$  is a non-zero constant polynomial which obviously has no roots.

Suppose that the statement is proved for  $n = k$ . We want to prove it for  $n = k + 1$ . To do so, let  $f$  be a polynomial of degree  $k + 1$ . If  $f$  has no roots, then the statement is trivially true. Suppose that  $f$  does have a root  $a \in F$ . Then, by Corollary 1,

$$f(x) = q(x)(x - a) + f(a) = q(x)(x - a) + 0 = q(x)(x - a).$$

By Proposition 1,  $\deg f = \deg(x - a) + \deg q$ . But  $\deg(x - a) = 1$ . So  $\deg q = k$ . By the inductive hypothesis,  $q$  has at most  $k$  roots. Now suppose that  $f$  has a root  $b \neq a$ . Then  $0 = f(b) = q(b)(b - a)$ . Since  $b - a \neq 0$ , we can multiply both sides by the inverse:  $0(b - a)^{-1} = q(b)(b - a)(b - a)^{-1}$ . Thus  $0 = q(b)$ . So every root of  $f$  not equal to  $a$  must be a root of  $q(x)$ . Since  $q(x)$  has at most  $k$  roots, it follows that  $f(x)$  must have at most  $k + 1$  roots.  $\square$

The following is usually attributed to Lagrange.

**Corollary 2** (Lagrange). *Let  $f \in \mathbb{F}_p[x]$  be a non-zero polynomial with coefficients considered modulo  $p$  where  $p$  is a prime. Then  $f$  has at most  $\deg f$  roots in  $\mathbb{F}_p$ .*

*Proof.* It follows from the previous theorem since  $\mathbb{F}_p$  is a field.  $\square$

*Remark.* Observe how this can fail if  $m$  is not a prime. The polynomial  $x^2 - \bar{1} \in \mathbb{Z}_8$  has degree 2, yet it has four roots! (Can you find them?)

Of course, Lagrange and Gauss would have stated (and proved) Corollary 2 differently since the concept of a field is essentially a twentieth century idea. They might have said something closer to

*If  $p$  is a prime and  $f(x)$  is a polynomial with integer coefficients not all divisible by  $p$ , then the congruence  $f(x) \equiv 0 \pmod{p}$  has at most  $\deg f$  solutions modulo  $p$ .*

or

*If  $p$  is a prime and  $f(x)$  is a polynomial with integer coefficients not all divisible by  $p$ , then  $p \mid f(a)$  for at most  $\deg f$  integers  $a$  in the range  $0 \leq a < p$ .*

#### 5. FUTURE SECTIONS

There is more that can be said about  $F[x]$ . For example, one can prove a version of Bezout's identity, as well as unique factorization into irreducible polynomials.

**Definition 4.** The polynomials  $f \in F[x]$  is said to be *irreducible* if it is not a constant and if it has no divisors  $g$  with  $0 < \deg g < \deg f$ . These polynomials play the role of prime numbers in polynomial rings.

One can prove, in a manner similar to that used for primes in  $\mathbb{Z}$ , that there is an infinite number of irreducible polynomials in  $F[x]$ .

*Remark.* This section will be expanded as needed for the last part of the course.

DR. WAYNE AITKEN, CAL. STATE, SAN MARCOS, CA 92096, USA  
*E-mail address:* `waitken@csusm.edu`