Math 425: Abstract Algebra I
Theorems from the Textbook - Chapter 4

Theorems

Theorem 4.1.1. *Let R be a ring and let x be an indeterminate over R. Then*

(1) $R[x]$ is a ring.

(2) R is the subring of all constant polynomials in $R[x]$.

(3) If $Z = Z(R)$ denotes the center of R, then the center of $R[x]$ is $Z[x]$.

(4) In fact, x is in the center of $R[x]$.

(5) If R is commutative, then $R[x]$ is commutative.

Theorem 4.1.2. *Let R be a domain. Then*

(1) $R[x]$ is a domain.

(2) If $f \neq 0$ and $g \neq 0$ in $R[x]$, then $\deg(fg) = \deg(f) + \deg(g)$.

(3) The units in $R[x]$ are the units in R.

Theorem 4.1.3. *Let R be any ring and let $f \neq 0$ and $g \neq 0$ be polynomials in $R[x]$. If the leading coefficient of either f or g is a unit in R, then*

(1) $fg \neq 0$ in $R[x]$

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

Theorem 4.1.4 (Division Algorithm)**.** *Let R be any ring and let f and g be polynomials in $R[x]$. Assume $f \neq 0$ and that the leading coefficient of f is a unit in R. Then there exist unique $q, r \in R[x]$ such that*

(1) $g = qf + r$.

(2) Either $r = 0$ or $\deg r < \deg f$.

Theorem 4.1.5. *Let R be a ring and $a \in Z(R)$, the center of R. Define $\phi_a : R[x] \to R$ by*

$$\phi_a(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_0 + a_1(a) + a_2(a)^2 + \cdots + a_n(a)^n.$$

Then the map ϕ_a is an onto ring homomorphism.

Theorem 4.1.6 (1) (Factor Theorem)**.** *Let R be a commutative ring, $a \in R$, and $f \in R[x]$. Then $f(a) = 0$ if and only if $f = (x - a)g$ for some $g \in R[x]$.*

Theorem 4.1.6 (2) (Remainder Theorem)**.** *Moreover, in general, when dividing f by $x - a$, we get $f = (x - a)q + f(a)$. That is, the remainder when dividing f by $x - a$ is $f(a) \in R$.*

Corollary 1. *Let R be a commutative ring, $a \in R$, and $\phi_a : R[x] \to R$ the evaulation map at a. Then*
$$\ker(\phi_a) = (x-a) = \{(x-a)g \mid g \in R[x]\}$$
and $R[x]/(x-a) \cong R$.

Theorem 4.1.8. *Let R be an integral domain and let f be a nonzero polynomial of degree n in $R[x]$. Then f has at most n roots in R.*

Theorem 4.1.9 (Rational Roots Theorem)**.** *Let $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be a polynomial in $\mathbb{Z}[x]$ with $a_0, a_n \neq 0$. Then every root of f in $\mathbb{Q}$ is of the form $\frac{c}{d}$ where $c \mid a_0$ and $d \mid a_n$.*

Theorem 4.2.1. *Let F be a field and consider p in $F[x]$ where $\deg p \geq 2$.*

(1) If p is irreducible, then p has no root in F.

(2) If $\deg p$ is 2 or 3, then p is irreducible if and only if it has no root in F.

Theorem 4.2.2 (Fundamental Theorem of Algebra)**.** *If $f \in \mathbb{C}[x]$ with $\deg f > 0$, then f has at least one root in $\mathbb{C}$.*

Theorem 4.2.3. *(1) If $\deg f = n \geq 1$, $f \in \mathbb{C}[x]$, then f factors completely as*
$$f = u(x-a_1)(x-a_2)\cdots(x-a_n),$$
for $u \neq 0$, $a_1, a_2, \ldots, a_n \in \mathbb{C}$.

(2) The only irreducible polynomials in $\mathbb{C}[x]$ are linear.

Theorem 4.2.4. *Every nonconstant polynomial $f \in \mathbb{R}[x]$ factors as*
$$f = u(x-r_1)(x-r_2)\cdots(x-r_m)q_1q_2\cdots q_k,$$
where $r_1, r_2, \ldots, r_m$ are the real roots of f and $q_1, q_2, \ldots, q_k$ are monic irreducible quadratics in $\mathbb{R}[x]$.

Corollary 1. *The irreducible polynomials in $\mathbb{R}[x]$ are either linear or quadratic.*

Theorem 4.2.5 (Gauss' Lemma)**.** *Let $f = gh$ in $\mathbb{Z}[x]$. If a prime $p \in \mathbb{Z}$ divides every coefficient of f, then p divides every coefficient of g or p divides every coefficient of h.*

Theorem 4.2.6. *Let $f \in \mathbb{Z}[x]$ be a non-constant polynomial.*

(1) If $f = gh$ with $g, h \in \mathbb{Q}[x]$, then $f = g_0h_0$ where $g_0, h_0 \in \mathbb{Z}[x]$, $\deg g = \deg g_0$, and $\deg h = \deg h_0$.

(2) f is irreducible in $\mathbb{Q}[x]$ if and only if $f = ag$ where $a \in \mathbb{Z}$ are the only factorizations of f in $\mathbb{Z}[x]$.

Theorem 4.2.7 (Modular Irreducibility)**.** *Let $0 \neq f \in \mathbb{Z}[x]$ and suppose that a prime p exists such that*

(1) p *does not divide the leading coefficient of* f.

(2) *The reduction,* $\bar{f}$ *of* f *modulo* p *is irreducible in* $\mathbb{Z}_p[x]$.

Then f *is irreducible over* $\mathbb{Q}$.

Theorem 4.2.8 (Eisenstein's Criterion)**.** *Consider* $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ *in* $\mathbb{Z}[x]$, *where* $n \geq 1$ *and* $a_0 \neq 0$. *Let* $p \in \mathbb{Z}$ *be a prime number satisfying*

(1) p *divides each of* $a_0, a_1, a_2, \ldots, a_{n-1}$.

(2) p *does not divide* a_n.

(3) p^2 *does not divide* a_0.

Then f *is irreducible in* $\mathbb{Q}[x]$.

Theorem 4.2.9. *Let* F *be a field and let* f *and* g *be nonzero monic polynomials in* $F[x]$, *each of which divides the other. Then* $f = g$.

Corollary 1. *If* F *is a field and* $p \in F[x]$ *is monic, the following are equivalent:*

(1) p *is irreducible.*

(2) *If* d *is a monic divisor of* p, *then either* $d = 1$ *or* $d = p$.

Theorem 4.2.10. *Let* f *and* g *be nonzero polynomials in* $F[x]$, *where* F *is a field. Then a uniquely determined polynomial* d *exists in* $F[x]$ *satisfying the following conditions:*

(1) d *is monic.*

(2) d *divides both* f *and* g.

(3) *If* h *divides both* f *and* g, *then* h *divides* d.

(4) $d = uf + vg$ *for some polynomials* u *and* v *in* $F[x]$.

Moreover d *is the unique polynomial satisfying (1), (2) and (3).*

Theorem 4.2.11. *Let* $p \in F[x]$ *be irreducible,* F *a field. If* p *divides the product* $f_1f_2 \cdots f_n$ *of nonzero polynomials in* $F[x]$, *then* p *divides* f_i *for some* i.

Theorem 4.2.12 (Unique Factorization Theorem)**.** *Let* F *be a field and* f *be a nonconstant polynomial in* $F[x]$. *Then*

(1) $f = ap_1p_2 \cdots p_m$, *where* $a \in F$ *and* $p_1, p_2, \ldots, p_m$ *are monic irreducible polynomials in* $F[x]$.

(2) *The factorization is unique up to the order of the factors.*

Theorem 4.3.1. *If* F *is a field, then every ideal* A *of* $F[x]$ *is principal. In fact, if* $A \neq 0$, *then there is a unique monic polynomial* $h \in F[x]$ *for which* $A = (h)$.

Theorem 4.3.2. *Let h be a monic polynomial of degree $m \geq 1$ in $F[x]$, there F is a field. Then*

$$F[x]/(h) \cong \{a_0 + a_1 t + a_2 t^2 + \cdots + a_{m-1} t^{m-1} \; | a_i \in F, h(t) = 0\}.$$

Moreover, this representation is unique. That is,

$$a_0 + a_1 t + a_2 t^2 + \cdots + a_{m-1} t^{m-1} = b_0 + b_1 t + b_2 t^2 + \cdots + b_{m-1} t^{m-1}$$

if and only if $a_i = b_i$ for all i.

Theorem 4.3.3. *Let h be a monic polynomial of degree $m \geq 1$ in $F[x]$, there F is a field. Then $F[x]/(h)$ is a field if and only if h is irreducible.*

Theorem 4.3.4 (Kronecker's Theorem)**.** *Let F be a field and $h \in F[x]$ an irreducible polynomial. Then there is some field K containing F that has a root of h.*

Definitions

Definition. A symbol, x is called an *indeterminate* over a ring R if given $a_0, a_1, a_2, \ldots, a_n \in R$ satisfying

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0,$$

then $a_i = 0$ for all i.

Definition. Given a ring R and an indeterminate x, the *ring of polynomials* over R in x is the set

$$R[x] = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \mid n \geq 0, \; a_0, a_1, a_2, \ldots, a_n \in R\}$$

along with the operations given as follows:

Let $f = a_0 + a_1 x + a_2 x^2 + \cdots$ and $g = b_0 + b_1 x + b_2 x^2 + \cdots$.

- Addition: $f + g = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots$
- Multiplication $fg = c_0 + c_1 x + c_2 x^2 + \cdots$ where

$$c_i = a_0 b_i + a_1 b^{i-1} + \cdots + a_{i-1} b_1 + a_i b_0 = \sum_{k=0}^{i} a_k b_{i-k}$$

Definition. We call two polynomials *equal* if the corresponding coefficients are equal.

Definition. We call a_0 the *constant term* or *constant coefficient.*

Definition. A polynomial of the form $f = a_0$ is a *constant polynomial.*

Definition. The *zero* of $R[x]$ is 0_R and the *unity* is 1_R.

Definition. The *negative* of $f = a_0 + a_1 x + a_2 x^2 + \cdots$ is $-f = -a_0 - a_1 x - a_2 x^2 - \cdots$.

Definition. The *degree* of f is the highest power of x that has a nonzero coefficient. We write $\deg(f)$ for the degree.

Definition. If $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ has degree n, then we call a_n the *leading coefficient* of f.
If $a_n = 1$, we call f *monic.*

Definition. Given a polynomial $f \in R[x]$,

- If $\deg(f) = 1$, we call f a *linear* polynomial.
- If $\deg(f) = 2$, we call f a *quadratic* polynomial.
- If $\deg(f) = 3$, we call f a *cubic* polynomial.
- If $\deg(f) = 4$, we call f a *quartic* polynomial.
- If $\deg(f) = 5$, we call f a *quintic* polynomial.

Definition. If R is a ring, $a \in Z(R)$, and ϕ_a is the map described in Theorem 4.1.5, then we call ϕ_a the evaluation map at a.

Definition. Let $f \in R[x]$ and $a \in R$. We call a a *root* or f if the following conditions (which are all equivalent) are true:

(1) $f(a) = 0$.

(2) $f = (x - a)g$ for some $g \in R[x]$.

(3) $f \in (x - a)$.

If $a \in R$ is a root of f, we say it has multiplicity $m \in \mathbb{Z}_{>0}$ if $f = (x - a)^m q$ and $q(a) \neq 0$.

Definition. Let F be a field and $p \neq 0$ in $F[x]$ a polynomial. We call p *irreducible over* F if $\deg(p) \geq 1$ and

$$\text{If } p = fg \text{ for } f, g \in F[x], \text{ then either} \deg f = 0 \text{ or } \deg g = 0.$$

Otherwise we call p *reducible.*

Definition. Given a commutative ring R and polynomials $f, q \in R[x]$, we say q divides f if there is some $d \in R[x]$ with $f = qd$.

Definition. If F is a field and $f, g \in F[x]$. Then the *greatest common divisor* of f and g is the unique monic polynomial d that satisfies properties (1), (2), and (3) of Theorem 4.2.10.
We say f and g are relatively prime if $\gcd(f, g) = 1$.