# Day 17

## Polynomial Rings and Unique Factorization

### Characteristic

Suppose $R$ is an integral domain. There is always a ring homomorphism from $f : \mathbb{Z} \to R$ that sends $f(n) = n \cdot 1$ where 1 is the identity element in $R$.

By the isomorphism theorem, this gives an injective map $\overline{f} : \mathbb{Z}/I \to R$ where $I$ is the kernel of $f$.

Since the image of this map is an integral domain, $I$ is a prime ideal in $\mathbb{Z}$. Therefore either $I = (0)$ or $I = (p)$ for some prime $p$. In the first case we say that $R$ has *characteristic zero* and in the second we say that $R$ has characteristic $p$.

In the first case, $R$ contains a copy of $\mathbb{Z}$; in the second, a copy of $\mathbb{Z}/p\mathbb{Z}$.

In an integral domain of characteristic $p$, $px = 0$ for any $x \in R$. In characteristic zero, if $nx = 0$ for $n \in \mathbb{Z}$ and $n \neq 0$, then $x = 0$.

The rings $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$,... all have characteristic zero.

The rings $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}[x]$,... have characteristic $p$.

**Lemma:** In a ring of characteristic $p$, $(x + y)^p = x^p + y^p$.

**Proof:** The binomial coefficients $\binom{p}{i}$ are divisible by $p$ whenever $1 \leq i \leq p - 1$.

### Fraction fields

Suppose that $R$ is an integral domain. We can construct a field containing $R$ considering

$$K(R) = \{\frac{a}{b} : a, b \in R, b \neq 0\}$$

and imposing the usual "fraction rules":

- $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$
- $\frac{xa}{xb} = \frac{a}{b}$ if $x \neq 0$.
- $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$

More formally we can consider ordered pairs $(a, b) \in R \times R$ with $b \neq 0$ and define an equivalence relation saying $(a, b) \sim (xa, xb)$ for all $x \neq 0$ in $R$; then

defining the operations as above on equivalence classes, checking everything is well defined, and so on. See DF Section 7.5, especially Theorem 15 of that chapter, for all the details.

**Proposition:** Suppose that $R$ is an integral domain and $F$ is a field. If $f : R \to F$ is an injective map sending 1 to 1, then $f$ extends to a map from $K(R)$ into $F$. Expressed differently, if $F$ is a field that contains a subring isomorphic to $R$, then the smallest subfield of $F$ containing $R$ is isomorphic to $K(R)$. Informally, $K(R)$ is the smallest field containing $R$.

**Examples:**

- $K(\mathbb{Z}) = \mathbb{Q}$.
- $K(\mathbb{R}[x])$=$\mathbb{R}(x)$ (this is notation) – the field of rational functions over $\mathbb{R}$.
- $K(\mathbb{Z}[x])$=$\mathbb{Q}(x)$ – the field of rational functions over $\mathbb{Q}$.

- $K(\mathbb{Z}[i])$=$Q(i)$=$Q[i]$=$\{a + bi : a, b \in \mathbb{Q}\}$

**Polynomial Rings**

Let $R$ be a commutative ring with unity.

1. An element $f \in R[x]$ is *monic* if its highest degree coefficient is 1.
2. The units in $R[x]$ are the units in $R$.
3. If $R$ is an integral domain, so is $R[x]$ (look at highest degree terms of the polynomials)
4. If $I$ is an ideal of $R$, then $R[x]/IR[x]$ is isomorphic to $(R/I)[x]$.
5. If $I$ is a prime ideal in $R$, then $IR[x]$ is a prime ideal in $R[x]$.
6. If $f$ is a monic polynomial in $R[x]$ and $g$ is any polynomial, then there is a division algorithm yielding $g = qf + r$ with the degree of $r$ less than the degree of $f$.
7. If $R$ is a field, any polynomial can be made monic multiplying by the inverse of its highest degree coefficient.

The ring $R[x_1, x_2, \ldots, x_n]$ is the ring of polynomials in $n$ variables with coefficients in $R$. The terms of such a polynomial are monomials

$$a(i_1, \ldots, i_n)x_1^{i_1} \cdots x_n^{i_n}.$$

The *total degree* of such a monomial is the sum of its degrees, and the total degree of a polynomial is the highest total degree of its monomials.

A polynomial in $R[x_1, \ldots, x_n]$ may also be viewed as a polynomial in $x_n$ whose coefficients are polynomials in $x_1, \ldots, x_{n-1}$. (In other words, $R[x_1, \ldots, x_{n-1}][x] = R[x_1, \ldots, x_n]$).$ In this case we can talk about the degree of a polynomial as the highest power of $x_n$ with nonzero coefficient.

A polynomial in variables $x_1, \ldots, x_n$ is *homogeneous* if all monomials have the same total degree. Any polynomial in $n$ variables can be written as a sum of homogeneous polynomials.

**Proposition:** $R[x]$ is a PID if and only if $R$ is a field.

**Proof:** If $R$ is a field we know this by Euclid's algorithm and polynomial division. If $R$ is not a field, it has a proper maximal ideal $I$. Then $IR[x]$ is prime since $R[x]/IR[x] = R/I[x]$ is an integral domain. But $R/I[x]$ is not a field – it contains the proper ideal generated by $x + I$. Thus $R[x]$ contains non-maximal prime ideals, so it can't be a PID.

**Polynomial rings over UFD's are UFD's.**

If $R$ is a UFD, a polynomial $f(x)$ in $R[x]$ is called *primitive* if the greatest common divisor of its coefficients is 1; or, put another way, if the ideal generated by the coefficients in $R$ is $R$.

**Theorem:** (DF, Theorem 7, page 304) $R$ is a UFD if and only if $R[x]$ is a UFD.

Since $R$ is a subring of $R[x]$ and a factorization of an element of $R$ in $R[x]$ involves only elements of $R$, if $R[x]$ is a UFD, so is $R$.

Going the other way is the interesting part.

The basic strategy is: - start with a polynomial $f(x) \in R[x]$. - factor out the gcd of the coefficients in $f$ so that $f = df_1$ and $f_1$ is primitive. - The term $d$ has a unique factorization, since it's in $R$, so we have to worry about the primitive polynomial $f_1$. - View $f_1$ as a polynomial in $K(R)[x]$, which is a polynomial ring over a field and therefore a PID/UFD. - Since the leading coefficient $a$ of $f_1$ is a unit in $K(R)$, we can factor it out and write $f_1 = af_2$ where $f_2$ is a monic polynomial in $K(R)[x]$. - Thus $f_2 = g_1 \cdots g_k$ where the $g_i$ are irreducible monic polynomials with coefficients in $K(R)[x]$. - Therefore $f_1$ factors as $ag_1 \cdots g_k$.

**Problem 1:** At this point, the $g_i$ have coefficients in $K(R)[x]$ – they have "denominators". We need to clear out those denominators. We have the leading coefficient $a$. Can we somehow split $a$ up into pieces $a = a_1 \dots a_k$ so that $a_i g_i$ belongs to $R[x]$? If so, then we've factored

$$f_1 = (a_1 g_1) \cdots (a_k g_k) = h_1 \cdots h_k$$

where each factor is in $R[x]$ and is irreducible in $K(R)[x]$.

**Suppose we can do this!**

We're happy because we've factored $f_1$ as a product of polynomials $h_i$ in $R[x]$, each of which is irreducible in $K(R)[x]$. And they must also be irreducible in $R[x]$, because $R[x] \subset K(R)[x]$.

**Problem 2:** We need to establish uniqueness. The idea is that if we had two factorizations of $f_1$ in $R[x]$, we'd have two factorizations in $K(R)[x]$. Since $K(R)[x]$ is a PID, we can show that these two factorizations are "the same" in $K(R)[x]$ – they have the same number of terms, and the terms can be matched up as associates in $K(R)[x]$. But two irreducibles can be associates in $K(R)[x]$ and maybe not in $R[x]$ – this is another "denominator problem." So we need

to sort that out as well. This reduces to the question: suppose $q_1(x)$ and $q_2(x)$ are irreducibles in $K(R)[x]$ that are associates. This means that we can "clear denominators" in $q_1$ and $q_2$ so that both are in $R[x]$ and primitive and $q_1(x) = uq_2(x)$ for some $u$ in $K(R)$. Since $u = a/b$ for elements $a$ and $b$ in $R$, this amounts to the equation $bq_1(x) = aq_2(x)$. But since $q_1$ and $q_2$ are primitive, the gcd of the coefficients of $bq_1$ is $b$, and of $aq_2$ is $a$, so $a$ and $b$ are equal up to a unit in $R$ and $q_1$ and $q_2$ are associates in $R[x]$.

Once we're done, we have unique factorization!