9. Unique factorization and polynomial rings

Polynomial rings and unique factorization

Definition: If R is an integral domain, the set of integers n such that $n \cdot 1 = 0$ is a prime ideal in $\mathbb{Z}$. If this ideal is the zero ideal, R has *characteristic zero*; if this ideal is $p\mathbb{Z}$ then R has *characteristic* p.

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

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 $x \neq 0$.
- $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$

See DF Section 7.5 for a more formal definition.

The fraction field $K(R)$ is the "smallest field containing R".

Polynomial rings: vocabulary and basics

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 principal ideal domain if and only if R is a field. If R is a field, then $R[x]$ is a Euclidean domain.

Unique Factorization in $R[x]$.

Theorem: If R is a UFD, then so is $R[x]$.

Criteria for irreducibility

- Polynomials of degree 2 or 3 over a field are irreducible or have a root in the field.
- If a monic polynomial is irreducible in $R/I[x]$, it is irreducible in $R[x]$.

Theorem: (Eisenstein's Criterion) Let P be a prime ideal of R and suppose $f(x)$ is a monic polynomial in $R[x]$ of degree n. If $f(x) \equiv x^n \pmod{P}$ and the constant term a_0 of f is not in P^2 then f is irreducible.

If a monic polynomial with integer coefficients has all its coefficients except its leading one divisible by a prime p, and its constant term is divisible by p but not p^2, then it is irreducible.

Corollary: The polynomial $f(x) = \frac{x^p - 1}{x - 1}$, the p^{th} cyclotomic polynomial, is irreducible in $\mathbb{Z}[x]$ (and $\mathbb{Q}[x]$).