27. Polynomials rings

27.1. **Definition and basic properties.** Let R be a commutative ring with 1. We want to define a new commutative ring with 1 denoted by $R[x]$ and called the ring of polynomials over R. It will contain R as a subring with 1.

Let us start with the set $\widehat{R[x]}$ of formal expressions of the form $\sum_{i=0}^{n} a_i x^i$ where $n \in \mathbb{Z}_{\geq 0}$ and each $a_i \in R$. We cannot just define $R[x]$ to be the set of such formal expressions since, for instance, $1 \cdot x^0$ and $1 \cdot x^0 + 0 \cdot x^1$ are formally distinct expressions, but we want to treat them as the same polynomial.

One way to resolve this issue is as follows. Let us introduce a relation $\sim$ on $\widehat{R[x]}$ by $\sum_{i=0}^{n} a_i x^i \sim \sum_{i=0}^{m} b_i x^i$ if either

(i) $n \geq m$, $a_i = b_i$ for all $0 \leq i \leq m$ and $a_i = 0$ for all $m < i \leq n$ or
(ii) $m \geq n$, $a_i = b_i$ for all $0 \leq i \leq n$ and $b_i = 0$ for all $n < i \leq m$.

It is not difficult to check that $\sim$ is an equivalence relation. We define $R[x]$ to be the set of equivalence classes with respect to this relation.

Note that in practice we will never write polynomials using the general notation for equivalence classes (with $[f]$ denoting the equivalence class of f) as this would make the formulas unreadable. Instead we will, as usual, still treat polynomials as expressions of the form $\sum_{i=0}^{n} a_i x^i$, but keep in mind that adding or removing any terms of the form $0 \cdot x^k$ does not change the polynomial.

The polynomial $0 \cdot x^0$ (simply written as 0 from now on) is called the zero polynomial.

Any nonzero polynomial $f \in R[x]$ can be uniquely written in the form $f = \sum_{i=0}^{n} a_i x^i$ where $a_n \neq 0$. In this case, we define $\deg(f) = n$, called the degree of f. The monomial $a_n x^n$ is called the leading term of f and a_n is called the leading coefficient of f.

We also define $\deg(0) = -\infty$. The leading term or the leading coefficient of the zero polynomial are undefined.

Addition and mupliplication of polynomials are given by the formulas

$$(\sum_{i=0}^{n} a_i x^i) + (\sum_{i=0}^{n} b_i x^i) = \sum_{i=0}^{n} (a_i + b_i) x^i \text{ and}$$

$$(\sum_{i=0}^{n} a_i x^i) \cdot (\sum_{i=0}^{m} b_i x^i) = \sum_{k=0}^{n+m} c_k x^k \text{ where } c_k = \sum_{i+j=k} a_i b_j.$$

Note that we did not lose any generality by using the same upper bound for summation (n) for both polynomials in the formula for addition since we can always add extra terms with the 0 coefficient. We could have done the same for multiplication, but that would not make the formula any simpler.

It is straighforward (but rather tedious) to show that $R[x]$ with the operations defined above is a commutative ring with 1.

The following basic properties of the degree function are immediate from the definition:

Lemma 27.1. *Let $f, g \in R[x]$. Then*

(a) $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$
(b) $\deg(fg) \leq \deg(f) + \deg(g)$.

Note that we do not have to exclude the zero polynomial in Lemma 27.1 if adopt the usual convention that $-\infty \leq x$ for all $x \in \mathbb{R}$ and $-\infty + x = -\infty$ for all $x \in \mathbb{R} \cup \{-\infty\}$.

The following additional properties of degree were established in HW#5:

Lemma 27.2. *Let $f, g \in R[x]$. The following hold:*

(a) $\deg(f+g) = \max\{\deg(f), \deg(g)\}$ *whenever* $\deg(f) \neq \deg(g)$
(b) $\deg(fg) = \deg(f) + \deg(g)$ *whenever R is a domain (has no zero divisors); in particular, this is true if R is a field.*

27.2. **Polynomials with coefficients in a field.** Let us now restrict our attention to polynomial rings of the form $F[x]$ where F is a field. The key result which does not hold in more general polynomial rings is the division with remainder theorem:

Theorem 27.3. *Let F be a field, let $f, g \in F[x]$, and assume that $g \neq 0$. Then there exist unique polynomials $q, r \in F[x]$ (called the quotient and remainder of dividing f by g) such that $f = gq + r$ and $\deg(r) < \deg(g)$.*

Remark: The remainder r of dividing f by g is frequently denoted by the symbol '$f \bmod g$'.

Proof. We briefly sketch a proof of the existence part. If $\deg(g) = 0$, so that g is a nonzero constant, we can simply set $q = g^{-1}f$ and $r = 0$ (note that g^{-1} exists since F is a field).

Assume now that $m = \deg(g) > 0$. Let us treat g as fixed and prove the existence of q and r by complete induction on $n = \deg(f)$. More precisely, let $P(n)$ be the following statement:

$P(n)$: For every $f \in F[x]$ with $\deg(f) = n$ there exist $q, r \in F[x]$ such that $f = gq + r$ and $\deg(r) < m = \deg(g)$.

The base case will include all values of n which are $< m$ (that is, $n = 0, 1, \ldots, m-1$). For those values of n we can set $q = 0$ and $r = f$.

Induction Step: Let us now fix some $n \geq m$, and assume that $P(k)$ is true for all $k < n$. Let us prove that $P(n)$ is true.

Take any polynomial $f \in F[x]$ with $\deg(f) = n$, and let $a_n x^n$ be its leading term. By assumption the leading term of g is $b_m x^m$ where $b_m \neq 0$. Since F is a field, b_m is invertible in F, so we can consider the monomial $h = \frac{a_n}{b_m} x^{n-m}$. Then f and gh both have degree n and the same leading term, namely $a_n x^n$, so their difference $f - gh$ has degree $< n$. Thus, we can apply the induction hypothesis to conclude that there exist $q, r \in F[x]$ with $\deg(r) < m$ such that $f - gh = gq + r$. But then $f = gh + gq + r = g(h+q) + r$, so $P(n)$ is true. □

Note that the above proof effectively gives an algorithm for calculating the quotient and the remainder, although in practice there are more efficient ways to find those.

Using division with remainder, we can extend many basic properties of integers ($\mathbb{Z}$) established in this course to $F[x]$. We start with the definition of gcd (greatest common divisor) and the polynomial version of the gcd theorem.

Definition. A polyomial $f \in F[x]$ is called monic if its leading coefficient is equal to 1, that is $f = x^n + \sum_{i=0}^{n-1} a_i x^i$ for some $a_i \in F$ (here $n = 0$ is allowed, so constant 1 is considered monic).

Definition. Let $f, g \in F[x]$, and assume that $(f, g) \neq (0, 0)$, that is, at least one of the polynomials f and g is nonzero. A polynomial $d \in F[x]$ is called a greatest common divisor (gcd) of f and g if

(i) d is monic;
(ii) d divides both f and g;
(iii) for any polynomial h which divides both f and g we have $\deg(h) \leq \deg(d)$.

We will denote such d by $gcd(f, g)$. Neither the existence nor the uniqueness of $gcd(f, g)$ is obvious from the definition, but both are true by Theorem 27.4 below:

Theorem 27.4 (GCD Theorem for polynomials)**.** *Let F be a field, and let $f, g \in F[x]$ with $(f, g) \neq (0, 0)$. The following hold:*

(a) *$gcd(f, g)$ exists and is unique;*

(b) *Let*

$$S = \{h \in F[x] : h = fu + gv \text{ for some } u, v \in F[x]\}.$$

Then $gcd(f, g) \in S$ *and* $\deg(gcd(f, g)) \leq \deg(h)$ *for any* $h \in S$. *Moreover,* $gcd(f, g)$ *is the unique monic polynomial of smallest possible degree in* S.

(c) *If* p *is any polynomial such that* $p \mid f$ *and* $p \mid g$, *then* $p \mid gcd(f, g)$.

About the proof. The proof is similar to the case of $\mathbb{Z}$, but involves some additional technicalities. We start by defining m to be the smallest degreee of a nonzero polynomial in the set S (defined in part (b)), then show that S contains a unique monic polynomial of degree m, call it d. Next we show that this d satisfies the conclusion of (c): if p is any polynomial such that $p \mid f$ and $p \mid g$, then $p \mid d$. Using Lemma 27.2(b), it is now straightforward to deduce that d satisfies the definition of $gcd(f, g)$ and moreover that $gcd(f, g)$ is unique. This proves (a) and (c), and because of the way d was defined, (b) holds as well. □

We can now define coprime polynomials and prove the coprime lemma for polynomials in complete analogy with $\mathbb{Z}$:

Definition. Polynomials $f, g \in F[x]$ are called coprime if $gcd(f, g) = 1$.

Lemma 27.5. *Let* $f, g, h \in F[x]$. *Assume that* $f \mid gh$ *and that* f *and* g *are coprime. Then* $f \mid h$.

In order to formulate the analogue of Euclid's lemma for polynomials, we need to define a property of polynomials analogous to being prime for integers. Such property is irreducibility.

Definition. Let F be a field and $p \in F[x]$. We say that p is irreducible if

(i) p is nonconstant;

(ii) p cannot be written as $p = fg$ where $f, g \in F[x]$ are both nonconstant.

Note that the convention not to consider constant polynomials irreducible matches the convention not to count 1 as a prime number.

In the case of monic polynomials one can give a characterization of irreducible polynomials which looks exactly like the definition of a prime number:

Lemma 27.6. *Let* $p \in F[x]$, *and assume that* p *is monic. Then* p *is irreducible if and only if* $p \neq 1$ *and the only monic divisors of* p *are* p *and* 1.

We can now state the polynomial analogue of Euclid's lemma (which follows from the coprime Lemma as in the case of $\mathbb{Z}$) and (a suitable form of) the unique factorization theorem for $F[x]$.

Lemma 27.7. *Let F be a field, $p, f, g \in F[x]$. Assume that $p \mid fg$ and p is irreducible. Then $p \mid f$ or $p \mid g$.*

Theorem 27.8. *Let F be a field, and let $f \in F[x]$ be a nonzero polynomial. Then f can be written as $a \cdot \prod_{i=1}^{k} p_i$ where $a \in F$ is a nonzero constant and each $p_i \in F[x]$ is monic and irreducible. Moreover, a and k (the number of factors) are uniquely determined by f and the sequence $p_1, \ldots, p_k$ is unique up to permutation of factors.*

27.3. **Ideals in and quotients of polynomial rings.** We continue studying the rings $R = F[x]$ where F is a field. As stated in Lecture 25, any ideal in such a ring is principal:

Theorem 27.9. *Let F be a field. Then any ideal I of $F[x]$ is equal to $(f) = fF[x]$ for some $f \in F[x]$.*

Theorem 27.9 can be proved using the same general idea as Theorem 27.4. If $I = \{0\}$ is the zero ideal, we can just take $f = 0$. If $I \neq \{0\}$, we define f to be a nonzero polynomial of smallest possible degree in I. Then I contains (f) by product absorption, and if (f) happens to be a proper ideal of I, we can find another nonzero element $r \in I$ with $\deg(r) < \deg(f)$, contradicting the choice of f.

Theorem 27.9 actually provides a different way to think about part (b) of Theorem 27.4 (gcd Theorem):

Proposition 27.10. *Let F be a field, let $a, b \in F[x]$, and let*

$$I = \{au + bv : u, v \in F[x]\}.$$

Then I is an ideal of $F[x]$ and $I = dF[x]$ where $d = gcd(a, b)$.

We now turn to the discussion of quotient rings $F[x]/(f)$.

First recall that for any ring R and ideal I of R elements of the quotient ring R/I are additive cosets $a + I$ with $a \in R$, and the operations on R/I are defined by $(a + I) + (b + I) = (a + b) + I$ and $(a + I)(b + I) = ab + I$.

Let us now fix $f \in R$. Given $a, b \in R$, we say that a is congruent to b mod f and write $a \equiv b \mod f$ if $f \mid (b - a)$, that is, $b = a + ft$ for some $t \in R$. Similarly to congruences in $\mathbb{Z}$, this gives us an equivalence relation on R. If we denote by $[a]_f$ the equivalence class of a with respect

to this relation (called the congruence class of a mod f), then by definition $[a]_f = a + fR = a + (f)$.

Thus, we can think of elements of the quotient ring $R/(f)$ simply as congruence classes mod f, and ring operations can be rewritten as

$$[a]_f + [b]_f = [a+b]_f \text{ and } [a]_f[b]_f = [ab]_f.$$

Let us now go back to the case $R = F[x]$, with F a field, and assume that $f \in F[x]$ is nonzero. Then for any $h \in R$ we have $[h]_f = [r]_f$ where $r = h \mod f$, the remainder of dividing h by f.

Thus, if we set $n = \deg(f)$, then any element of $F[x]/(f)$ can be written as $[r]_f$ with $\deg(r) < n$, and moreover such a representation is unique. This gives a notationally simpler way to think about the quotient ring $F[x]/(f)$.

Let $P_n(F)$ be the set of all polynomials in $F[x]$ of degree $< n$. Then we can identify $F[x]/(f)$ with $P_n(F)$ as a set, and ring operations (denoted by $\oplus$ and $\odot$ below to avoid confusion with usual addition and multiplication) are given by

- $g \oplus h = g + h$ (addition is the usual addition) and
- $g \odot h = (gh) \mod f$.

Example: Let $F = \mathbb{Z}_2$ and $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Then $P_2(F) = \{0, 1, x, x+1\}$, and the addition and multiplication on $\mathbb{Z}_2[x]/(f)$ (under the above identification) are given as follows:

$\oplus$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\odot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

From the multiplication table we see that any nonzero element of the quotient ring $\mathbb{Z}_2[x]/(x^2+x+1)$ is invertible, so this quotient ring is a field. We could have proved this without directly computing the multiplication table and instead using the following theorem:

Theorem 27.11. *Let F be a field and $f \in F[x]$. Then the quotient ring $F[x]/(f)$ is a field $\iff$ f is irreducible.*

This is a direct analogue of Corollary 9.2 which asserts that $\mathbb{Z}_n$ is a field $\iff$ n is prime. Recall that Corollary 9.2 was deduced from Theorem 9.1

which gives a complete description of invertible elements in $\mathbb{Z}_n$. Analogous characterization remains true in polynomial rings and can be used to prove Theorem 27.11 using similar logic:

Theorem 27.12. *Let F be a field and $f \in F[x]$ and $Q = F[x]/(f)$. Let $g \in F[x]$. Then an element $[g]_f = g + (f)$ of Q is invertible $\iff$ $gcd(f, g) = 1$.*