9. Polynomial Rings

Proposition 9.1. Let I be an ideal of R and let $(I) = I[x]$ denote the ideal of $R[x]$ generated by I. Then

$$R[x]/(I) \cong (R/I)[x].$$

In particular, if I is a prime ideal of R then (I) is a prime ideal of $R[x]$

Definition 9.2. The *polynomial ring in the variables* $x_1, x_2, \ldots, x_n$ *with coefficients in* R, denoted $R[x_1, x_2, \ldots, x_n]$, is defined inductively by

$$R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}][x_n]$$

Theorem 9.3. Let F be a field. The polynomial ring $F[x]$ is a Euclidean Domain. Specifically, if $a(x)$ and $b(x)$ are two polynomials in $F[x]$ with $b(x)$ nonzero, the there are *unique* $q(x)$ and $r(x)$ in $F[x]$ such that

$$a(x) = q(x)b(x) + r(x) \qquad \text{with } r(x) = 0 \text{ or } deg(r(x)) < deg(b(x)).$$

Proposition 9.4. *(Gauss' Lemma)* Let R be a UFD with field of fractions F and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$. More precisely, if $p(x) = A(x)B(x)$ for some nonconstant polynomials $A(x), B(x) \in F[x]$, then there are some nonzero elements $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ both lie in $R[x]$ and $p(x) = a(x)b(x)$ is a factorization in $R[x]$.

Corollary 9.5. Let R be a UFD, let F be its field of fractions and let $p(x) \in R[x]$. Suppose the gcd of the coefficients of $p(x)$ is 1. Then $p(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$. In particular, if $p(x)$ is a monic polynomial that is irreducible in $R[x]$, then $p(x)$ is irreducible in $F[x]$.

Theorem 9.6. R is a UFD if and only if $R[x]$ is a UFD.

Corollary 9.7. If R is a UFD, then a polynomial ring in an arbitrary number of variables with coefficients in R is also a UFD.

Proposition 9.8. Let F be a field and let $p(x) \in F[x]$. Then $p(x)$ has a factor of degree one if and only if $p(x)$ has a root in F.

Proposition 9.9. A polynomial of degree two or three is reducible over a field F if and only if it has a root in F.

Proposition 9.10. Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with integer coefficients. If $r/s \in \mathbb{Q}$ is in lowest terms and r/s is a root of $p(x)$, then r divides the constant term and s divides the leading coefficient of $p(x)$. In particular, if $p(x)$ is a monic polynomial with integer coefficients and $p(d) \neq 0$ for all integers dividing the constant term of $p(x)$, then $p(x)$ has no roots in $\mathbb{Q}$.

Proposition 9.11. Let I be a proper ideal in the integral domain R and let $p(x)$ be a nonconstant monic polynomial in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ cannot be factored in $(R/I)[x]$ into two polynomials of smaller degree, then $p(x)$ is irreducible in $R[x]$.

Proposition 9.12. *(Eisenstein's Criterion)* Let P be a prime ideal of the integral domain R and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial in $R[x]$ where $n \geq 1$. Suppose $a_{n-1}, \ldots a_0$ are all elements of P and suppose a_0 is not an element of P^2. Then $f(x)$ is irreducible in $R[x]$.

Proposition 9.13. The maximal ideals in $F[x]$ are the ideals $(f(x))$ generated by irreducible polynomials $f(x)$. In particular $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

Proposition 9.14. Let $g(x)$ be a nonconstant monic element of $F[x]$ and let

$$g(x) = f_1(x)^{n_1} f_2(x)^{n_2} \cdots f_k(x)^{n_k}$$

be its factorization into irreducible, where the $f_i(x)$ are distinct. Then we have the following isomorphism of rings:

$$F[x]/(g(x)) \cong F[x]/(f_1(x)^{n_1}) \times F[x]/(f_2(x)^{n_2}) \times \cdots F[x]/(f_k(x)^{n_k}).$$

Proposition 9.15. If the polynomial $f(x)$ has roots $\alpha_1, \alpha_2, \ldots, \alpha_k$ in F, then $f(x)$ has $(x - \alpha_1) \cdots (x - \alpha_k)$ as a factor. In particular, a polynomial of degree n in one variable has at most n roots in F, even counted with multiplicity.

Proposition 9.16. A finite subgroup of the multiplicative group of a field is cyclic. In particular, if F is a finite field, the the multiplicative group $F^\times$ of nonzero elements of F is a cyclic group.

Corollary 9.17. Let $n \geq 2$ be an integer with factorization $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ in $\mathbb{Z}$, where $p_1, p_2, \ldots, p_r$ are distinct primes. We have the following isomorphism of (multiplicative) groups:

1. $(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times$
2. $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ is the direct product of a cyclic group of order 2 and a cyclic group of order $2^{\alpha-2}$, for all $\alpha \geq 2$
3. $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is a cyclic group of order $p^{\alpha-1}(p-1)$, for all odd primes p.