

1 Groups

1.1 Isomorphism Theorems

THM: “First Isomorphism Theorem” If $\varphi : G \rightarrow H$ is a homomorphism of groups, then $\ker \varphi \trianglelefteq G$ and $G/\ker \varphi \cong \text{im } \varphi$.¹

COR: Let $\varphi : G \rightarrow H$ be a homomorphism of groups.

- (i) φ is injective if and only if $\ker \varphi = \{e\}$.
- (ii) $|G : \ker \varphi| = |\text{im } \varphi|$.²

THM: “Second/Diamond Isomorphism Theorem” Let G be a group, let A and B be subgroups of G and assume $A \leq N_G(B)$. Then:

- (i) AB is a subgroup of G ,
- (ii) $B \trianglelefteq AB$,
- (iii) $A \cap B \trianglelefteq A$,
- (iv) $AB/B \cong A/(A \cap B)$.³

THM: “Third Isomorphism Theorem” Let G be a group and let $H, K \trianglelefteq G$. Then,

- (i) $K/H \trianglelefteq G/H$,
- (ii) $(G/H)/(K/H) \cong G/K$.⁴

THM: “Fourth/Lattice Isomorphism Theorem” Let G be a group and let $N \trianglelefteq G$. Then there is a bijection from the set of subgroups A of G which contain N onto the set of subgroups $\bar{A} = A/N$ of G/N . In particular, every subgroup of \bar{G} is of the form A/N for some subgroup A of G containing N (namely, its preimage in G under the natural projection homomorphism from G to G/N). This bijection has the properties for all $A, B \leq G$ with $N \leq A, N \leq B$:

- (i) $A \leq B$ if and only if $\bar{A} \leq \bar{B}$,
- (ii) if $A \leq B$, then $[B : A] = [\bar{B}, \bar{A}]$,
- (iii) $\langle \bar{A}, \bar{B} \rangle = \overline{\langle A, B \rangle}$,
- (iv) $\overline{A \cap B} = \bar{A} \cap \bar{B}$,
- (v) $A \trianglelefteq G$ if and only if $\bar{A} \trianglelefteq \bar{G}$.⁵

THM: “Fundamental Theorem of Finitely Generated Abelian Groups” Let G be a finitely generated abelian group, then $G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$ for $r, n_1, \dots, n_s \in \mathbb{Z}$ with $r \geq 0, n_i \geq 2$ and $n_i \mid n_{i+1}$. Also, this form is unique.⁶

DEF: The integer r in the FTFGAG is called the *free rank* or *Betti number* of G . The numbers n_1, \dots, n_s are the *invariant factors* of G . This form is the *invariant factor decomposition* of G .

THM: “Elementary Divisors Form” Let G be an abelian group with $|G| = n > 1$. Let the unique prime factorization of n be $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Then,

- (i) $G \cong A_1 \times \cdots \times A_k$ where $|A_i| = p_i^{\alpha_i}$.
- (ii) Each A_i has $A_i \cong \mathbb{Z}_{p_i^{\beta_1}} \times \cdots \times \mathbb{Z}_{p_i^{\beta_t}}$ where $\beta_1 \leq \cdots \leq \beta_t$ and $\beta_1 + \cdots + \beta_t = \alpha_i$.
- (iii) The decomposition in (i) and (ii) is unique.⁷

DEF: The integers $p_i^{\beta_j}$ in the elementary divisor form above are the *elementary divisors* of G .⁸

DEF: If G is a finite abelian group of type (n_1, \dots, n_t) , the integer t is called the *rank* of G . If G is a group, the *exponent* of G is the smallest $n > 0$ such that $x^n = e$ for all $x \in G$ (if no such integer exists, then the exponent of G is ∞).⁹

1.2 Subgroup Technology

DEF: Let $\varphi : G \rightarrow H$ be a homomorphism with kernel K . The *quotient group* or *factor group*, G/K is the group whose elements are the fibers of φ with operation defined by representatives of the fibers.¹⁰

DEF: Let $H \leq G$. If $xHx^{-1} = H$ for all $x \in G$, then H is *normal* in G , written $H \trianglelefteq G$.

PROP: Let $N \trianglelefteq G$. The set of left cosets of N partitions G , and $u, v \in G$ have that $uN = vN$ if and only if $v^{-1}u \in N$.¹¹

DEF: Let S be a subset of G . Let $N = N_S = \{x \in G \mid xSx^{-1} = S\}$ be called the *normalizer* of S in G .¹²

DEF: Let S be a subset of G . Let $Z = Z_S = \{x \in G \mid xyx^{-1} = y, \forall y \in S\}$ be called the *centralizer* of S in G .¹³

PROP: Let G be a finite group of order $n > 1$. Let a be an element of $G \setminus \{e\}$. Then the period of a divides n . If the order of G is a prime number p , then G is cyclic and the period of any generator is equal to p .¹⁴

PROP: Let G be a group and let $x \in G$ and $a \in \mathbb{Z} \setminus \{0\}$.

- (i) If $|x| = \infty$, then $|x^a| = \infty$.
- (ii) If $|x| = n < \infty$, then $|x^a| = \frac{n}{\gcd(n, a)}$.
- (iii) In particular, if $|x| = n < l\infty, a \mid n$, then $|x^a| = \frac{n}{a}$.¹⁵

PROP: Let $H = \langle x \rangle$.

(i) Assume $|x| = \infty$, then $H = \langle x^a \rangle$ if and only if $a = \pm 1$.

(ii) Assume $|x| = n < \infty$, then $H = \langle x^a \rangle$ if and only if $\gcd(a, n) = 1$.¹⁶

PROP: Let G be a cyclic group. Then every subgroup of G is cyclic. If f is a homomorphism of G , then the image of f is cyclic.¹⁷

PROP: "Properties of Generators in Cyclic Groups"

(i) An infinite cyclic group has exactly two generators (if a is a generator, then a^{-1} is the only other generator).

(ii) Let G be a finite cyclic group of order n , and let x be a generator. The set of generators of G consists of those powers x^v of x such that v is relatively prime to n .

(iii) Let G be a cyclic group, and let a, b be to generators. Then there exists an automorphism of G mapping a onto b . Conversely, any automorphism of G maps a on some generator of G .

(iv) Let G be a cyclic group of order n . Let d be a positive integer dividing n . Then there exists a unique subgroup of G of order d .

(v) "Chinese Remainder Thm" Let G_1, G_2 be cyclic of orders m, n . If m, n are relatively prime, then $G_1 \times G_2 \cong C_{mn}$.

(vi) Let G be a finite abelian group. If G is not cyclic, then there exists a prime p and a subgroup of G isomorphic to $C \times C$ where C is cyclic of order p .¹⁸

THM: "Properties of Isomorphisms" Let ϕ be an isomorphism from G to H . Then, for $a, b \in G, k, n \in \mathbb{Z}$:

(i) $\phi(e_G) = e_H$ (ii) $\phi(a^n) = \phi(a)^n$ (iii) $G = \langle a \rangle \Leftrightarrow H = \langle \phi(a) \rangle$

(iv) $ab = ba \Leftrightarrow \phi(a)\phi(b) = \phi(b)\phi(a)$. (v) $|a| = |\phi(a)|$

(vi) The equation $x^k = b$ has the same # of solutions in G as $x^k = \phi(b)$ in H .

(vii) G is abelian/cyclic iff H is abelian/cyclic. (viii) ϕ^{-1} is an isomorphism from H to G .

(ix) If $K \leq G$, then $\phi(K) \leq H$.¹⁹

COR: $G \not\cong H$ if *any* of these conditions fail.

THM: Some automorphism groups:

(i) For every positive integer n , $\text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$. $|\mathbb{Z}_n^\times| = \varphi(n) :=$ the Euler φ function.

(ii) For p an odd prime, $\text{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$.

(iii) For p an odd prime and $m = p^n$, $\text{Aut}(\mathbb{Z}_m)$ is cyclic of order $p^{n-1}(p-1)$.

(iv) For $m = 2^n$, $\text{Aut}(\mathbb{Z}_m) \cong \mathbb{Z}_2 \times \mathbb{Z}_r$ where $r = 2^{n-2}$ (not cyclic, but has a cyclic subgroup of index 2).

(v) If p is prime and V is an abelian group of order p^n such that $pv = 0$, for all $v \in V$, then V is an n -dim vector space over the field \mathbb{Z}_p , and $\text{Aut}(V) \cong \text{GL}(V) \cong \text{GL}_n(\mathbb{Z}_p)$.

(vi) If $n \neq 6$, then $\text{Aut}(S_n) \cong \text{Inn}(S_n) \cong S_n$ (every automorphism is inner). (vii) $[\text{Aut}(S_6) : \text{Inn}(S_6)] = 2$ and there exists an automorphism $S_6 \rightarrow S_6$.²⁰ (viii) $\text{Aut}(D_8) \cong D_8$ and $\text{Aut}(Q_8) \cong S_4$.²¹

(ix) If $G = C_p \times C_p$ for some p prime, G acts as a 2-dim v.s. over \mathbb{F}_p . $\sigma \in \text{Aut}(G)$ can take $(a, 0)$ to any non-zero element (for $a \neq 0$) since every nonzero element has order p . Now, $\sigma(a, 0)$ is determined, so $\sigma(0, b)$ has $p^2 - p$ choices left. $|\text{Aut}(G)| = (p^2 - 1)(p^2 - p)$.

THM: If ϕ is a homomorphism from G to H , $a, b, g \in G$, $n \in \mathbb{Z}$, then

(i) $\phi(e_G) = e_H$ (ii) $\phi(g^n) = \phi(g)^n$ (iii) If $|g| < \infty$, then $|\phi(g)| \mid |g|$. (iv) $\ker \phi \leq G$.

(v) $\phi(a) = \phi(b) \Leftrightarrow b^{-1}a \in \ker \phi \Leftrightarrow a \ker \phi = b \ker \phi$. (vi) If $\phi(a) = b$, then $\phi^{-1}(b) = \{x \in G \mid \phi(x) = b\} = a \ker \phi$.²²

THM: "Properties of Subgroups under Homomorphisms" If $H \leq G$ and $\phi : G \rightarrow L$ a group homomorphism,

(i) $\phi(H)$ is a subgroup of L . (ii) If H is cyclic/abelian/normal, then $\phi(H)$ is cyclic/abelian/normal.

(iii) If $|\ker \phi| = n$, then ϕ is n -to-1 mapping from G to $\phi(G)$. (iv) If $\ker \phi = \{e\}$, then ϕ is injective.

(v) If $|H| = n$, then $|\phi(H)|$ divides n . (vi) If $K \leq L$, then $\phi^{-1}(K) = \{x \in G \mid \phi(x) \in K\}$ is a subgroup of G .

(vii) If $K \trianglelefteq L$, then $\phi^{-1}(K) \trianglelefteq G$. (viii) If ϕ surjective and $\ker \phi = \{e\}$, then ϕ is isomorphism.²³

PROP: "Recognition Theorem" Let H and K be subgroups of a group G .

(i) If $H \cap K = \{1\}$, the product map $p : H \times K \rightarrow G$ defined by $p(h, k) = hk$ is injective. $\text{im } p = HK \subseteq G$.

(ii) If either H or K is a normal subgroup of G then the product sets HK and KH are equal, and $HK \leq G$.

(iii) If H and K are both normal, $H \cap K = \{1\}$, and $HK = G$, then $G \cong H \times K$.²⁴

(iv) $|HK| = \frac{|H||K|}{|H \cap K|}$.²⁵ (v) HK is a subgroup if and only if $HK = KH$.²⁶ (vi) The number of distinct ways to write each element of HK in the form hk for some $h \in H$ and some $k \in K$ is $|H \cap K|$.²⁷

DEF: Let H be a subgroup of G . A subgroup $K \leq G$ is called a *complement* for H in G if $G = HK$ and $H \cap K = \{e\}$.²⁸

DEF: For an action of G on S , a *fixed point* of G is an element $s \in S$ such that $xs = s$ for all $x \in G$. The subset of S consisting of all elements xs for $x \in G$ is the *orbit* of s under G , denoted Gs . The set of all $x \in G$ such that $xs = s$ is called the *stabilizer* of s in G , denoted G_s .²⁹

DEF: An action of G on S is *faithful* if the map $\phi : G \rightarrow \text{Perm}(S)$ is injective. the action is *transitive* if there is only

one orbit.³⁰

PROP: Let S be a G -set, and let s be an element of S . Let H be the stabilizer of s , and let O_s be the orbit of s . There is a natural bijective map $G/H \xrightarrow{\varphi} O_s$ defined by $aH \mapsto as$. This map is comparable with the operations of G in the sense that $\varphi(gC) = g\varphi(C)$ for every coset C and every element $g \in G$.³¹

PROP: Let S be a G -set, and let $s \in S$. Let s' be an element in the orbit of s , say $s' = as$. Then A. the set of elements g of G such that $gs = s'$ is the left coset $aG_s = \{ah \mid h \in H\}$. B. The stabilizer of s' is a *conjugate subgroup* of the stabilizer of s : $G_{s'} = aG_s a^{-1} = \{aha^{-1} \mid h \in H\}$.³²

PROP: "LOIS" If G is a group operating on a set S , and $s \in S$, then $|Gs| = [G : G_s]$.³³

PROP: The number of conjugate subgroups to H is equal to the index of the normalizer in H .³⁴

THM: "Orbit Decomposition Formula" Let a group G act on a set S . Let I be an indexing set where $G_{s_i} \cap G_{s_j} \neq \emptyset \Rightarrow i = j$ for all $i, j \in I$. Then, $|S| = \sum_{i \in I} (G : G_{s_i})$.³⁵

COR: "Class Equation" Let G be a group acting on itself by conjugation. Let X be a system of distinct representatives for the conjugacy classes of G . Then, $|G| = \sum_{x \in X} (G : G_x)$.³⁶

THM: "Conjugation Action Rules" Let $a, b \in G$ and suppose $aba^{-1} = b^r$. Then, $\forall t, s$,

(i) $ab^t a^{-1} = b^{rt}$. (ii) $a^s b^t a^{-s} = b^{r^s t}$.

DEF: If N, H are groups and $\psi : H \rightarrow \text{Aut}(N)$ is a homomorphism (written $\psi(h) = \psi_h$), then there exists a *semidirect product* group $G = \{(n, h) \mid n \in N, h \in H\}$ with multiplication $(n_1, h_1) \cdot (n_2, h_2) = (n_1 \psi_{h_1}(n_2), h_1 h_2)$. Then also, $N_1 = \{(n, e_H) \mid n \in N\} \trianglelefteq G$ and $H_1 = \{(e_N, h) \mid h \in H\} \leq G$, and $G = N_1 H_1$, $N_1 \cap H_1 = \{e\}$.

DEF: A subgroup $H \leq G$ is *characteristic*, written $H \text{ char } G$, if $\sigma(H) = H$ for all $\sigma \in \text{Aut}(G)$. A group G is *characteristically simple* if G has no non-trivial proper subgroups that are characteristic.³⁷

THM: (i) If $H \text{ char } K$ and $K \text{ char } G$, then $H \text{ char } G$. (ii) If $H \text{ char } K$ and $K \trianglelefteq G$, then $H \trianglelefteq G$.

(iii) If $H \trianglelefteq G$, then $(H)_\phi \trianglelefteq G$ for any automorphism ϕ of G .

(iv) If $H \subseteq K$ are subgroups of G such that $H \text{ char } G$ and $K/H \text{ char } G/H$, then $K \text{ char } G$.³⁸

THM: If H is a normal subgroup of G whose order and index are relatively prime, then $H \text{ char } G$.³⁹

THM: A characteristically simple group is the direct product of isomorphic simple groups.⁴⁰

DEF: An *elementary* abelian p -group for p prime is $\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$.⁴¹

THM: If H is a minimal normal subgroup of G , then either H is an elementary abelian p -group for some prime p or H is the direct product of isomorphic nonabelian simple groups.⁴²

PROP: If \mathcal{A} is any nonempty collection of subgroups of G , then the intersection of all members of \mathcal{A} is also a subgroup of G .⁴³

1.3 Sylow/Solvability Problems

THM: "Sylow Theorems" Let $G = p^k m$ with p prime, and $\gcd(p, m) = 1$.

(I) If H is a p -subgroup of G , $H \leq P$, a p -Sylow subgroup of G .

(II) All p -Sylow subgroups are conjugate in G .

(III) Let s_p denote the number of p -Sylow subgroups in G . $s_p \equiv 1 \pmod{p}$, and $s_p \mid m$.⁴⁴

LMA: Let P be a p -Sylow subgroup of G . If Q is any p -subgroup of G , then $Q \cap N_G(P) = Q \cap P$.⁴⁵

LMA: Let H be a p -group acting on a finite set S . Then:

(a) The number of fixed points of H is $\equiv |S| \pmod{p}$.

(b) If H has exactly one fixed point, then $|S| \equiv 1 \pmod{p}$.

(c) If $p \mid |S|$, then the number of fixed points of H is $\equiv 0 \pmod{p}$.⁴⁶

THM: Let G be a finite p -group. Then G is solvable. If $|G| > 1$, then G has non-trivial center.⁴⁷

COR: Let G be a p -group which is not of order 1. Then there is a normal, cyclic tower $\{e\} = G_0 \leq G_1 \leq \cdots \leq G_n = G$.

LMA: Let G be a finite group and let p be the smallest prime dividing the order of G . Let H be a subgroup of index p . Then H is normal.⁴⁸

PROP: Let p, q be distinct primes and let G be a group of order pq . Then G is solvable.⁴⁹

THM: "Little Cayley" For $H \leq G$, there exists a homomorphism $\theta : G \rightarrow \text{Perm}(G/H)$ by the action of left-multiplication on the cosets of H . Then, $\ker \theta \trianglelefteq H$.⁵⁰

THM: Let $H \leq G$ and have G act on the left cosets of H by left-multiplication. Then,

(i) G acts transitively on the left cosets of H .

(ii) The stabilizer of $1H$ is H .

(iii) The kernel of the action is $K = \bigcap_{x \in G} xHx^{-1}$, and K is the largest normal subgroup of G contained in H .⁵¹

LMA: If G is a finite group, $H \leq G$, and $|H| = p^r$, p prime, then $[G : H] \equiv [N_G(H) : H] \pmod{p}$.⁵²

LMA: In a finite group G , if $s_p \not\equiv 1 \pmod{p^2}$, then there are distinct p -Sylow subgroups P and R of G such that $P \cap R$ is of index p in both P and R (hence is normal in each).⁵³

PROP: If the number of p -Sylow subgroups in G is given by $s_p = k$, there exists a homomorphism $\theta : G \rightarrow S_k$.

PROP: If $H \leq G$ and $N \trianglelefteq G$, then there exists a homomorphism $\theta : H \rightarrow \text{Aut}(N)$. The kernel, $\ker \theta = Z_N$, the centralizer of H . And, G/Z_N is isomorphic to a subgroup of $\text{Aut}(N)$.⁵⁴

COR: For any $H \leq G$, $N_G(H)/Z_H$ is isomorphic to a subgroup of $\text{Aut}(H)$. In particular, $G/Z(G)$ is isomorphic to a subgroup of $\text{Aut}(G)$.⁵⁵

PROP: "Methods for finding subgroups" Consider a group G .

- (i) Find p -Sylow subgroups.
- (ii) $N_G(H)$ for $H \leq G$.
- (iii) $N_K(H)$ for $H, K \leq G$.
- (iv) HN for $H \leq G, N \trianglelefteq G$.
- (v) $H \cap K$ for $H, K \leq G$.

PROP: For p, q prime, $p \neq q$, groups of the following orders are solvable (requires proof):

- (i) pq
- (ii) p^2q
- (iii) p^2q^2

LMA: Let $S, N, H, K \leq G, N \trianglelefteq G, S \trianglelefteq H$. Then

- (i) $SN = NS$ & $NH = HN$.
- (ii) $H \cap N \trianglelefteq H$.
- (iii) $S \cap N \trianglelefteq H, S \cap K \trianglelefteq H \cap K$.
- (iv) $NS \trianglelefteq NH$.⁵⁶

LMA: "Butterfly Lemma" Let U, V be subgroups of a group. Let $u \trianglelefteq U$ and $v \trianglelefteq V$. Then:

- (i) $u(U \cap v) \trianglelefteq u(U \cap V)$.
- (ii) $(u \cap V)v \trianglelefteq (U \cap V)v$.
- (iii) $u(U \cap V)/u(U \cap v) \cong (U \cap V)v/(u \cap V)v$.⁵⁷

PROP: Let G be a finite group. An abelian tower of G admits a cyclic refinement. Let G be a finite solvable group. Then G admits a cyclic tower whose last element is $\{e\}$.⁵⁸

THM: Let G be a group and $H \trianglelefteq G$. Then G is solvable if and only if H and G/H are solvable.⁵⁹

DEF: A *commutator* in G is an element of the form $xyx^{-1}y^{-1}$. Let G^C be the subgroup of G generated by the commutators, called the *commutator subgroup* of G .⁶⁰

DEF: The *commutator* of two subgroups $A, B \leq G$ is noted as $[A, B] = \{aba^{-1}b^{-1} \mid a \in A, b \in B\}$.⁶¹

PROP: Let G be a group and G^C be the commutator of G .

- (i) $G^C \trianglelefteq G, G/G^C$ abelian.
- (ii) $N \trianglelefteq G, G/N$ abelian implies $G^C \subseteq N$. (So, G^C is smallest normal subgroup with an abelian factor group).
- (iii) G is solvable if and only if $\exists n$ so that $\underbrace{(\dots (G^C)^C) \dots}_n^C = \{e\}$.

- (iv) For $H \leq G, H \trianglelefteq G$ if and only if $[H, G] \leq H$.
- (v) If $\varphi : G \rightarrow A$ is any homomorphism of G into an abelian group A , then there is a map $\psi : G/G^C \rightarrow A$ such that $\psi \circ \pi = \varphi$.⁶²

LMA: Suppose G is solvable, and has a solvable series of length r . Then, $G^{C^{r-1}} = \{e\}$ (where G^{C^n} denotes the n th commutator of G).

PROP: Let H be a group which operates on a set S , and let U be a subset of S . Then H stabilizes U if and only if U is a union of H -orbits.⁶³

THM: The finite group G is solvable if and only if for every divisor n of $|G|$ such that $\gcd(n, \frac{|G|}{n}) = 1$, G has a subgroup of order n .⁶⁴

THM: "The Unusables!" Let G be a finite group.

- (i) [Burnside] If $|G| = p^a q^b$ for p, q primes, then G is solvable.
- (ii) [Philip Hall] If for every prime p dividing $|G|$ we factor the order of G as $|G| = p^a m$ where $\gcd(p, m) = 1$, and G has a subgroup of order m , then G is solvable (i.e. if for all prime p , G has a subgroup whose index equals the order of a Sylow p -subgroup, then G is solvable – such subgroups are called *Sylow p -complements*).
- (iii) [Feit-Thompson] If $|G|$ is odd, then G is solvable.
- (iv) [Thompson] If for every pair of elements $x, y \in G, \langle x, y \rangle$ is a solvable group, then G is solvable.⁶⁵

1.4 Symmetric Group

PROP: "Conjugation in S_n " For $\tau = (i_1 i_2 \dots i_r)$ and r -cycle in S_n and $\sigma \in S_n, \sigma \tau \sigma^{-1} = (\sigma(i_1) \sigma(i_2) \dots \sigma(i_r))$.⁶⁶

THM: Recall automorphisms of S_n :

- (vi) If $n \neq 6$, then $\text{Aut}(S_n) \cong \text{Inn}(S_n) \cong S_n$ (every automorphism is inner).
- (vii) $[\text{Aut}(S_6) : \text{Inn}(S_6)] = 2$ and there exists an automorphism $S_6 \rightarrow S_6$.⁶⁷

THM: If $n \geq 5$, then S_n is not solvable.⁶⁸

PROP: A_n is generated by the 3-cycles. If $n \geq 5$, all 3-cycles are conjugate in A_n . If $n \geq 5, A_n$ is simple.

PROP: The permutation $\sigma \in S_n$ is odd if and only if the number of cycles of even length in its cycle decomposition is odd.⁶⁹

DEF: If $\sigma \in S_n$ is the product of disjoint cycles of length n_1, n_2, \dots, n_r with $n_i \leq n_{i+1}$, then the integers n_1, n_2, \dots, n_r are the *cycle type* of σ .⁷⁰

PROP: Two elements of S_n are conjugate in S_n if and only if they have the same cycle type. The number of conjugacy classes of S_n equals the number of partitions of n , or the n th Bell number B_n .⁷¹

PROP: (i) If G has no subgroup of index 2 and $G \leq S_k$, then $G \leq A_k$.

(ii) If P is a p -Sylow subgroup of S_k for some odd prime p , then P is a p -Sylow subgroup of A_k and $|N_{A_k}(P)| = \frac{1}{2}|N_{S_k}(P)|$.⁷²

1.5 Free/Dual Groups

DEF: Let G be a finite abelian group. Let $\hat{G} = \text{Hom}(G, \mathbb{Q}/\mathbb{Z})$.

FACT: If $f : G_1 \rightarrow G_2$, then $\exists \hat{f} : \hat{G}_2 \rightarrow \hat{G}_1$ with $\hat{f}(\sigma) = \sigma \circ f$.

FACT: $\widehat{G_1 \times G_2} \cong \hat{G}_1 \times \hat{G}_2$, for G_1, G_2 , finite abelian groups.

FACT: If $G_1 \xrightarrow{f} G_2$ is surjective, then $\hat{G}_2 \xrightarrow{\hat{f}} \hat{G}_1$ is surjective.

DEF: Let X be a set. We construct $F(X)$ defined to be the *free group on X* . If $X = \emptyset$, $F(X) = \{e\}$. If $X \neq \emptyset$, let X^{-1} be disjoint from X , $|X| = |X^{-1}|$. Let $f : X \rightarrow X^{-1}$ be a bijection, label $f(x) =: x^{-1}$. Add an element $e \notin X \cup X^{-1}$ to $S = X \cup X^{-1} \cup \{e\}$. $F(X)$ is the group of reduced concatenations of words over S .

DEF: A *word* on X is a sequence (a_1, a_2, \dots) with each $a_i \in S$, and existing a k with $a_n = e$ for all $n \geq k$. The constant (e, e, \dots) is denoted ε , the *empty word*.

DEF: A word is *reduced* if (i) $\forall x \in X$, x and x^{-1} are not adjacent. (ii) $a_n = 1 \Rightarrow a_k = 1$ for all $k \geq n$. Denote reduced words as $x_1^{\delta_1} x_2^{\delta_2} \dots x_n^{\delta_n}$ where $x_i \in X$, $\delta = \pm 1$, or ε for the empty word.

THM: If $X \neq \emptyset$, then $F(X)$ is a group and $F = \langle X \rangle$ (F is generated by $X \subseteq F(X)$).

THM: "Universal Property of Free Groups" there exists an $i : X \rightarrow F(X)$ injective and: if G is a group and $f : X \rightarrow G$ is a set map then there exists a unique $\bar{f} : F \rightarrow G$ such that $\bar{f} \circ i = f$.

COR: Every group G is the homomorphic image of a free group: Take F to be free on the generators of G . Then, $G \cong F/W$ where W is the set of relations satisfied by generators of G .

DEF: Let X be a set and Y a set of reduced words on X . A group G is said to be the *group defined by the generators X and relations $w = e$* (with $w \in Y$) provided $G \cong F/N$, where F is the free group on X and N the normal subgroup of F generated by Y . One says that $\langle X|Y \rangle$ is a *presentation* of G .

THM: Let X be a set, Y a set of reduced words on X and $G = \langle X|Y \rangle$. If H is any group such that $H = \langle X \rangle$ and H satisfies all the relations $w = e$ (with $w \in Y$) then there is a homomorphism $G \rightarrow H$.

1.6 Cardinality

THM: Let A be an infinite set. Then $\text{card}(A \times A) = \text{card}(A)$.⁷³

COR: Let A be an infinite set, and let Φ be the set of finite subsets of A . Then $\text{card}(\Phi) = \text{card}(A)$.

THM: Let A be an infinite set, and $T = \{0, 1\}$. Let M be the set of all maps of A into T . Then, $\text{card}(A) \not\leq \text{card}(M)$.⁷⁴

COR: Let A be an infinite set, and S the set of all subsets of A . Then $\text{card}(A) \not\leq \text{card}(S)$.⁷⁵

1.7 Category Theory

DEF: A *category* \mathcal{C} consists of a collection of objects and for two objects $A, B \in \mathcal{C}$, a set $\text{Hom}(A, B)$ is called the set of *morphisms* from A to B . For three objects $A, B, C \in \mathcal{C}$, a law of composition: $\text{Hom}(B, C) \times \text{Hom}(A, B) \rightarrow \text{Hom}(A, C)$, satisfying the axioms:

(CAT 1) Two sets $\text{Hom}(A, B)$ and $\text{Hom}(A', B')$ are disjoint unless $A = A'$ and $B = B'$, in which case they are equal.

(CAT 2) For each object A of \mathcal{C} , there is a morphism $\text{id}_A \in \text{Hom}(A, A)$ which acts as right and left identity on the elements of $\text{Hom}(A, B)$ and $\text{Hom}(B, A)$, respectively.

(CAT 3) The law of composition is associative.⁷⁶

DEF: The *product* of $\{A_i\}_{i \in I}$ in the category \mathcal{C} is a $P \in \mathcal{C}$ such that there exist maps $\pi_i : P \rightarrow A_i$ so that if there exists a $D \in \mathcal{C}$ with maps $\varphi_i : D \rightarrow A_i$ there exists a unique $\varphi : D \rightarrow P$ so that $\varphi_i = \pi_i \circ \varphi$.⁷⁷

DEF: The *coproduct* of $\{A_i\}_{i \in I}$ in the category \mathcal{C} is a $P \in \mathcal{C}$ such that there exist maps $\tau_i : A_i \rightarrow P$ so that if there exists a $D \in \mathcal{C}$ with maps $\psi_i : A_i \rightarrow D$ there exists a unique $\psi : P \rightarrow D$ so that $\psi_i = \tau_i \circ \psi$.⁷⁸

DEF: For some $X, Y, Z \in \mathcal{C}$, with morphisms $f : X \rightarrow Z$ and $g : Y \rightarrow Z$, the *fiber product* (or *pull-back*) of f and g in \mathcal{C} is an object $P \in \mathcal{C}$ with morphisms $p_1 : P \rightarrow X$, $p_2 : P \rightarrow Y$ such that $f \circ p_1 = g \circ p_2$ with the addition that if $Q \in \mathcal{C}$ with morphisms $\phi : Q \rightarrow X$ and $\gamma : Q \rightarrow Y$ with $f \circ \phi = g \circ \gamma$, there exists a unique morphism $p : Q \rightarrow P$ such that $f \circ p_1 \circ p = g \circ p_2 \circ p$.

DEF: For some $X, Y, Z \in \mathcal{C}$, with morphisms $f : Z \rightarrow X$ and $g : Z \rightarrow Y$, the *fiber coproduct* (or *push-out*) of f and g in \mathcal{C} is an object $P \in \mathcal{C}$ with morphisms $p_1 : X \rightarrow P$, $p_2 : Y \rightarrow P$ such that $p_1 \circ f = p_2 \circ g$ with the addition that if $Q \in \mathcal{C}$ with morphisms $\phi : X \rightarrow Q$ and $\gamma : Y \rightarrow Q$ with $\phi \circ f = \gamma \circ g$, there exists a unique morphism $p : P \rightarrow Q$ such that $p \circ p_1 \circ f = p \circ p_2 \circ g$.

PROP: Products/Coproducts/Pull-backs/Push-outs, if they exist, are unique.

DEF: Let \mathcal{C}, \mathcal{D} be categories. A *covariant functor* $F : \mathcal{C} \rightarrow \mathcal{D}$ is a rule so that $\forall C \in \mathcal{C}, F(C) \in \mathcal{D}, \forall f \in \text{Arr}(\mathcal{C})$, say $f : A \rightarrow B, A, B \in \mathcal{C}, F(f) : F(A) \rightarrow F(B)$. F satisfies

(F1) $\forall C \in \mathcal{C}, F(\text{id}_C) = \text{id}_{F(C)}$.

(F2) If $A \xrightarrow{f} B \xrightarrow{g} C$ in \mathcal{C} , then $F(g \circ f) = F(g) \circ F(f)$.

DEF: A *contravariant functor* G satisfies similar properties, except $f : A \rightarrow B \Rightarrow G(f) : G(B) \rightarrow G(A)$.

Artin: Algebra by Michael Artin.

D&F: Abstract Algebra by Dummit & Foote.

H: Algebra by Thomas W. Hungerford.

Lang: Algebra by Serge Lang.

Notes

¹D&F. Theorem 16. p.97.

²D&F. Corollary 17. p. 97.

³D&F. Theorem 18. p.97.

⁴D&F. Theorem 19. p. 98.

⁵D&F. Theorem 20. p. 99.

⁶D&F. Theorem 3. p.158.

⁷D&F. Theorem 5. p. 161.

⁸D&F. p. 161.

⁹D&F. p. 165.

¹⁰D&F. p. 76.

¹¹D&F. Proposition 4. p. 80.

¹²Lang, p. 14; D&F, p. 50.

¹³Lang, p.14; D&F, p. 49.

¹⁴Lang, Chapter 1, Prop 4.1. p.24.

¹⁵D&F, Proposition 5, p. 57.

¹⁶D&F, Proposition 6. p. 57.

¹⁷Lang, Chapter 1, Prop 4.2. p.24.

¹⁸Lang, Chapter 1, Prop 4.3. pp. 24-25.

¹⁹Gallian 6.2, 6.3 pp. 126-127

²⁰Described in Dummit&Foote p. 222, #10

²¹Gallian 6.5, p. 131; D&F, Prop 17 p. 136.

²²Gallian, 10.1

²³Gallian, Theorem 10.2

²⁴Artin, Section 2.8.

²⁵D&F. Proposition 13. p. 93.

²⁶D&F. Proposition 14. p. 94.

²⁷D&F. Proposition 8. p. 171.

²⁸D&F. p.180.

²⁹Lang, p. 15.

³⁰Lang, p. 15.

³¹Artin, Section 5.6.

³²Artin, Section 5.6.

³³Lang, Chapter 1. Prop 5.1. p.15.

³⁴Lang, Chapter 1. Prop 5.2. p.15.

³⁵Lang, p.29.

³⁶Lang, p.29.

³⁷S. Wiegand, Sept 28,2007; Gorenstein 1968

³⁸S. Wiegand Sept 28,2007, handouts, Theorem 1.2.

³⁹S. Wiegand, Sept 28,2007, handouts, Theorem 1.3.

⁴⁰S. Wiegand, Sept 28,2007, handouts, Theorem 1.4.

⁴¹S. Wiegand, Sept 28,2007; Gorenstein 1968

⁴²S. Wiegand Sept 28,2007, handouts, Theorem 1.5.

⁴³D&F. Proposition 8. p. 62.

⁴⁴Lang, Chapter 1, Theorem 6.4, pp. 34-35.

⁴⁵D&F. Lemma 19. p. 140.

⁴⁶Lang, Chapter 1, Lemma 6.3, p. 34.

⁴⁷Lang, Chapter 1, Theorem 6.5, p. 35

⁴⁸Lang, Chapter 1, Lemma 6.7. p. 36

⁴⁹Lang, Chapter 1, Proposition 6.8. p.36

⁵⁰S. Wiegand Sept 10, 2007 handout.

⁵¹D&F. Theorem 3. p.119.

⁵²Hungerford, Lemma 5.5 p. 94.

⁵³D&F. Lemma 13. p. 207.

⁵⁴D&F. Proposition 13. p.133.

⁵⁵D&F. Corollary 15. p.134.

⁵⁶S. Wiegand, Sept 10, 2007, handout. Lma for Butterfly Lma.

⁵⁷Lang, Chapter 1. Lemma 3.3. pp. 20-21.

⁵⁸Lang, Chapter 1. Proposition 3.1. p.18

⁵⁹R. Wiegand, "Galois Theory Review" Lemma 3.6,3.7.

⁶⁰Lang, p.20

⁶¹D&F. p.169.

⁶²D&F. Proposition 7. p.169.

⁶³Artin, Section 6.2.

⁶⁴D&F. p. 105.

⁶⁵D&F. Theorem 11. p. 196.

⁶⁶D&F. Proposition 10. p. 125.

⁶⁷Described in Dummit&Foote p. 222, #10

⁶⁸Lang, Chapter 1, Theorem 5.4. p. 31.

⁶⁹D&F. Proposition 25. p.110.

⁷⁰D&F. p.126.

⁷¹D&F. Proposition 11. p. 126.

⁷²D&F. Proposition 12. p. 204.

⁷³Lang, Appendix 2, Theorem 3.6. p. 888.

⁷⁴Lang Appendix 2. Theorem 3.10, p.890.

⁷⁵Lang Appx 2. Cor 3.11, p. 891. Hungerford, Thm 8.5. p. 17.

⁷⁶Lang, p. 57.

⁷⁷Lang, p. 58.

⁷⁸Lang, p. 59.

2 Rings

2.1 Definitions

DEF: A *ring* is a nonempty set R together with binary operations (addition and multiplication) such that

(i) $(R, +)$ is an abelian group. (ii) Multiplication is associative. (iii) $a(b+c) = ab+ac, \forall a, b, c \in R$ (distributive law)

If in addition, (iv) $ab = ba$ for all $a, b \in R$ then R is *commutative*. If R contains an element 1_R such that

(v) $1_R a = a = a 1_R$ for all $a \in R$, then R is said to be a *ring with identity*.⁷⁹

THM: Let R be a ring, $a, b \in R$, and 0 be the additive identity. Then

(i) $0a = a0 = 0$; (ii) $(-a)b = a(-b) = -(ab)$; (iii) $(-a)(-b) = ab$;

(iv) $(na)b = a(nb) = n(ab)$ for all $n \in \mathbb{Z}$; (v) $(\sum_{i=1}^n a_i) (\sum_{j=1}^m b_j) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j$ for all $a_i, b_j \in R$.⁸⁰

DEF: A nonzero element a in a ring R is a *left [right] zero divisor* if there is a nonzero $b \in R$ such that $ab = 0$ [$ba = 0$].

A *zero divisor* is an element of R which is both a left and right zero divisor.⁸¹

DEF: An element a in a ring R with identity is said to be *left [right] invertible* if there exists a $c \in R$ [$b \in R$] such that $ca = 1_r$ [$ab = 1_R$]. The element c [b] is called a *left [right] inverse* of a . An element $a \in R$ that is both left and right invertible is said to be *invertible* or to be a *unit*.⁸²

THM: “Binomial Theorem” Let R be a ring with identity, n a positive integer, and $a, b, a_1, a_2, \dots, a_s \in R$.

(i) if $ab = ba$, then $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$;

(ii) If $a_i a_j = a_j a_i$ for all i, j , then $(a_1 + a_2 + \dots + a_s)^n = \sum \frac{n!}{(i_1! \dots (i_s!) } a_1^{i_1} a_2^{i_2} \dots a_s^{i_s}$,

where the sum is over all s -tuples (i_1, i_2, \dots, i_s) such that $i_1 + i_2 + \dots + i_s = n$.⁸³

DEF: Let R and S be rings. A function $f: R \rightarrow S$ is a *homomorphism of rings* provided that for all $a, b \in R$, $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.⁸⁴ A *monomorphism [epimorphism, isomorphism] of rings* is a homomorphism of rings which is injective [surjective, bijective]. A monomorphism of rings $R \rightarrow S$ is also called an *embedding* of R in S . An isomorphism $R \rightarrow R$ is an *automorphism* of R . The *kernel* of a homomorphism is the kernel as a map of additive groups.⁸⁵

DEF: Let R be a ring. If there is a least positive integer n such that $na = 0$ for all $a \in R$, then R is said to have *characteristic n* , written $\text{char } R = n$. If no such n exists, R is said to have *characteristic zero*.⁸⁶

THM: Let R be a ring with identity 1_R and characteristic $n > 0$.

(i) If $\varphi: \mathbb{Z} \rightarrow R$ is the map given by $m \mapsto m1_R$, then φ is a homomorphism of rings with kernel $\langle n \rangle = \{kn | k \in \mathbb{Z}\}$.

(ii) n is the least positive integer such that $n1_R = 0$.

(iii) If R has no zero divisors (in particular if R is an integral domain) then n is prime.⁸⁷

THM: Every ring R may be embedded in a ring S with identity. The ring S (which is not unique) may be chosen to be either characteristic zero or of the same characteristic as R .⁸⁸

DEF: An element of a ring is *nilpotent* if $a^n = 0$ for some n .⁸⁹

2.2 Ideals

DEF: Let R be a ring and S a nonempty subset of R that is closed under the operations of addition and multiplication in R . If S is itself a ring under these operations then S is called a *subring* of R . A subring I of a ring R is called a *left ideal* provided $r \in R$ and $x \in I$ implies $rx \in I$. I is a *right ideal* provided $r \in R$ and $x \in I$ implies $xr \in I$. I is an *ideal* (or *two-sided ideal* for emphasis) if it is both a left and right ideal.⁹⁰

DEF: The *center* of R is the set $C = \{c \in R | cr = rc \forall r \in R\}$. C is a subring of R but may not be an ideal.⁹¹

DEF: Every ring R has at least two ideals, R itself and the *trivial ideal*: the set $0 = \{0_R\}$. An ideal I is called *proper* if $I \neq 0$ and $I \neq R$.⁹²

THM: A nonempty subset I of a ring R is a left [right] ideal if and only if for all $a, b \in I$ and $r \in R$:

(i) $a - b \in I$; and (ii) $ra \in I$.⁹³

COR: Let $\{A_i | i \in I\}$ be a family of [left] ideals in a ring R . Then $\bigcap_{i \in I} A_i$ is also a [left] ideal.⁹⁴

DEF: Let X be a subset of a ring R . Let $\{A_i | i \in I\}$ be the family of all [left] ideals in R which contain X . Then $\bigcap_{i \in I} A_i$ is called the [left] *ideal generated by X* . This ideal is denoted $\langle X \rangle$. The elements of X are called *generators* of the ideal $\langle X \rangle$. If X is finite, then $\langle X \rangle$ is *finitely generated*. An element generated by a single element is called a *principal ideal*. A *principal ideal ring* is a ring in which every ideal is principal.⁹⁵

THM: Let R be a ring and $a \in R$ and $X \subseteq R$.

(i) The principal ideal $\langle a \rangle$ consists of all elements of the form $ra + as + na + \sum_{i=1}^m r_i a s_i$ for $r, s, r_i, s_i \in R, m \in \mathbb{N}$,

and $n \in \mathbb{Z}$;

(ii) If R has an identity, then $\langle a \rangle = \{\sum_{i=1}^n r_i a s_i \mid r_i, s_i \in R, n \in \mathbb{N}\}$;

(iii) If a is in the center of R , then $\langle a \rangle = \{\sum_{i=1}^m r_i a + n a \mid r_i \in R, m \in \mathbb{N}, n \in \mathbb{Z}\}$;

(iv) $Ra = \{ra \mid r \in R\}$ is a left ideal in R . If R has an identity, then $a \in Ra$. Define aR similarly as a right ideal.

(v) If R has an identity and a is in the center of R , then $Ra = \langle a \rangle = aR$.

(vi) If R has an identity and X is in the center of R , then the ideal $\langle X \rangle$ consists of all finite sums $r_1 a_1 + \cdots + r_n a_n$, where $n \in \mathbb{N}, r_i \in R, a_i \in X$.⁹⁶

THM: Let A, A_1, \dots, A_n, B and C be [left] ideals in a ring R .

(i) $A_1 + A_2 + \cdots + A_n$ and $A_1 A_2 \cdots A_n$ are [left] ideals;

(ii) $(A + B) + C = A + (B + C)$; (iii) $(AB)C = ABC = A(BC)$;

(iv) $B(A_1 + A_2 + \cdots + A_n) = BA_1 + \cdots + BA_n$ and $(A_1 + \cdots + A_n)C = A_1 C + \cdots + A_n C$.⁹⁷

THM: Let R be a ring and I an ideal of R . Then the additive quotient group R/I is a ring with multiplication given by

$(a + I)(b + I) = ab + I$. If R is commutative or has an identity, then the same is true of R/I .⁹⁸

THM: If $f : R \rightarrow S$ is a homomorphism of rings, then the kernel of f is an ideal in R . Conversely, if I is an ideal in R , then the map $\pi : R \rightarrow R/I$ given by $r \mapsto r + I$ is an epimorphism of rings with kernel I . The map π is called the *canonical epimorphism* (or *projection*) onto R/I .⁹⁹

THM: If $f : R \rightarrow S$ is a homomorphism of rings and I is an ideal of R which is contained in the kernel of f , then there is a unique homomorphism of rings $\bar{f} : R/I \rightarrow S$ such that $\bar{f}(a + I) = f(a)$ for all $a \in R$. $\text{im } \bar{f} = \text{im } f$ and $\ker \bar{f} = (\ker f)/I$. \bar{f} is an isomorphism if and only if f is an epimorphism and $I = \ker f$.¹⁰⁰

COR: "First Isomorphism Theorem of Rings" If $f : R \rightarrow S$ is a homomorphism of rings, then f induces an isomorphism of rings $R/\ker f \cong \text{im } f$.¹⁰¹

COR: If $f : R \rightarrow S$ is a homomorphism of rings, I is an ideal in R and J is an ideal in S such that $f(I) \subseteq J$, then f induces a homomorphism of rings $\bar{f} : R/I \rightarrow S/J$, given by $a + I \mapsto f(a) + J$, \bar{f} is an isomorphism if and only if $\text{im } f + J = S$ and $f^{-1}(J) \subseteq I$. In particular, if f is an epimorphism such that $f(I) = J$ and $\ker f \subseteq I$, then \bar{f} is an isomorphism.¹⁰²

THM: Let I and J be ideals in a ring R .

(i) "Second Isomorphism Theorem" there is an isomorphism of rings $I/(I \cap J) \cong (I + J)/J$;

(ii) "Third Isomorphism Theorem" if $I \subseteq J$, then J/I is an ideal of R/I and there is an isomorphism of rings $(R/I)/(J/I) \cong R/J$.¹⁰³

THM: "Ideal Correspondence Theorem" If I is an ideal in a ring R , then there is a one-to-one correspondence between the set of all ideals of R which contain I and the set of all ideals of R/I , given by $J \mapsto J/I$. Hence every ideal in R/I is of the form J/I , where J is an ideal of R which contains I .¹⁰⁴

DEF: An ideal P in a ring R is said to be *prime* if $P \neq R$ and for any ideals A, B in R , $AB \subseteq P$ implies $A \subseteq P$ or $B \subseteq P$.¹⁰⁵

THM: If P is an ideal in a ring R such that $P \neq R$ and for all $a, b \in R$ $ab \in P$ implies $a \in P$ or $b \in P$, then P is prime. Conversely, if P is prime and R is commutative, then the reverse holds.¹⁰⁶

DEF: An ideal [left ideal] M in a ring R is *maximal* [left maximal] if $M \neq R$ and for every [left] ideal N such that $M \subseteq N \subseteq R$ then either $N = M$ or $N = R$.¹⁰⁷

PROP: Let R be a commutative ring with an ideal I .

(i) I is prime if and only if R/I is an integral domain.

(ii) I is maximal if and only if R/I is a field.¹⁰⁸

THM: In a nonzero ring R with identity maximal [left] ideals always exist. In fact, every [left] ideal in R (except R itself) is contained in a maximal [left] ideal.¹⁰⁹

THM: If R is a commutative ring such that $R^2 = R$ (in particular if R has an identity), then every maximal ideal M in R is prime.¹¹⁰

EX: Given a ring R with $R^2 = R$, it is not true that every prime ideal is maximal: Consider $0 \subseteq \mathbb{Z}$, prime but not maximal.¹¹¹

THM: Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and $\prod_{i \in I} R_i$ the direct product of the additive abelian groups R_i ;

(i) $\prod_{i \in I} R_i$ is a ring with multiplication defined by $\{a_i\}_{i \in I} \{b_i\}_{i \in I} = \{a_i b_i\}_{i \in I}$, called the (*external*) *direct product* of the family $\{R_i\}$; (ii) If R_i has an identity [is commutative] for every $i \in I$, then $\prod_{i \in I} R_i$ has an identity [is commutative].

(iii) for each $k \in I$ the canonical projection $\pi_k : \prod_{i \in I} R_i \rightarrow R_k$ given by $\{a_i\} \mapsto a_k$, is an epimorphism of rings;

(iv) for each $k \in I$ the canonical injection $\iota_k : R_k \rightarrow \prod_{i \in I} R_i$, given by $a_k \mapsto \{a_i\}$ where $a_i = 0$ for $i \neq k$, is a monomorphism of rings.¹¹²

THM: Let $\{R_i \mid i \in I\}$ be a nonempty family of rings, S a ring and $\{\varphi_i : S \rightarrow R_i \mid i \in I\}$ a family of homomorphisms of rings. Then there is a unique homomorphism of rings $\varphi : S \rightarrow \prod_{i \in I} R_i$ such that $\pi_i \varphi = \varphi_i$ for all $i \in I$. The ring $\prod_{i \in I} R_i$ is uniquely determined up to isomorphism by this property. In other words, $\prod_{i \in I} R_i$ is a product in the category of rings.¹¹³

THM: Let A_1, \dots, A_n be ideals in a ring R such that (i) $A_1 + \dots + A_n = R$ and (ii) For each k , $A_k \cap (A_1 + \dots + A_{k-1} + A_{k+1} + \dots + A_n) = 0$. Then there is a ring isomorphism $R \cong A_1 \times \dots \times A_n$. R is said to be the (*internal*) *direct product* of the ideals A_i .¹¹⁴

DEF: Let A be an ideal in a ring R and $a, b \in R$. The element a is said to be *congruent* to b modulo A (denoted $a \equiv b \pmod{A}$) if $a - b \in A$. Thus, $a \equiv b \pmod{A} \Leftrightarrow a - b \in A \Leftrightarrow a + A = b + A$.¹¹⁵

THM: “Chinese Remainder Theorem” Let A_1, \dots, A_n be ideals in a ring R such that $R^2 + A_i = R$ for all i and $A_i + A_j = R$ for all $i \neq j$. If $b_1, \dots, b_n \in R$, then there exists $b \in R$ such that $b \equiv b_i \pmod{A_i}$ for all i . Furthermore, b is uniquely determined up to congruence modulo the ideal $A_1 \cap A_2 \cap \dots \cap A_n$.¹¹⁶

COR: Let m_1, m_2, \dots, m_n be positive integers such that $\gcd(m_i, m_j) = 1$ for $i \neq j$. If b_1, \dots, b_n are any integers, then the system of congruences $x \equiv b_i \pmod{m_i}$ has an integral solution that is uniquely determined modulo $m = m_1 m_2 \dots m_n$.¹¹⁷

COR: If A_1, \dots, A_n are ideals in a ring R , then there is a monomorphism of rings $\theta : R/(A_1 \cap \dots \cap A_n) \rightarrow R/A_1 \times \dots \times R/A_n$. If $R^2 + A_i = R$ for all i and $A_i + A_j = R$ for all $i \neq j$ then θ is an isomorphism.¹¹⁸

DEF: An element e in a ring R is said to be *idempotent* if $e^2 = e$. Idempotent elements e_1, \dots, e_n in a ring R are said to be *orthogonal* if $e_i e_j = 0$ for $i \neq j$. An element of the center of the ring R is said to be *central*.¹¹⁹

2.3 Domains and Factorization

DEF: A commutative ring R with identity $1_R \neq 0$ and no zero divisors is called an *integral domain*. A ring D with identity $1_D \neq 0$ in which every nonzero element is a unit is called a *division ring*. A *field* is a commutative division ring.¹²⁰

EX: The zero ideal in any integral domain is prime since $ab = 0$ if and only if $a = 0$ or $b = 0$.¹²¹

THM: In a commutative ring R with identity 1_R , an ideal P is prime if and only if the quotient ring R/P is an integral domain.¹²²

THM: Let M be an ideal in a ring R with identity $1_R \neq 0$.

(i) If M is maximal and R is commutative, then the quotient ring R/M is a field.

(ii) If the quotient ring R/M is a division ring, then M is maximal.¹²³

COR: The following conditions on a commutative ring R with identity $1_R \neq 0$ are equivalent:

(i) R is a field; (ii) R has no proper ideals; (iii) 0 is a maximal ideal in R ;

(iv) every nonzero homomorphism of rings $R \rightarrow S$ is a monomorphism.¹²⁴

DEF: A principal ideal ring which is an integral domain is called a *principal ideal domain*.¹²⁵

DEF: A nonzero element a of a commutative ring R is said to *divide* an element $b \in R$ (noted $a \mid b$) if there exists $x \in R$ such that $ax = b$. Elements a, b of R are said to be *associates* if $a \mid b$ and $b \mid a$.¹²⁶

THM: Let a, b and u be elements of a commutative ring R with identity.

(i) $a \mid b$ if and only if $\langle b \rangle \subseteq \langle a \rangle$;

(ii) a and b are associates if and only if $\langle a \rangle = \langle b \rangle$;

(iii) u is a unit if and only if $u \mid r$ for all $r \in R$;

(iv) u is a unit if and only if $\langle u \rangle = R$;

(v) The relation “ a is an associate of b ” is an equivalence relation on R .

(vi) If $a = br$ with $r \in R$ a unit, then a and b are associates. If R is an integral domain, the converse is true.¹²⁷

DEF: Let R be a commutative ring with identity. An element c of R is *irreducible* provided that :

(i) c is a nonzero nonunit; (ii) $c = ab$ implies a or b is a unit.

An element p of R is *prime* provided that:

(i) p is a nonzero nonunit; (ii) $p \mid ab$ implies $p \mid a$ or $p \mid b$.¹²⁸

THM: Let p and c be nonzero elements in an integral domain R .

(i) p is prime if and only if $\langle p \rangle$ is a nonzero prime ideal;

(ii) c is irreducible if and only if $\langle c \rangle$ is maximal in the set S of all proper principal ideals of R ;

(iii) Every prime element of R is irreducible;

(iv) If R is a principal ideal domain, then p is prime if and only if p is irreducible;

(v) Every associate of an irreducible [prime] element of R is irreducible [prime].

(vi) The only divisors of an irreducible element of R are its associates and the units of R .¹²⁹

DEF: An integral domain R is a *unique factorization domain* provided that:

- (i) every nonzero nonunit element a of R can be written $a = c_1 c_2 \cdots c_n$ with c_1, \dots, c_n irreducible.
- (ii) If $a = c_1 c_2 \cdots c_n$ and $a = d_1 d_2 \cdots d_m$ (c_i, d_i irreducible), then $n = m$ and for some permutation $\sigma \in S_n$, c_i and $d_{\sigma(i)}$ are associates for every i .¹³⁰

LMA: If R is a principal ideal ring and $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \cdots$ is a chain of ideals in R , then for some positive integer n , $\langle a_j \rangle = \langle a_n \rangle$ for all $j \geq n$.¹³¹

THM: Every principal ideal domain R is a unique factorization domain.¹³²

DEF: Let \mathbb{N}_0 be the set of nonnegative integers and R a commutative ring. R is a *Euclidean ring* if there is a function $\varphi : R \setminus \{0\} \rightarrow \mathbb{N}_0$ such that

- (i) if $a, b \in R$ and $ab \neq 0$, then $\varphi(a) \leq \varphi(ab)$;
- (ii) if $a, b \in R$ and $b \neq 0$, then there exist $q, r \in R$ such that $a = qb + r$ with $r = 0$, or $r \neq 0$ and $\varphi(r) < \varphi(b)$.

A Euclidean ring that is an integral domain is called a *Euclidean domain*.¹³³

EX: The *Gaussian integers*, $\mathbb{Z}[i]$, are a Euclidean domain. Define $\varphi(a + bi) = a^2 + b^2$.¹³⁴

THM: Every Euclidean ring R is a principal ideal ring with identity. Consequently every Euclidean domain is a unique factorization domain.¹³⁵

DEF: Let X be a nonempty subset of a commutative ring R . An element $d \in R$ is a *greatest common divisor* of X provided:

- (i) $d \mid a$ for all $a \in X$;
- (ii) $c \mid a$ for all $a \in X$ implies $c \mid d$.

If R has an identity and a_1, \dots, a_n have greatest common divisor 1_R , then these elements are *relatively prime*.¹³⁶

THM: Let a_1, \dots, a_n be elements of a commutative ring R with identity.

- (i) $d \in R$ is a greatest common divisor of $\{a_1, \dots, a_n\}$ such that $d = r_1 a_1 + \cdots + r_n a_n$ for some $r_i \in R$ if and only if $\langle d \rangle = \langle a_1 \rangle + \cdots + \langle a_n \rangle$;
- (ii) If R is a principal ideal ring, then a greatest common divisor of a_1, \dots, a_n exists and every one is of the form $r_1 a_1 + \cdots + r_n a_n$, $r_i \in R$;
- (iii) if R is a unique factorization domain, then there exists a greatest common divisor of a_1, \dots, a_n .¹³⁷

2.4 Polynomial Rings

Sections: Hungerford III.5,

THM: Let R be a ring and let $R[x]$ denote the set of all sequences of elements of $R(a_0, a_1, \dots)$ such that $a_i = 0$ for all but a finite number of indices i , called the *ring of polynomials* over R .

- (i) $R[x]$ is a ring.
- (ii) if R is commutative [ring with identity, integral domain], then so is $R[x]$.
- (iii) The map $R \rightarrow R[x]$ given by $r \mapsto (r, 0, 0, \dots)$ is a monomorphism of rings.¹³⁸

THM: Let R be a ring and denote by $R[x_1, \dots, x_n]$ the set of all functions $f : \mathbb{N}_0^n \rightarrow R$ such that $f(u) \neq 0$ for at most a finite number of elements $u \in \mathbb{N}_0^n$. $R[x_1, \dots, x_n]$ is called the *ring of polynomials in n indeterminants* over R .

- (i) $R[x_1, \dots, x_n]$ is a ring.
- (ii) If R is commutative [ring with identity, has no zero divisors, integral domain], then so is $R[x_1, \dots, x_n]$.
- (iii) The map $R \rightarrow R[x_1, \dots, x_n]$ given by $r \mapsto f_r$, where $f_r(0, 0, \dots, 0) = r$ and $f(u) = 0$ otherwise, is a monomorphism of rings.¹³⁹

THM: "Evaluation Principle" Let R and S be commutative rings with identity and $\varphi : R \rightarrow S$ a homomorphism of rings such that $\varphi(1_R) = 1_S$. If $s_1, s_2, \dots, s_n \in S$, then there is a unique homomorphism of rings $\bar{\varphi} : R[x_1, \dots, x_n] \rightarrow S$ such that $\bar{\varphi}|_R = \varphi$ and $\bar{\varphi}(x_i) = s_i$ for $i = 1, 2, \dots, n$. This property completely determines the polynomial ring $R[x_1, \dots, x_n]$ up to isomorphism.¹⁴⁰

COR: If $\varphi : R \rightarrow S$ is a homomorphism of commutative rings and $s_1, \dots, s_n \in S$, then the map $R[x_1, \dots, x_n] \rightarrow S$ given by $f \mapsto \varphi f(s_1, \dots, s_n)$ is a homomorphism of rings.¹⁴¹

COR: Let R be a commutative ring with identity and n a positive integer. For each k ($1 \leq k \leq n$) there are isomorphisms of rings $R[x_1, \dots, x_k][x_{k+1}, \dots, x_n] \cong R[x_1, \dots, x_n] \cong R[x_{k+1}, \dots, x_n][x_1, \dots, x_k]$.¹⁴²

PROP: Let R be a ring and denote by $R[[x]]$ the set of all sequences of elements of $R(a_0, a_1, \dots)$. This is called the *ring of formal power series* over R .

- (i) $R[[x]]$ is a ring.
- (ii) The polynomial ring $R[x]$ is a subring of $R[[x]]$.
- (iii) If R is commutative [ring with identity, has no zero divisors, integral domain] then so is $R[[x]]$.¹⁴³

PROP: Let R be a ring with identity and $f = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$.

- (i) f is a unit in $R[[x]]$ if and only if its constant term a_0 is a unit in R .

(ii) If a_0 is irreducible in R , then f is irreducible in $R[[x]]$.¹⁴⁴

COR: If R is a division ring, then the units in $R[[x]]$ are precisely those power series with nonzero constant term. The principal ideal $\langle x \rangle$ consists precisely of the nonunits in $R[[x]]$ and is the unique maximal ideal of $R[[x]]$. Thus if R is a field, $R[[x]]$ is a local ring.¹⁴⁵

DEF: The *degree of a monomial* $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n} \in R[x_1, \dots, x_n]$ is the nonnegative integer $k_1 + k_2 + \cdots + k_n$. The (*total degree of the polynomial* $f \in R[x_1, \dots, x_n]$ is the maximum of the degrees of the monomials $a_ix_1^{k_{i,1}}\cdots x_n^{k_{i,n}}$ such that $a_i \neq 0$. A polynomial which is a sum of monomials, each of which has degree k , is *homogeneous of degree k* .¹⁴⁶

THM: Let R be a ring and $f, g \in R[x_1, \dots, x_n]$.

(i) $\deg(f + g) \leq \max\{\deg f, \deg g\}$. (ii) $\deg(fg) \leq \deg f + \deg g$.

(iii) If R has no zero divisors, $\deg(fg) = \deg f + \deg g$.

(iv) If $n = 1$ and the leading coefficient of f or g is not a zero divisor in R (in particular, if it is a unit), then $\deg(fg) = \deg f + \deg g$.¹⁴⁷

THM: “Division Algorithm” Let R be a ring with identity and $f, g \in R[x]$ nonzero polynomials such that the leading coefficient of g is a unit in R . Then there exist unique polynomials $q, r \in R[x]$ such that $f = qg + r$ and $\deg r < \deg g$.¹⁴⁸

COR: “Remainder Theorem” Let R be a ring with identity and $f(x) = \sum_{i=0}^n a_i x^i \in R[x]$. For any $c \in R$ there exists a unique $q(x) \in R[x]$ such that $f(x) = q(x)(x - c) + f(c)$.¹⁴⁹

COR: If F is a field, then the polynomial ring $F[x]$ is a Euclidean domain, whence $F[x]$ is a PID, UFD. The units in $F[x]$ are precisely the nonzero constant polynomials.¹⁵⁰

DEF: Let R be a subring of a commutative ring S , $c_1, c_2, \dots, c_n \in S$ and $f = \sum_{i=0}^n a_i x_1^{k_{i,1}} \cdots x_n^{k_{i,n}} \in R[x_1, \dots, x_n]$ a polynomial such that $f(c_1, \dots, c_n) = 0$. Then (c_1, \dots, c_n) is a *root* or *zero* of f (or a *solution* of the polynomial equation $f(x_1, \dots, x_n) = 0$).¹⁵¹

THM: Let R be a commutative ring with identity and $f \in R[x]$. Then $c \in R$ is a root of f if and only if $x - c$ divides f .¹⁵²

THM: If D is an integral domain contained in an integral domain E and $f \in D[x]$ has degree n , then f has at most n distinct roots in E .¹⁵³

PROP: “Rational Roots Theorem” Let D be a UFD with quotient field F and let $f = \sum_{i=0}^n a_i x^i \in D[x]$. If $u = c/d \in F$ with c and d relatively prime, and u is a root of f , then c divides a_0 and d divides a_n .¹⁵⁴

LMA: Let D be an integral domain and $f = \sum_{i=0}^n a_i x^i \in D[x]$. Let $f' \in D[x]$ be the polynomial $f' = \sum_{k=1}^n k a_k x^{k-1}$, the *formal derivative* of f . Then for all $f, g \in D[x]$ and $c \in D$:

(i) $(cf)' = cf'$; (ii) $(f + g)' = f' + g'$; (iii) $(fg)' = f'g + fg'$; $(g^n)' = ng^{n-1}g'$.¹⁵⁵

THM: Let D be an integral domain which is a subring of an integral domain E . Let $f \in D[x]$ and $c \in E$.

(i) c is a multiple root of f if and only if $f(c) = 0$ and $f'(c) = 0$.

(ii) If D is a field and f is relatively prime to f' , then f has no multiple roots in E .

(iii) If D is a field, f is irreducible in $D[x]$ and E contains a root of f , then f has no multiple roots in E if and only if $f' \neq 0$.¹⁵⁶

DEF: Let D be a UFD and let $f = \sum_{i=0}^n a_i x^i$ a nonzero polynomial in $D[x]$. A greatest common divisor of a_0, a_1, \dots, a_n is called a *content* of f , denoted $C(f)$. If $a \in D$ and $f \in D[x]$, then $C(af)$ and $aC(f)$ are the same up to associates.

If $f \in D[x]$ and $C(f)$ is a unit in D , then f is said to be *primitive*.¹⁵⁷

LMA: “Gauss’s Lemma” If D is a unique factorization domain and $f, g \in D[x]$, then $C(fg) = C(f)C(g)$. In particular, the product of primitive polynomials is primitive.¹⁵⁸

LMA: Let D be a UFD with quotient field F and let f and g be primitive polynomials in $D[x]$. Then f and g are associates in $D[x]$ if and only if they are associates in $F[x]$.¹⁵⁹

LMA: Let D be a UFD with quotient field F and f a primitive polynomial of positive degree in $D[x]$. Then f is irreducible in $D[x]$ if and only if f is irreducible in $F[x]$.¹⁶⁰

THM: If D is a UFD, then so is the polynomial ring $D[x_1, \dots, x_n]$.¹⁶¹

THM: “Eisenstein’s Criterion” Let D be a UFD with quotient field F . If $f = \sum_{i=0}^n a_i x^i \in D[x]$, $\deg f \geq 1$ and p is an irreducible element of D such that $p \nmid a_n, p \mid a_i$ for $i = 0, 1, \dots, n - 1$, and $p^2 \nmid a_0$ then f is irreducible in $F[x]$. If f is primitive, then f is irreducible in $D[x]$.¹⁶²

2.5 Localizations

Sections: Hungerford III.4

DEF: A nonempty subset $S \subseteq R$, a ring, is *multiplicative* provided that $a, b \in S \Rightarrow ab \in S$.¹⁶³

THM: Let S be mult-closed of commie ring R . The relation \sim on $R \times S$ given by $(r, s) \sim (r', s') \Leftrightarrow s_1(rs' - r's) = 0$ for some $s_1 \in S$ is an equivalence relation.¹⁶⁴

THM: Let S be mult-closed of commie ring R and let $S^{-1}R$ be the equiv-classes of \sim above.¹⁶⁵

- (i) $S^{-1}R$ is a commie ring w/ identity.
- (ii) If R is a nonzero ring with no zero divisors and $0 \notin S$, then $S^{-1}R$ is an integral domain.
- (iii) If R is a nonzero ring with no zero divisors and S is the set of all nonzero elements of R , then $S^{-1}R$ is a field, called the *field of fractions* over R .

THM: Let S be mult-closed of commie ring R .¹⁶⁶

- (i) $\varphi_S : R \rightarrow S^{-1}R$ given by $r \mapsto rs/s$ is well-defined hom. of rings with $\varphi_S(s)$ is a unit in $S^{-1}R$ for all $s \in S$.
- (ii) If $0 \notin S$ and S contains no zero divisors, then φ_S is injective. In particular, any integral domain is embedded in its quotient field.
- (iii) If R has an identity and S consists of units, then φ_S is an isomorphism. In particular, the complete ring of quotients of a field is isomorphic to F .

THM: Let S be mult-closed of commie ring R and let T be any commie ring with identity. If $f : R \rightarrow T$ is a hom. of rings such that $f(s)$ is a unit in T for all $s \in S$, then there exists a unique homomorphism of rings $\bar{f} : S^{-1}R \rightarrow T$ such that $\bar{f} \circ \varphi_S = f$. The ring $S^{-1}R$ is completely determined by this property.¹⁶⁷

COR: Let R be an integral domain considered as a subring of its quotient field F . If E is a field and $f : R \rightarrow E$ an injection of rings, then there is a unique injection of field $\bar{f} : F \rightarrow E$ so that $\bar{f}|_R = f$. In particular any field E_1 containing R contains an isomorphic copy F_1 of F with $R \subseteq F_1 \subseteq E_1$.¹⁶⁸

THM: Let S be mult-closed of a commie ring R .¹⁶⁹ (i) If I is an ideal in R , then $S^{-1}I = \{a/s \mid a \in I, s \in S\}$ is an ideal in $S^{-1}R$, called the *extension* of I .

- (ii) If J is another ideal in R , then
- (a) $S^{-1}(I + J) = S^{-1}I + S^{-1}J$ (b) $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$ (c) $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$

THM: Let S be a mult-closed of commie ring R with identity and I an ideal of R . Then $S^{-1}I = S^{-1}R$ if and only if $S \cap I = \emptyset$.¹⁷⁰

LMA: Let S be mult-closed of a commie ring R with identity and let I be an ideal of R .¹⁷¹

- (i) $I \subseteq \varphi_S^{-1}(S^{-1}I)$
- (ii) If $I = \varphi_S^{-1}(J)$ for some ideal J in $S^{-1}R$, then $S^{-1}I = J$. In other words, every ideal in $S^{-1}R$ is of the form $S^{-1}I$ for some ideal I in R .
- (iii) If P is a prime ideal in R and $S \cap P = \emptyset$, then $S^{-1}P$ is a prime ideal in $S^{-1}R$ and $\phi_S^{-1}(S^{-1}P) = P$.

THM: Let S be mult-closed of a commie ring R with identity. Then there is a one-to-one correspondence between the prime ideals of R disjoint from S and the set of prime ideals of $S^{-1}R$ given by $P \mapsto S^{-1}P$.¹⁷²

DEF: Let R be a commie ring with identity and P a prime ideal of R . Then $S = R - P$ is mult-closed and define $R_P = S^{-1}R$ to be the *localization of R at P* .¹⁷³

DEF: A *local ring* is a commutative ring with identity which has a unique maximal ideal.¹⁷⁴

THM: Let P be a prime ideal in a commie ring R .¹⁷⁵ (i) There is a one-to-one correspondence between the set of prime ideals of R which are contained in P and the set of prime ideals of R_P , given by $Q \mapsto Q_P$.

- (ii) The ideal P_P in R_P is the unique maximal ideal of R_P . Hence, R_P is local.

THM: If R is a commutative ring with identity, then the following conditions are equivalent.

- (i) R is a local ring;
- (ii) all nonunits of R are contained in some ideal $M \neq R$;
- (iii) the nonunits of R form an ideal.¹⁷⁶

2.6 Dedekind Domains

DEF: A *Dedekind domain* is an integral domain R in which every ideal ($\neq R$) is the product of a finite number of prime ideals.¹⁷⁷

DEF: Let R be an integral domain with quotient field K . A *fractional ideal* of R is a nonzero R -submodule I of K such that $aI \subseteq R$ for some nonzero $a \in R$.¹⁷⁸

THM: If R is an integral domain with quotient field K , then the set of all fractional ideals of R forms a commutative monoid, with identity R and multiplication given by $IJ = \{\sum a_i b_i \mid a_i \in I, b_i \in JU, n \in \mathbb{N}\}$.¹⁷⁹

DEF: A fractional ideal I of an integral domain R is said to be *invertible* if $IJ = R$ for some fractional ideal J of R .¹⁸⁰

LMA: Let I, I_1, \dots, I_n be ideals in an integral domain R .¹⁸¹

- (i) The ideal $I_1 I_2 \cdots I_n$ is invertible if and only if every I_j is invertible.

(ii) If $P_1 \cdots P_m = I = Q_1 \cdots Q_n$ where each P_i, Q_j is prime in R and P_i is invertible, then $m = n$ and $P_i = Q_i$ with a suitable reordering.

THM: If R is a Dedekind domain, then every nonzero prime ideal of R is invertible and maximal.¹⁸²

LMA: If I is a fractional ideal of an integral domain R with quotient field K and $f \in \text{Hom}_R(I, R)$ then for all $a, b \in I$, $af(b) = bf(a)$.¹⁸³

LMA: Every invertible fractional ideal of an integral domain R with quotient field K is a finitely generated R -module.¹⁸⁴

THM: Let R be an integral domain and I a fractional ideal of R . Then I is invertible if and only if I is a projective R -module.¹⁸⁵

LMA: If R is a Noetherian, integrally closed integral domain and R has a unique nonzero prime ideal P , then R is a discrete valuation ring.¹⁸⁶

THM: The following conditions on an integral domain R are equivalent:¹⁸⁷ (i) R is a Dedekind domain.

(ii) Every proper ideal in R is uniquely a product of a finite number of prime ideals.

(iii) Every nonzero ideal in R is invertible.

(iv) Every fractional ideal of R is invertible.

(v) The set of all fractional ideals of R is a group under multiplication.

(vi) Every ideal in R is projective.

(vii) Every fractional ideal of R is projective.

(viii) R is Noetherian, integrally closed, and every nonzero prime ideal is maximal.

(ix) R is Noetherian and for every nonzero prime ideal P of R , the localization R_P of R at P is a discrete valuation ring.

Artin: Algebra by Michael Artin.

D&F: Abstract Algebra by Dummit & Foote.

H: Algebra by Thomas W. Hungerford.

Lang: Algebra by Serge Lang.

¹¹¹H Rmk p.128

¹¹²H Thm 2.22 pp.129-30

¹¹³H Thm 2.23 p.130

¹¹⁴H Thm 2.24 p.130

¹¹⁵H p.131

¹¹⁶H Thm 2.25 p.131

¹¹⁷H Cor 2.26 p.132

¹¹⁸H Cor 2.27 p.132

¹¹⁹H Exs 23,24 p.135

¹²⁰H Def 1.5 p.116

¹²¹H Eg p.127

¹²²H Thm 2.16 p.127

¹²³H Thm 2.20

¹²⁴H Cor 2.21 p.129

¹²⁵H Def 2.4 p.123

¹²⁶H Def 3.1 p.135

¹²⁷H Thm 3.2 p.136

¹²⁸H Def 3.3 p.136

¹²⁹H Thm 3.4 p.136

¹³⁰H Def 3.5 p.137

¹³¹H Lma 3.6 p.137

¹³²H Thm 3.7

¹³³H Def 3.8 p.139

¹³⁴H Eg p.139

¹³⁵H Thm 3.9 p.139

¹³⁶H Def 3.10 p.140

¹³⁷H Thm 3.11 p.140

¹³⁸H Thm 5.1 p.149

¹³⁹H Thm 5.3 p.151

¹⁴⁰H Thm 5.5 p.152

¹⁴¹H Cor 5.6 p.153

¹⁴²H Cor 5.7 p.153

¹⁴³H Prop 5.8 p.154

¹⁴⁴H Prop 5.9 p.155

¹⁴⁵H Cor 5.10 p.155

¹⁴⁶H pp.157-8

¹⁴⁷H Thm 6.1 p.158

¹⁴⁸H Thm 6.2 p.158

¹⁴⁹H Cor 6.3 p.159

¹⁵⁰H Cor 6.4 p.159

¹⁵¹H Def 6.5 p.160

Notes

⁷⁹H Def 1.1 p.115

⁸⁰H Thm 1.2 p.115

⁸¹H Def 1.3 p.116

⁸²H Def 1.4 p.116

⁸³H Thm 1.6 p.118

⁸⁴H Def 1.7 p.118

⁸⁵H pp.118-9

⁸⁶H Def 1.8 p.119

⁸⁷H Thm 1.9 p.119

⁸⁸H Thm 1.10 p.119

⁸⁹H Ex 12 p.121

⁹⁰H Def 2.1 p.122

⁹¹H Eg p.122

⁹²H Eg/Rmk p.123

⁹³H Thm 2.2 p.123

⁹⁴H Cor 2.3 p.123

⁹⁵H Def 2.4 p.123

⁹⁶H Thm 2.5 pp.123-4

⁹⁷H Thm 2.6 p.124

⁹⁸H Thm 2.7 p.125

⁹⁹H Thm 2.8 p.125

¹⁰⁰H Thm 2.9 p.125

¹⁰¹H Cor 2.10 p.126

¹⁰²H Cor 2.11 p.126

¹⁰³H Thm 2.12 p.126

¹⁰⁴H Thm 2.13 p.126

¹⁰⁵H Def 2.14 p.126

¹⁰⁶H Thm 2.15 p.127

¹⁰⁷H Def 2.17 p.127

¹⁰⁸Class 01/18

¹⁰⁹H Thm 2.18 p.128

¹¹⁰H Thm 2.19

¹⁵²H Thm 6.6 p.160
¹⁵³H Thm 6.7 p.160
¹⁵⁴H Prop 6.8 p.161
¹⁵⁵H Lma 6.9 p.161
¹⁵⁶H Thm 6.10 p.161
¹⁵⁷H p.162
¹⁵⁸H Lma 6.11 p.162
¹⁵⁹H Lma 6.12 p.163
¹⁶⁰H Lma 6.13 p. 163
¹⁶¹H Thm 6.14 p.164
¹⁶²H Thm 6.15 pp.164-5
¹⁶³H Def 4.1 p.142
¹⁶⁴H Thm 4.2 p.142
¹⁶⁵H Thm 4.3 p.143
¹⁶⁶H Thm 4.4 p.144
¹⁶⁷H Thm 4.5 p.144
¹⁶⁸H Cor 4.6 p.145
¹⁶⁹H Thm 4.7 p.145

¹⁷⁰H Thm 4.8 p.146
¹⁷¹H Lma 4.9 p.146
¹⁷²H Thm 4.10 p.146
¹⁷³H p.147
¹⁷⁴H Def 4.12 p.147
¹⁷⁵H Thm 4.11 p.147
¹⁷⁶H Thm 4.13 p.147
¹⁷⁷H p.401
¹⁷⁸H Def 6.2 p.401
¹⁷⁹H Thm 6.3 p.401
¹⁸⁰H p.401
¹⁸¹H Lma 6.4 p.402
¹⁸²H Thm 6.5 p.402
¹⁸³H Lma 6.6 p.403
¹⁸⁴H Lma 6.7 p.403
¹⁸⁵H Thm 6.8 p.404
¹⁸⁶H Lma 6.9 p.404
¹⁸⁷H Thm 6.10 pp.405-6

3 Modules

3.1 Definitions

DEF: Let R be a ring. A [left] R -module is an additive abelian group A together with a function $R \times A \rightarrow A$ (written as multiplication) such that for all $r, s \in R$ and $a, b \in A$:

$$(i) r(a + b) = ra + rb. \quad (ii) (r + s)a = ra + sa. \quad (iii) r(sa) = (rs)a.$$

If R has an identity element 1_R , and

$$(iv) 1_R a = a \text{ for all } a \in A,$$

then A is a *unitary R -module*. If R is a division ring, then a unitary R -module is called a [left] *vector space*.¹⁸⁸

EX: If R is a ring, every abelian group A can be made into an R -module with *trivial module structure* by defining $ra = 0$ for all $r \in R$ and $a \in A$. *H Eg p.170*

DEF: A non-zero unitary R -module A is *simple* if its only submodules are 0 and A .¹⁸⁹

DEF: Let A and B be modules over a ring R . A function $f : A \rightarrow B$ is an R -module *homomorphism* provided for all $a, c \in A$ and $r \in R$, $f(ra + c) = rf(a) + f(c)$. If R is a division ring, then an R -module homomorphism is called a *linear transformation*. Define similarly *monomorphism*, *epimorphism*, *isomorphism*, *image* and *kernel*.¹⁹⁰

DEF: Let R be a ring, A an R -module and B a nonempty subset of A . B is a *submodule* of A provided B is an additive subgroup of A and $rb \in B$ for all $r \in R$, $b \in B$. A submodule of a vector space is called a *subspace*.¹⁹¹

DEF: If X is a subset of a module A over a ring R , then the intersection of all submodules of A containing X is called the *submodule generated by X* (or *spanned by X*). If X is finite and X generates the module B , then B is said to be *finitely generated*. If X consists of a single element $X = \{a\}$, then the submodule generated by X is called the *cyclic (sub)module* generated by a . If $\{B_i \mid i \in I\}$ is a family of submodules of A , then the submodule generated by $X = \cup_{i \in I} B_i$ is called the *sum* of the modules B_i . If I is finite, label this as $B_1 + B_2 + \dots + B_n$.¹⁹²

THM: Let R be a ring, A an R -mod, $X \subseteq A$, $\{B_i \mid i \in I\}$ a family of submodules of A and $a \in A$. Let $Ra = \{ra \mid r \in R\}$.

(i) Ra is a submodule of A and the map $R \rightarrow Ra$ given by $r \mapsto ra$ is an R -mod epimorphism.

(ii) The cyclic submodule C generated by a is $\{ra + na \mid r \in R, n \in \mathbb{Z}\}$. If R has an identity and C is unitary, then $C = Ra$.

(iii) The submodule D generated by X is $\left\{ \sum_{i=1}^s r_i a_i + \sum_{j=1}^t n_j b_j \mid s, t \in \mathbb{N}, a_i, b_j \in X, r_i \in R, n_i \in \mathbb{Z} \right\}$.

If R has an identity and A is unitary, then $D = RX = \left\{ \sum_{i=1}^s r_i a_i \mid s \in \mathbb{N}, a_i \in X, r_i \in R \right\}$.

(iv) The sum of the family $\{B_i \mid i \in I\}$ consists of all finite sums $b_{i_1} + \dots + b_{i_n}$ with $b_{i_k} \in B_{i_k}$.¹⁹³

THM: Let B be a submodule of a module A over a ring R . Then the quotient group A/B is an R -module with the action of R on A/B given by $r(a + B) = ra + B$ for all $r \in R, a \in A$. The map $\pi : A \rightarrow A/B$ given by $a \mapsto a + B$ is an R -mod epimorphism with kernel B , called the *canonical epimorphism* or *projection*.¹⁹⁴

THM: "First Isomorphism Theorem of Modules" If R is a ring and $f : A \rightarrow B$ is an R -module homomorphism and C is a submodule of $\ker f$, then there is a unique R -mod homomorphism $\bar{f} : A/C \rightarrow B$ such that $\bar{f}(a + C) = f(a)$ for all $a \in A$, $\text{im } \bar{f} = \text{im } f$, and $\ker \bar{f} = (\ker f)/C$. \bar{f} is an R -mod isomorphism if and only if f is an R -module epimorphism and $C = \ker f$. In particular, $A/\ker f \cong \text{im } f$.¹⁹⁵

COR: If R is a ring and A' is a submodule of the R -module A and B' a submodule of the R -module B and $f : A \rightarrow B$ is an R -module homomorphism such that $f(A') \subseteq B'$, then f induces an R -module homomorphism $\bar{f} : A/A' \rightarrow B/B'$ given by $a + A' \mapsto f(a) + B'$. \bar{f} is an R -module isomorphism if and only if $\text{im } f + B' = B$ and $f^{-1}(B') \subseteq A'$. In particular if f is an epimorphism such that $f(A') = B'$ and $\ker f \subseteq A'$, then \bar{f} is an R -module isomorphism.¹⁹⁶

THM: Let B and C be submodules of a module A over a ring R .

(i) "Second Isomorphism Theorem of Modules" There is an R -module isomorphism $B/(B \cap C) \cong (B + C)/C$;

(ii) "Third Isomorphism Theorem of Modules" if $C \subseteq B$, then B/C is a submodule of A/C , and there is an R -module isomorphism $(A/C)/(B/C) \cong A/B$.¹⁹⁷

THM: If R is a ring and B a submodule of an R -mod A , then there is a one-to-one correspondence between the set of all submodules of A containing B and the set of all submodules of A/B given by $C \mapsto C/B$. Hence every submodule of A/B is of the form C/B , where C is a submodule of A which contains B .¹⁹⁸

THM: Let R be a ring and $\{A_i \mid i \in I\}$ a nonempty family of R -modules, $\prod_{i \in I} A_i$ the *direct product* of the abelian groups A_i , and $\sum_{i \in I} A_i$ the *direct sum* of the abelian groups A_i . If I is finite, then $\prod A_i = \sum A_i = A_1 \oplus \dots \oplus A_n$.

(i) $\prod_{i \in I} A_i$ is an R -module with the action of R given by $r\{a_i\} = \{ra_i\}$.

(ii) $\sum_{i \in I} A_i$ is a submodule of $\prod_{i \in I} A_i$.

(iii) For each $k \in I$, the *canonical projection* $\pi_k : \prod A_i \rightarrow A_k$ is an R -module epimorphism.

(iv) For each $k \in I$, the *canonical injection* $\iota_k : A_k \rightarrow \sum A_i$ is an R -module monomorphism.¹⁹⁹

THM: If R is a ring, $\{A_i \mid i \in I\}$ a family of R -modules, C an R -mod, and $\{\varphi_i : C \rightarrow A_i \mid i \in I\}$ a family of R -module homomorphisms, then there is a unique R -mod homomorphism $\varphi : C \rightarrow \prod A_i$ such that $\pi_i \varphi = \varphi_i$ for all $i \in I$. $\prod A_i$ is uniquely determined up to isomorphism by this property, so $\prod A_i$ is a product in the category of R -modules.²⁰⁰

THM: If R is a ring, $\{A_i \mid i \in I\}$ a family of R -modules, D an R -module, and $\{\psi_i : A_i \rightarrow D \mid i \in I\}$ a family of R -module homomorphisms, then there is a unique R -module homomorphism $\psi : \sum A_i \rightarrow D$ such that $\psi \iota_i = \psi_i$ for all $i \in I$. $\sum A_i$ is uniquely determined up to isomorphism by this property, so $\sum A_i$ is a coproduct in the category of R -modules.²⁰¹

THM: Let R be a ring and A, A_1, \dots, A_n R -modules. Then $A \cong A_1 \oplus \dots \oplus A_n$ if and only if for each $i = 1, 2, \dots, n$ there are R -module homomorphisms $\pi_i : A \rightarrow A_i$ and $\iota_i : A_i \rightarrow A$ such that

- (i) $\pi_i \iota_i = \text{id}_{A_i}$ for all i ;
- (ii) $\pi_j \iota_i = 0$ for $i \neq j$;
- (iii) $\iota_1 \pi_1 + \dots + \iota_n \pi_n = 1_A$.²⁰²

THM: Let R be a ring and $\{A_i \mid i \in I\}$ a family of submodules of an R -mod A such that

- (i) A is the sum of the family $\{A_i \mid i \in I\}$;
- (ii) for each $k \in I$, $A_k \cap A_k^* = 0$, where A_k^* is the sum of the family $\{A_i \mid i \neq k\}$.

Then there is an isomorphism $A \cong \sum A_i$ and A is called the (*internal*) *direct sum* of $\{A_i \mid i \in I\}$.²⁰³

DEF: A pair of module homomorphisms, $A \xrightarrow{f} B \xrightarrow{g} C$ is *exact* at B if $\text{im } f = \ker g$. A finite sequence of module homomorphisms, $A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} \dots \xrightarrow{f_n} A_n$ is *exact* provided $\text{im } f_i = \ker f_{i+1}$ for $i = 1, \dots, n-1$. An infinite sequence of module homomorphisms is *exact* provided $\text{im } f_i = \ker f_{i+1}$ for all $i \in \mathbb{Z}$. A finite exact sequence starting and ending with the trivial module is a *short exact sequence*.²⁰⁴

3.2 Free and Projective Modules

DEF: A subset X of an R -mod A is *linearly independent* provided that for distinct $x_1, \dots, x_n \in X$ and $r_i \in R$, $\sum_{i=1}^n r_i x_i = 0$ implies $r_i = 0$ for all i . A set that is not linearly independent is *linearly dependent*. If A is generated by linear combinations of the elements of X , then X *spans* A . A linearly independent subset of A that spans A is a *basis* of A . An R -mod F that has a nonempty basis is called a *free R -module*.²⁰⁵

THM: Let R be a ring with identity. The following conditions on a unitary R -module F are equivalent:

- (i) F has a nonempty basis;
- (ii) F is the internal direct sum of a family of cyclic R -modules, each of which is isomorphic as a left R -module to R ;
- (iii) F is R -module isomorphic to a direct sum of copies of the left R -module R ;
- (iv) there exists a nonempty set X and a function $\iota : X \rightarrow F$ with the following property: given any unitary R -module A and function $f : X \rightarrow A$, there exists a unique R -module homomorphism $\bar{f} : F \rightarrow A$ such that $\bar{f} \iota = f$. In other words, F is a free object in the category of unitary R -modules.²⁰⁶

COR: Every [unitary] module A over a ring R [with identity] is the homomorphic image of a free R -module F . If A is finitely generated, then F may be chosen to be finitely generated.²⁰⁷

LMA: A maximal linearly independent subset X of a vector space V over a division ring D is a basis of V .²⁰⁸

THM: Every vector space V over a division ring D has a basis and is therefore a free D -module. More generally every linearly independent subset of V is contained in a basis of V .²⁰⁹

THM: If V is a vector space over a division ring D and X is a subset that spans V , then X contains a basis of V .²¹⁰

THM: Let R be a ring with identity and F a free R -module with an infinite basis X . Then every basis of F has the same cardinality as X .²¹¹

THM: If V is a vector space over a division ring D , then any two bases of V have the same cardinality.²¹²

DEF: Let R be a ring with identity such that for every free R -module F , any two bases of F have the same cardinality.

Then R is said to have the *invariant dimension property* and the cardinal number of any basis of F is called the *dimension* (or *rank*) of F over R .²¹³ A vector space V over a division ring D is *finite dimensional* if $\dim_D V$ is finite.²¹⁴

PROP: Let E and F be free modules over a ring R that has the invariant dimension property. Then $E \cong F$ if and only if E and F have the same rank.²¹⁵

LMA: Let R be a ring with identity, $I (\neq R)$ an ideal of R , F a free R -module with basis X and $\pi : F \rightarrow F/IF$ the canonical epimorphism. Then F/IF is a free R/I -module with basis $\pi(X)$ and $|\pi(X)| = |X|$.²¹⁶

PROP: Let $f : R \rightarrow S$ be a nonzero epimorphism of rings with identity. If S has the invariant dimension property, then so does R .²¹⁷

COR: If R is a ring with identity that has a homomorphic image which is a division ring, then R has the invariant dimension property. In particular, every commutative ring with identity has the invariant dimension property.²¹⁸

THM: Let W be a subspace of a vector space V over a division ring D .

- (i) $\dim_D W \leq \dim_D V$;
- (ii) if $\dim_D W = \dim_D V$ and $\dim_D V$ is finite, then $W = V$;
- (iii) $\dim_D V = \dim_D W + \dim_D(V/W)$.²¹⁹

COR: If $f : V \rightarrow V'$ is a linear transformation of vector spaces over a division ring D , then there exists a basis X of V such that $X \cap \ker f$ is a basis of $\ker f$ and $\{f(x) \mid f(x) \neq 0, x \in X\}$ is a basis of $\text{im } f$. In particular, $\dim_D V = \dim_D(\ker f) + \dim_D(\text{Im } f)$.²²⁰

COR: If V and W are finite dimensional subspaces of a vector space over a division ring D , then $\dim_D V + \dim_D W = \dim_D(V \cap W) + \dim_D(V + W)$.^{221s}

THM: Let R, S, T be division rings such that $R \subseteq S \subseteq T$. Then $\dim_R T = (\dim_S T)(\dim_R S)$. Furthermore, $\dim_R T$ is finite if and only if $\dim_S T$ and $\dim_R S$ are finite.²²²

DEF: A module P over a ring R is *projective* if given any R -hom $f : P \rightarrow B$ and exact sequence $A \xrightarrow{g} B \rightarrow 0$, there exists a map $h : P \rightarrow A$ so that $g \circ h = f$.²²³

THM: Every free module F over a ring R with identity is projective.²²⁴

COR: Every module A over a ring R is the homomorphis image of a projective R -module.²²⁵

THM: Let R be a ring. The following conditions on an R -mod P are equivalent:²²⁶ (i) P is projective.

- (ii) Every short exact sequence $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} P \rightarrow 0$ is split exact, hence $B \cong A \oplus P$.
- (iii) there is a free module F and an R -mod K so that $F \cong K \oplus P$.

PROP: Let R be a ring. A direct sum of R -mods $\sum P_i$ is projective if and only if each P_i is projective.²²⁷

3.3 Modules over PIDs

3.4 Exact Sequences and Homs

THM: Let A, B, C, D be module over a ring R and $\varphi : C \rightarrow A$, $\psi : B \rightarrow D$ are R -homs. Then the map $\theta : \text{Hom}_R(A, B) \rightarrow \text{Hom}_R(C, D)$ given by $f \mapsto \psi f \varphi$ is a homomorphism of abelian groups.²²⁸

THM: Let R be a ring. $0 \rightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ is an exact sequence of R -modules if and only if for every R -module D , $0 \rightarrow \text{Hom}_R(D, A) \xrightarrow{\bar{\varphi}} \text{Hom}_R(D, B) \xrightarrow{\bar{\psi}} \text{Hom}_R(D, C)$ is an exact sequence of abelian groups.²²⁹

PROP: Let R be a ring. $A \xrightarrow{\varphi} B \xrightarrow{\psi} C \rightarrow 0$ is an exact sequence of R -modules if and only if for every R -module D , $0 \rightarrow \text{Hom}_R(C, D) \xrightarrow{\bar{\psi}} \text{Hom}_R(B, D) \xrightarrow{\bar{\varphi}} \text{Hom}_R(A, D)$ is an exact sequence of abelian groups.²³⁰

DEF: The theorems above show that $\text{Hom}_R(A, B)$ is *left exact*.²³¹

PROP: The following conditions on modules over a ring R are equivalent:²³²

- (i) $0 \rightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \rightarrow 0$ is a split exact sequence of R -modules.
- (ii) $0 \rightarrow \text{Hom}_R(D, A) \xrightarrow{\bar{\varphi}} \text{Hom}_R(D, B) \xrightarrow{\bar{\psi}} \text{Hom}_R(D, C)$ is an exact sequence of abelian groups for every R -mod D .
- (iii) $0 \rightarrow \text{Hom}_R(C, D) \xrightarrow{\bar{\psi}} \text{Hom}_R(B, D) \xrightarrow{\bar{\varphi}} \text{Hom}_R(A, D)$ is an exact sequence of abelian groups for every R -mod D .

THM: The following conditions on a module P over a ring R are equivalent.²³³

- (i) P is projective.
- (ii) If $\psi : B \rightarrow C$ is any injective R -hom then $\bar{\psi} : \text{Hom}_R(P, B) \rightarrow \text{Hom}_R(P, C)$ is an injective homomorphism of abelian groups.
- (iii) If $0 \rightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \rightarrow 0$ is any short exact sequence of R -mods, then $0 \rightarrow \text{Hom}_R(P, A) \xrightarrow{\bar{\varphi}} \text{Hom}_R(P, B) \xrightarrow{\bar{\psi}} \text{Hom}_R(P, C) \rightarrow 0$ is an exact sequence of abelian groups.

THM: Let $A, B, \{A_i \mid i \in I\}, \{B_j \mid j \in J\}$ be R -mods. Then there are isomorphism of abelian groups: (i) $\text{Hom}_R\left(\sum_{i \in I} A_i, B\right) \cong$

$$\prod_{i \in I} \text{Hom}_R(A_i, B)$$

$$(ii) \text{Hom}_R\left(A, \prod_{j \in J} B_j\right) \cong \prod_{j \in J} \text{Hom}_R(A, B_j).^{234}$$

DEF: An abelian group A is an $R - S$ *bimodule* provided that A is both a left R -module and a right S -module and $r(as) = (ra)s$ for all $r \in R, s \in S$.²³⁵

THM: Let R and S be rings and ${}_R A, {}_R B, {}_R C, {}_R D$ be (bi)modules as indicated.²³⁶

- (i) $\text{Hom}_R(A, B)$ is a right S -module, with the action of S given by $(fs)(a) = (f(a))s, f \in \text{Hom}_R(A, B), s \in S, a \in A$.
- (ii) If $\varphi : A \rightarrow A'$ is a left R -hom, then the induced map $\bar{\varphi} : \text{Hom}_R(A', B) \rightarrow \text{Hom}_R(A, B)$ is a right S -hom.
- (iii) $\text{Hom}_R(C, D)$ is a left S -mod with the action of S given by $(sg)(c) = g(cs)$ for $g \in \text{Hom}_R(C, D), s \in S, c \in C$.

THM: If A is a unitary left R -mod, then there is an isomorphism of left R -modules $A \cong \text{Hom}_R(R, A)$.²³⁷

DEF: Given A a left R -module, consider R as a right R -mod and define $A^* = \text{Hom}_R(A, R)$, the *dual* module of A . The elements of A^* are sometimes called *linear functionals*.²³⁸

THM: Let A, B and C be left R -mods.²³⁹ (i) If $\varphi : A \rightarrow C$ is a R -hom, then the induced map $\bar{\varphi} : C^* = \text{Hom}_R(C, R) \rightarrow \text{Hom}_R(A, R) = A^*$ is a right R -hom.

- (ii) There is an R -mod isomorphism $(A \oplus C)^* \cong A^* \oplus C^*$.
- (iii) If R is a division ring, and $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ is a short exact sequence of left vector spaces, then $0 \rightarrow C^* \rightarrow B^* \rightarrow A^* \rightarrow 0$ is a short exact sequence of right vector spaces.

DEF: The *Kronecker delta notation* is the symbol $\delta_{ij} = \begin{cases} 0_R & i \neq j \\ 1_R & i = j \end{cases}$.²⁴⁰

THM: Let F be a free left R -0mod. Let X be a basis of F and for each $x \in X$ let $f_x : F \rightarrow R$ be defined by the operation on the basis $f_x(y) = \delta_{xy}$. Then,

- (i) $\{f_x \mid x \in X\}$ is a linearly independent subset of F^* of cardinality $|X|$;
- (ii) if X is finite, then F^* is a free right R -module with basis $\{f_x \mid x \in X\}$, called the *dual basis*.²⁴¹

3.5 Tensor Products

DEF: A *middle linear map* from $A_R \times_R B$ to C is a function $f : A \times B \rightarrow C$ such that for all $a, a_i \in A, b, b_i \in B$, and $r \in R$,

- (i) $f(a_1 + a_2, b) = f(a_1, b) + f(a_2, b)$
- (ii) $f(a, b_1 + b_2) = f(a, b_1) + f(a, b_2)$
- (iii) $f(ar, b) = f(a, rb)$.²⁴²

DEF: Let A be a right R -mod and B a left R -mod. Let F be the free abelian group on the set $A \times B$. Let K be the subgroup of F generated by all elements of the forms:

- (i) $(a + a', b) - (a, b) - (a', b)$
- (ii) $(a, b + b') - (a, b) - (a, b')$
- (iii) $(ar, b) - (a, rb)$.

The quotient group F/K is called the *tensor product* of A and B , denoted $A \otimes_R B$. The coset $(a, b) + K$ is denoted $a \otimes b$.²⁴³

THM: Let A_R and ${}_R B$ be R -mods and let C be an abelian group. If $g : A \times B \rightarrow C$ is a middle linear map, then there exists a unique group hom $\bar{g} : A \otimes_R B \rightarrow C$ so that $\bar{g}\iota = g$ where $\iota : A \times B \rightarrow A \otimes_R B$ is the canonical middle linear map. $A \otimes_R B$ is uniquely determined up to isomorphism by this property. Therefore, $\iota : A \times B \rightarrow A \otimes_R B$ is universal in the category of all middle linear maps on $A \times B$.²⁴⁴

COR: If $A_R, A'_R, {}_R B$ and ${}_R B'$ are R -mods and $f : A \rightarrow A'$ and $g : B \rightarrow B'$ are R -homs, then there is a unique group hom $A \otimes_R B \rightarrow A' \otimes_R B'$ such that $a \otimes b \mapsto f(a) \otimes g(b)$ for all $a \in A, b \in B$.²⁴⁵

PROP: If $A \rightarrow B \rightarrow C \rightarrow 0$ is an exact sequence of left R -mods and D is a right R -mod, then $D \otimes_R A \rightarrow D \otimes_R B \rightarrow D \otimes_R C \rightarrow 0$ is an exact sequence of abelian groups. An analogous statement holds for exactness in the first position.²⁴⁶

THM: Let R and S be rings and ${}_S A, {}_R, {}_R B, {}_R C, {}_R, {}_R D, {}_S$ (bi)mods as indicated.²⁴⁷

- (i) $A \otimes_R B$ is a left S -mod so that $s(a \otimes b) = sa \otimes b$ for all $s \in S, a \in A$.
- (ii) If $f : A \rightarrow A'$ is an $S - R$ -hom and $g : B \rightarrow B'$ is an R -hom, then the induced map $f \otimes g : A \otimes_R B \rightarrow A' \otimes_R B'$ is a left S -hom.
- (iii) If $h : C \rightarrow C'$ is an R -hom and $k : D \rightarrow D'$ is an $R - S$ -hom, then the induced map $h \otimes k : C \otimes_R D \rightarrow C' \otimes_R D'$ is a right S -hom.

THM: If A, B, C are modules over a commutative ring R and $g : A \times B \rightarrow C$ is a bilinear map, then there is a unique R -hom $\bar{g} : A \otimes_R B \rightarrow C$ so that $\bar{g}\iota = g$. $A \otimes_R B$ is uniquely determined up to isomorphism by this property.²⁴⁸

THM: If R is a ring with identity and A, B are unitary R -mods, then there are R -mod isomorphisms $A \otimes_R R \cong A$ and $R \otimes_R B \cong B$.²⁴⁹

THM: If R and S are rings and A, B, C are (bi)modules, then there is an isomorphism $(A \otimes_R B) \otimes_S C \cong A \otimes_R (B \otimes_S C)$. The isomorphism is unique given the restriction $(a \otimes b) \otimes c \mapsto a \otimes (b \otimes c)$.²⁵⁰

PROP: Let E, F be modules of a commie ring R . Then there is a unique isomorphism $E \otimes_R F \rightarrow F \otimes_R E$ so that $e \otimes f \mapsto f \otimes e$.²⁵¹

THM: Let R be a ring, A and $\{A_i \mid i \in I\}$ right R -mods, B and $\{B_j \mid j \in J\}$ left R -modes. Then there are group isomorphisms

(i) $(\sum A_i) \otimes_R B \cong \sum (A_i \otimes_R B)$;

(ii) $A \otimes_R (\sum B_j) \cong \sum (A \otimes_R B_j)$.²⁵²

THM: “Adjoint Associativity” Let R and S be rings and $A_{R,R}, B_S, C_S$ (bi)modules. Then there is an isomorphism of abelian groups $\alpha : \text{Hom}_S(A \otimes_R B, C) \cong \text{Hom}_R(A, \text{Hom}_S(B, C))$, defined for each $f : A \otimes_R B \rightarrow C$ by $[(\alpha f)(a)](b) = f(a \otimes b)$.²⁵³

THM: Let R be a ring with identity. If A is a unitary right R -mod and V is a free left R -mod with basis Y , then every element u of $A \otimes_R V$ may be written uniquely in the form $u = \sum_{i=1}^n a_i \otimes y_i$ where $a_i \in A$ and y_i are distinct elements of Y .²⁵⁴

COR: If R is a ring with identity and A_R and ${}_R B$ are free R -modules with bases X and Y , then $A \otimes_R B$ is a free (right) R -mod with basis $W = \{x \otimes y \mid x \in X, y \in Y\}$ of cardinality $|X| \cdot |Y|$.²⁵⁵

COR: Let S be a ring with identity and R a subring of S that contains 1_S . If F is a free left R -mod with basis X , then $S \otimes_R F$ is a free left S -module with basis $\{1_S \otimes x \mid x \in X\}$.²⁵⁶

PROP: Let E, F be free commie R -mods of finite dimension. Then we have an isomorphism $\text{End}_R(E) \otimes \text{End}_R(F) \rightarrow \text{End}_R(E \otimes F)$ which is the unique maps such that $f \otimes g \mapsto T(f, g)$ for $f \in \text{End}_R(E), g \in \text{End}_R(F)$.²⁵⁷

DEF: Let E, F, G be modules of a commie ring R . Then $L(E, F)$ is the set of linear maps $E \rightarrow F$. The set $L^2(E, F; G)$ is the set of bilinear maps $E \times F \rightarrow G$.²⁵⁸

PROP: For a commie ring R and three R -mods E, F , and G , $L(E, L(F, G)) \cong L^2(E, F; G) \cong L(E \otimes F, G)$.²⁵⁹

PROP: Let $0 \rightarrow E' \rightarrow E \rightarrow E'' \rightarrow 0$ be an exact sequence, and F any module. Then the sequence $F \otimes E' \rightarrow F \otimes E \rightarrow F \otimes E'' \rightarrow 0$ is exact. Therefore, the tensor product is *right exact*.²⁶⁰

PROP: Let I be an ideal of a commie ring R . Let E be an R -mod. Then the map $(R/I) \times E \rightarrow E/IE$ induced by $(a, x) \mapsto ax \pmod{IE}, a \in R, x \in E$ is bilinear and induces an isomorphism $(R/I) \otimes_R E \cong E/IE$.²⁶¹

3.5.1 Flat Modules

Artin: Algebra by Michael Artin.

D&F: Abstract Algebra by Dummit & Foote.

H: Algebra by Thomas W. Hungerford.

Lang: Algebra by Serge Lang.

²¹³H Def 2.8 p.185

²¹⁴H p.186

²¹⁵H Prop 2.9 p.185

²¹⁶H Lma 2.10 p.185

²¹⁷H Prop 2.11 p.186

²¹⁸H Cor 2.12 p.186

²¹⁹H Thm 2.13 p.187

²²⁰H Cor 2.14 p.187

²²¹H Cor 2.15 p.187

²²²H Thm 2.16 p.188

²²³H Def 3.1 pp.190-1

²²⁴H Thm 3.2 p.191

²²⁵H Cor 3.3 p.192

²²⁶H Thm 3.4 p.192

²²⁷H Prop 3.5 p.193

²²⁸H Thm 4.1 p.199

²²⁹H Thm 4.2 p.200

²³⁰H Prop 4.3 p.200

²³¹H p.201

²³²H Prop 4.4 p.201

²³³H Thm 4.5 p.201

²³⁴H Thm 4.7 p.202

²³⁵H p.202

²³⁶H Thm 4.8 p.203

²³⁷H Thm 4.9 p.203

²³⁸H p.203

²³⁹H Thm 4.10 p.204

²⁴⁰H p.204

²⁴¹H Thm 4.11 p.204

²⁴²H p.207

²⁴³H Def 5.1 p.208; L p.602

²⁴⁴H Thm 5.2 p.209

²⁴⁵H Cor 5.3 p.209

²⁴⁶H Prop 5.4 pp.209-210

Notes

- ¹⁸⁸H Def 1.1 p.169
- ¹⁸⁹H Ex 5 p.179
- ¹⁹⁰H Def 1.2 p.170
- ¹⁹¹H Def 1.3 p.171
- ¹⁹²H Def 1.4 p.171
- ¹⁹³H Thm 1.5 pp.171-2
- ¹⁹⁴H Thm 1.6 p.172
- ¹⁹⁵H Thm 1.7 p.172
- ¹⁹⁶H Cor 1.8 p.172
- ¹⁹⁷H Thm 1.9 p.173
- ¹⁹⁸H Thm 1.10 p.173
- ¹⁹⁹H Thm 1.11 p.173
- ²⁰⁰H Thm 1.12 p.173
- ²⁰¹H Thm 1.13 p.174
- ²⁰²H Thm 1.14 p.174
- ²⁰³H Thm 1.15 p.175
- ²⁰⁴H Def 1.16 pp.175-6
- ²⁰⁵H p.181
- ²⁰⁶H Thm 2.1 p.181
- ²⁰⁷H Cor 2.2 p.182
- ²⁰⁸H Lma 2.3 p.183
- ²⁰⁹H THm 2.4 p.183
- ²¹⁰H Thm 2.5 p.183
- ²¹¹H Thm 2.6 p.184
- ²¹²H Thm 2.7 p.185

²⁴⁷H Thm 5.5 p.210

²⁴⁸H Thm 5.6 p.211

²⁴⁹H Thm 5.7 p.212

²⁵⁰H Thm 5.8 p.212; L Prop 1.1 p.604

²⁵¹L Prop 1.2 p.605

²⁵²H Thm 5.9 p.213; L Prop 2.1, Cor 2.2 p.608

²⁵³H Thm 5.10 p.214

²⁵⁴H Thm 5.11; L Prop 2.3 p.609

²⁵⁵H Cor 5.12 p.215; L Cor 2.4 p.609

²⁵⁶H Cor 5.12

²⁵⁷L Prop 2.5 p.610

²⁵⁸L p.607

²⁵⁹L p.607

²⁶⁰L Prop 2.6 p.611

²⁶¹L Prop 2.7 p.612

4 Field Theory

4.1 Basic Extensions

DEF: A field F is said to be an *extension field* of k provided that k is a subfield of F .²⁶²

DEF: A field extension $k \subseteq F$ operates as a vector space. The dimension of this vector space is written as $[F : k] = \dim_k F$ and called the *degree* of the field extension.²⁶³

DEF: Let F/k be a field extension. An element $u \in F$ is *algebraic* over k if u is a root of some polynomial in $k[x]$. Otherwise, u is *transcendental* over k . F is called an *algebraic extension* if every element of F is algebraic over k . Otherwise, F is called a *transcendental extension* if at least one element of F is transcendental over k .²⁶⁴

PROP: Let F be a finite extension over k , then F/k is algebraic.²⁶⁵

DEF: A field E is called an *intermediate field* of F/k if $k \subseteq E \subseteq F$ are field extensions.²⁶⁶

THM: Let F be an extension field of E and E an extension field of k . Then $[F : k] = [F : E][E : k]$. Furthermore, $[F : k]$ is finite if and only if $[F : E]$ and $[E : k]$ are finite.²⁶⁷ Also, if $\{x_i\}_{i \in I}$ is a basis for E over k and $\{y_j\}_{j \in J}$ is a basis for F over E , then $\{x_i y_j\}_{(i,j) \in I \times J}$ is a basis for F over k .²⁶⁸

DEF: A *tower* of fields is a sequence $k \subseteq F_1 \subseteq F_2 \subseteq \dots \subseteq F_n$. A tower is *finite* if every step of the sequence is finite.²⁶⁹

DEF: The field $k(u_1, \dots, u_n)$ is called a *finitely generated* extension of k . An extension $k(u)$ is called *simple*.²⁷⁰

PROP: Let F be a finite extension over k . Then F is finitely generated.²⁷¹

THM: If F/k a field extension, $u, u_i \in F$ and $X \subseteq F$, then

- (i) the subring $k[u]$ consists of all elements of the form $f(u)$ where $f \in k[x]$.
- (ii) the subring $k[u_1, \dots, u_m]$ consists of all elements of the form $g(u_1, \dots, u_m)$ where $g \in k[x_1, \dots, x_m]$.
- (iii) The subring $k[X]$ consists of all elements of the form $h(u_1, \dots, u_m)$ where $h \in k[x_1, \dots, x_m]$ and each $u_i \in X$, for some m .
- (iv) The subfield $k(u)$ consists of all elements of the form $f(u)/g(u) = f(u)g(u)^{-1}$ where $f, g \in k[x]$ and $g(u) \neq 0$.
- (v) The subfield $k(u_1, \dots, u_m)$ consists of all elements of the form $f(u_1, \dots, u_m)/g(u_1, \dots, u_m)$ where $f, g \in k[x_1, \dots, x_m]$ and $g(u_1, \dots, u_m) \neq 0$.
- (vi) The subfield $k(X)$ consists of all elements of the form $f(u_1, \dots, u_m)/g(u_1, \dots, u_m)$ where $u_i \in X$ for some m , $f, g \in k[x_1, \dots, x_m]$ and $g(u_1, \dots, u_m) \neq 0$.²⁷²

DEF: If L and M are subfields of a field F , the *compositum* (or sometimes *composite*) of L and M in F , denoted LM is the subfield generated by the set $L \cup M$.²⁷³ Given two extensions E and F of a base field k , the extension EF over F as the *translation* or *lifting* of E to F .²⁷⁴

DEF: $K(x_1, \dots, x_n)$ is called the *field of rational functions* in x_1, \dots, x_n over k .²⁷⁵

THM: If F/k a field extension, and $u \in F$ transcendental over k , then there is an isomorphism of fields $k(u) \cong k(x)$ which is the identity on k .²⁷⁶

THM: If F/k a field extension, $u, u_i \in F$ algebraic over k , then

- (i) $k(u) = k[u]$.
- (ii) $k(u) \cong k[x]/\langle f \rangle$, where $f \in k[x]$ is an irreducible monic polynomial of degree $n \geq 1$ uniquely determined by the conditions that $f(u) = 0$ and $g(u) = 0 (g \in k[x])$ if and only if f divides g .²⁷⁷
- (iii) $[k(u) : k] = \deg f = n$.²⁷⁸
- (iv) $\{1_k, u, u^2, \dots, u^{n-1}\}$ is a basis for $k(u)$ over k .²⁷⁹ (v) $k(u_1, \dots, u_n) = k[u_1, \dots, u_n]$.
- (vi) $k[u_1, \dots, u_n]/k$ algebraic.²⁸⁰

DEF: Let F/k a field extension and $u \in F$ algebraic over k . The monic irreducible polynomial such that $f(u) = 0$ is called the *irreducible polynomial* of u , written $f = \text{IrrPoly}_k(u)$. The *degree of u over k* is $\deg f = [k(u) : k]$.²⁸¹

THM: Let $\sigma : k \rightarrow L$ be an isomorphism of fields, u an element of some extension field of k and v an element of some extension field of L . Assume either

- (i) u is transcendental over k and v is transcendental over L ; or
 - (ii) u is a root of an irreducible polynomial $f \in k[x]$ and v is a root of $\sigma(f) \in L[x]$.
- Then σ extends to an isomorphism of fields $k(u) \cong L(v)$ which maps u onto v .²⁸²

COR: Let E and F each be extensions of k and let $u \in E$ and $v \in F$ be algebraic over k . Then u and v are roots of the same irreducible polynomial $f \in k[x]$ if and only if there is an isomorphism of fields $k[u] \cong k[v]$ which sends u onto v and is the identity of k .²⁸³

THM: If k is a field and $f \in k[x]$ a polynomial of degree n , then there exists a simple extension field $F = k[u]$ of k such that:

- (i) $u \in F$ is a root of f .

(ii) $[k[u] : k] \leq n$ with equality holding if and only if f is irreducible in $k[x]$.

(iii) If f is irreducible in $k[x]$, then $k[u]$ is unique up to an isomorphism which is the identity on k .²⁸⁴

THM: If F is a finite dimensional extension field of k , then F is finitely generated and algebraic over k .²⁸⁵

THM: If F/k a field extension and X is a subset of F such that $F = k(X)$ and every element of X is algebraic over k , then F is an algebraic extension of k . If X is a finite set, then F is finite dimensional over k .²⁸⁶

THM: If $k \subseteq E \subseteq F$ with E/k algebraic and F/E algebraic, then F/k is algebraic.²⁸⁷

THM: Let F/k be a field extension and E the set of all elements of F algebraic over k . Then E is a subfield of F , algebraic over k .²⁸⁸

4.1.1 Distinguished Classes of Field Extensions

DEF: Let \mathcal{C} be a certain class of extension field $F \subseteq E$. \mathcal{C} is *distinguished* if it satisfies the following conditions:

(i) Let $k \subseteq F \subseteq E$ a tower of fields. The extension $k \subseteq E$ is in \mathcal{C} if and only if $k \subseteq F$ and $F \subseteq E$ are in \mathcal{C} .

(ii) If $k \subseteq E$ is in \mathcal{C} and F any extension of k , and E, F are both contained in some field, then $F \subseteq EF$ is in \mathcal{C} .

(iii) If $k \subseteq F$ and $k \subseteq E$ are in \mathcal{C} and F, E are subfields of a common field, then $k \subseteq EF$ is in \mathcal{C} .²⁸⁹

PROP: The class of algebraic extensions is distinguished, and so is the class of finite extensions.²⁹⁰

THM: Separable extensions form a distinguished class of extensions.²⁹¹

4.2 Normal Extensions

DEF: Let k be a field and $f \in k[x]$ with $\deg f \geq 1$. An extension F/k is a *splitting field* for f if f splits into linear factors in $F[x]$.²⁹² For a family $\{f_i\}_{i \in I} \subseteq k[x]$, the *splitting field* of this family is an extension F/k such that each f_i splits in F .²⁹³

THM: Let K be a splitting field of the polynomial $f(x) \in k[x]$. If E is another splitting field of f , then there exists an isomorphism $\sigma : E \rightarrow K$ inducing the identity on k . If $k \subseteq K \subseteq k^a$, where k^a is an algebraic closure of k , then any embedding of E in k^a inducing the identity on k must be an isomorphism of E onto K .²⁹⁴

COR: Let K be a splitting field for the family $\{f_i\}_{i \in I}$ and let E be another splitting field. Any embedding of E into K^a inducing the identity on k gives an isomorphism of E onto K .²⁹⁵

THM: "Conditions for Normal Extensions" Let K be an algebraic extension of k , contained in an algebraic closure k^a of k . Then the following conditions are equivalent:

(i) Every embedding of K in k^a over k induces an automorphism of K .

(ii) K is the splitting field of a family of polynomials in $k[x]$.

(iii) Every irreducible polynomial of $k[x]$ which has a root in K splits into linear factors in K .²⁹⁶

DEF: An extension K/k that satisfies the normality conditions is called a *normal* extension.²⁹⁷

THM: Normal extensions remain normal under lifting:

(i) If $k \subseteq E \subseteq K$ and K is normal over k , then E is normal over k .

(ii) If K_1, K_2 are normal over k and are contained in some field L , then $K_1 K_2$ is normal over k and so is $K_1 \cap K_2$.²⁹⁸

4.3 Separable Extensions

PROP: Let $p(x) = \text{IrrPoly}_k(\alpha)$ and let $\sigma : k \rightarrow L$ be an embedding of k into an algebraically closed field L . The number of possible extensions of σ to $k(\alpha)$ is $\leq \deg p$, and is equal to the number of distinct roots of p in k^a .²⁹⁹

DEF: Given an extension E/F , the *separable degree* of E over F , written $[E : F]_s$ is the cardinality of the set of embeddings of $E \hookrightarrow F^a$ over F .³⁰⁰

THM: "Separable Degrees Multiply" Let $k \subseteq F \subseteq E$ be a tower. Then $[E : k]_s = [E : F]_s [F : k]_s$. Furthermore, if E is finite over k , then $[E : k]_s$ is finite and $[E : k]_s \leq [E : k]$. The separable degree is at most equal to the degree.³⁰¹

COR: Let E be finite over k and $k \subseteq F \subseteq E$. The equality $[E : k]_s = [E : k]$ holds if and only if the corresponding equalities hold for each step of the tower (for E/F and F/k).³⁰²

DEF: An extension E/k is *separable* over k if $[E : k]_s = [E : k]$. An element $\alpha \in k^a$ is *separable* if $k[\alpha]$ is separable over k . A polynomial $f(x) \in k[x]$ is *separable* if it has no multiple roots.³⁰³

THM: Let E be a finite extension of k . Then E is separable over k if and only if each element of E is separable over k .³⁰⁴

DEF: A field E is *separable* over k if every finitely generated intermediate extension is separable over k .³⁰⁵

THM: Let E be an algebraic extension of k , generated by a family of elements $\{\alpha_i\}_{i \in I}$. If each α_i is separable over k , then E is separable over k .³⁰⁶

DEF: The compositum of all separable extensions of a field k in a given algebraic closure k^a is called the *separable closure*, denoted k^s or k^{sep} .³⁰⁷

DEF: If E is an algebraic extension of k and σ any embedding of E over k , then $\sigma(E)$ is a *conjugate* of E in k^a . For $\alpha \in k^a$, if $\sigma_1, \dots, \sigma_n$ are distinct embeddings of $k[\alpha]$ into k^a , then $\sigma(\alpha)$ is a *conjugate* of α in k^a .³⁰⁸

DEF: If a field $E = k[\alpha]$, then α is called a *primitive element* of E over k .³⁰⁹

THM: “Primitive Element Theorem” Let E be a finite extension of a field k . There exists an element $\alpha \in E$ such that $E = k[\alpha]$ if and only if there exists only a finite number of intermediate fields F . If E is separable over k , then there exists such an element α .³¹⁰

4.4 Splitting Fields

PROP: Let K/F be a splitting field of $f \in F[x]$, let $\phi : F \rightarrow \bar{F}$ be a field isomorphism, and let $\bar{f} \in \bar{F}[x]$ be the corresponding polynomial. Let \bar{K}/\bar{F} be a splitting field on \bar{f} . Then there are $[K : F]$ distinct isomorphisms $K \rightarrow \bar{K}$ that agree with ϕ on F .³¹¹

COR: “Uniqueness of Splitting Fields” If K/F and \bar{K}/F are splitting fields of $f \in F[x]$, then there is an isomorphism $K \rightarrow \bar{K}$ that fixes the elements of F .³¹²

THM: “Characterization of Galois Extensions” Let K/F be a field extension of finite degree n . The following are equivalent:

- (i) K/F is Galois ($|\text{Gal}(K/F)| = n$)
- (ii) $|\text{Gal}(K/F)| \geq n$
- (iii) $K^{\text{Gal}(K/F)} = F$.
- (iv) K/F is a splitting field of some $f \in F[x]$.
- (v) K/F is a splitting field of some irreducible $f \in F[x]$.
- (vi) If f is an irreducible polynomial in $F[x]$ and f has at least one root in K , then f splits into linear factors in $K[x]$.³¹³

4.5 Galois Extensions in Characteristic 0

DEF: Let K/F be a field extension of finite degree, and let $\text{Gal}(K/F)$ be the *Galois group* of automorphisms of K that fix every element of F . The extension K/F is *Galois* provided $|\text{Gal}(K/F)| = [K : F]$.³¹⁴

THM: “Primitive Element Theorem” Given an extension K/F of finite degree, there exists an $\alpha \in K$ such that $K = F(\alpha)$.³¹⁵

PROP: Let K/F be a field extension and let $f \in F[x]$.

- (i) Suppose $\alpha \in K$, $f(\alpha) = 0$, and $\sigma \in \text{Gal}(K/F)$. Then $f(\sigma(\alpha)) = 0$.
- (ii) Suppose α and β are roots of f in K . Assume f is irreducible over F . Then there is an isomorphism $F(\alpha) \rightarrow F(\beta)$ taking α to β and fixing every element of F .³¹⁶

THM: Let K be a field, and let G be a finite group of automorphisms of K and let $K^G = \{ \alpha \in K \mid g(\alpha) = \alpha \forall g \in G \}$. Then K/K^G is a Galois extension, and $G = \text{Gal}(K/K^G)$.³¹⁷

THM: “Fundamental Theorem of Galois Theory” Let K/F be a Galois extension. Let L , with $F \subseteq L \subseteq K$ be an intermediate field.

- (i) For each intermediate field L , K/L is Galois, and $\text{Gal}(K/L) \leq \text{Gal}(K/F)$.
- (ii) For each subgroup $H \leq \text{Gal}(K/F)$, K^H is an intermediate field.
- (iii) The mappings $L \mapsto \text{Gal}(K/L)$ and $H \mapsto K^H$ are reciprocal, order-reversing bijections between intermediate fields and subgroups of $\text{Gal}(K/F)$.

Suppose L is an intermediate field with corresponding subgroup $\text{Gal}(K/L) = H$.

- (iv) $[K : L] = |H|$ and $[L : F] = [\text{Gal}(K/F) : \text{Gal}(K/L)]$.
- (v) L/F is Galois $\iff \text{Gal}(K/L) \trianglelefteq \text{Gal}(K/F) \iff g(L) = L$ for every $g \in \text{Gal}(K/F)$.
- (vi) When the equivalent conditions of (v) are true, the restriction map $\rho : g \mapsto g|_L$ is a surjection $\text{Gal}(K/F) \rightarrow \text{Gal}(L/F)$ with kernel $\text{Gal}(K/L)$. In particular, $\text{Gal}(K/F)/\text{Gal}(K/L) \cong \text{Gal}(L/F)$.³¹⁸

4.6 Galois Theory

4.7 Radical Extensions and Solvable Groups

DEF: A field extension K/F is a *radical extension* provided there exist positive integers r, n_1, \dots, n_r , and elements $\beta_1, \dots, \beta_r \in K$ such that $\beta_j^{n_j} \in F(\beta_1, \dots, \beta_{j-1})$ for $j = 1, \dots, r$. The numbers n_j are called the *associated exponents*. These are not necessarily unique.³¹⁹

PROP: Let E/F be a splitting field of $x^n - 1$ over F . Then $\text{Gal}(E/F)$ is abelian.³²⁰

PROP: Let $K = E(\beta)$, where $\beta^n \in E$ for some integer n , and suppose E contains a primitive n th root of unity ζ . The K/E is Galois and $\text{Gal}(K/E)$ is abelian.³²¹

PROP: Let E/F be a Galois extension and K/E a radical extension. Then there is an extension L/E such that
 (i) L/F is Galois, (ii) L/E is a radical extension, and (iii) no new exponents are introduced.³²²

THM: Let $f \in F[x]$ be an irreducible polynomial with a root in some radical extension of F . Then the Galois group of f is solvable.³²³

4.8 Algebraic Closure

DEF: Let E be an extension field of F and let $\sigma : F \rightarrow L$ be an embedding. An embedding $\tau : E \rightarrow L$ is said to be *over* σ (or τ *extends* σ) if the restriction of τ to F is equal to σ . If $\sigma = \text{id}_F$, then τ is an embedding of E over F .³²⁴

LMA: Let E be an algebraic extension of k , and let $\sigma : E \rightarrow E$ be an embedding of E into itself over k . Then σ is an automorphism.³²⁵

LMA: Let E_1, E_2 be extensions of k , contained in some bigger field E and let σ be an embedding of E in some field L . Then $\sigma(E_1 E_2) = \sigma(E_1)\sigma(E_2)$.³²⁶

PROP: Let k be a field and f a polynomial in $k[x]$ of degree ≥ 1 . Then there exists an extension E of k in which f has a root.³²⁷

COR: Let k be a field and let f_1, \dots, f_n be polynomials in $k[x]$ of degrees ≥ 1 . Then there exists an extension field E of k in which each f_i has a root.³²⁸

DEF: A field L is *algebraically closed* if every polynomial in $L[x]$ of degree ≥ 1 has a root in L .³²⁹

THM: Let k be a field. There exists an algebraically closed field with k as a subfield.³³⁰

COR: Let k be a field. There exists an extension k^a which is algebraic over k and algebraically closed.³³¹

THM: Let k be a field, E an algebraic extension of k , and $\sigma : k \rightarrow L$ an embedding of k into an algebraically closed field L . Then there exists an extension of σ to an embedding of E in L . If E is algebraically closed and L is algebraic over $\sigma(k)$, then any such extension of σ is an isomorphism of E onto L .³³²

COR: Let k be a field, and let E, E' be algebraic extensions of k . If E and E' are algebraically closed, then there exists an isomorphism $\tau : E \rightarrow E'$ over k .³³³

DEF: The unique (up to isomorphism) field extension of k that is algebraic and is algebraically closed is the *algebraic closure* of k , written k^a .

4.9 Finite Fields

THM: For each prime p and integer $n \geq 1$ there exists a finite field of order p^n denoted \mathbb{F}_{p^n} , uniquely determined as a subfield of an algebraic closure \mathbb{F}_p^a . It is the splitting field of the polynomial $x^{p^n} - x$ and its elements are the roots of this polynomial. Every finite field is isomorphic to exactly one field \mathbb{F}_{p^n} .³³⁴

COR: Let \mathbb{F}_q be a finite field. Let n be an integer ≥ 1 . In a given algebraic closure \mathbb{F}_q^a , there exists one and only one extension of \mathbb{F}_q of degree n , and this extension is the field \mathbb{F}_{q^n} .³³⁵

THM: The multiplicative group of a finite field is cyclic.³³⁶

DEF: Let q be a prime power. Consider the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$. The *Frobenius map*, $\varphi_q : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n}$, such that $\varphi_q(x) = x^q$ is an automorphism of \mathbb{F}_{q^n} over \mathbb{F}_q .³³⁷

THM: The group of automorphisms of \mathbb{F}_{q^n} is cyclic of degree n , generated by φ_q .³³⁸

THM: Let m, n be integers ≥ 1 . Then in any algebraic closure of \mathbb{F}_p , the subfield \mathbb{F}_{p^n} is contained in \mathbb{F}_{p^m} if and only if n divides m . If that is the case, let $q = p^n$ and let $m = nd$. Then \mathbb{F}_{q^d} is normal and separable over \mathbb{F}_q , and the group of automorphisms of \mathbb{F}_{p^m} over \mathbb{F}_q is cyclic of order d , generated by $\varphi_p^d = \varphi_q$.³³⁹

Artin: Algebra by Michael Artin.

D&F: Abstract Algebra by Dummit & Foote.

H: Algebra by Thomas W. Hungerford.

Lang: Algebra by Serge Lang.

²⁶⁴Hungerford. Def. 1.4. p.233; Lang. p.224.

²⁶⁵Lang. Prop 1.1. p.224.

²⁶⁶Hungerford. p. 231.

²⁶⁷Hungerford. Thm. 1.2. p. 231; Lang. Cor. 1.3. p.225.

²⁶⁸Lang. Prop. 1.2. p. 224.

²⁶⁹Lang. p.225.

²⁷⁰Hungerford. p.232; Lang. p. 226.

²⁷¹Lang. Prop. 1.5. p.226.

²⁷²Hungerford. Thm. 1.3 p. 232.

²⁷³Hungerford. p. 233; Lang. p.226.

²⁷⁴Lang. p.227.

Notes

²⁶²Hungerford. Def 1.1. p. 231. Lang. p.223.

²⁶³Hungerford. p. 231. Lang p. 224.

- ²⁷⁵Hungerford. p. 233.
²⁷⁶Hungerford. Thm 1.5. p.233.
²⁷⁷Lang. p.224.
²⁷⁸Lang. Prop 1.4. p.225.
²⁷⁹Hungerford. Thm. 1.6. p. 234.
²⁸⁰Lang. Prop. 1.6. p.227.
²⁸¹Hungerford. Def. 1.7. p.234; Lang. p. 224.
²⁸²Hungerford. Thm 1.8. p. 235.
²⁸³Hungerford. Cor 1.9. p.236.
²⁸⁴Hungerford. Thm 1.10. p.236.
²⁸⁵Hungerford. Thm 1.11. p.237.
²⁸⁶Hungerford. Thm.1.12. p.237.
²⁸⁷Hungerford. Thm. 1.13. p.237.
²⁸⁸Hungerford. Thm. 1.14. p.238.
²⁸⁹Lang. p.227.
²⁹⁰Lang. Prop 1.7. p.228.
²⁹¹Lang. Thm 4.5. p.241.
²⁹²Lang. p.235.
²⁹³Lang. p.236.
²⁹⁴Lang. Thm. 3.1. p.236.
²⁹⁵Lang. Cor.3.2.p.237.
²⁹⁶Lang. Thm 3.3 p.237.
²⁹⁷Lang. p.238.
²⁹⁸Lang. Thm 3.4 p.238.
²⁹⁹Lang. Prop. 2.7. p. 233.
³⁰⁰Lang. p.239.
³⁰¹Lang. Thm 4.1 pp.239-240.
³⁰²Lang Cor 4.2 p.240.
³⁰³Lang p.240.
³⁰⁴Lang Thm 4.3 p.241.
³⁰⁵Lang p.241.
³⁰⁶Lang Thm 4.4 p.241.
³⁰⁷Lang p.243.
³⁰⁸Lang p.243.
³⁰⁹Lang p.244.
³¹⁰Lang Thm 4.6. p.243.
³¹¹R. Wiegand, "Galois Theory Review" Proposition 2.1.
³¹²R. Wiegand, "Galois Theory Review" Corollary 2.2.
³¹³R. Wiegand, "Galois Theory Review" Theorem 2.3.
³¹⁴R Wiegand. "Galois Theory Review" Definition 1.1.
³¹⁵R Wiegand. "Galois Theory Review" Theorem 1.2.
³¹⁶R Wiegand. "Galois Theory Review" Proposition 1.3.
³¹⁷R Wiegand. "Galois Theory Review" Theorem 1.5.
³¹⁸R Wiegand. "Galois Theory Review" Theorem 1.5
³¹⁹R. Wiegand, "Galois Theory Review" Definition 3.2.
³²⁰R. Wiegand, "Galois Theory Review" Proposition 3.2.
³²¹R. Wiegand, "Galois Theory Review" Proposition 3.3.
³²²R. Wiegand, "Galois Theory Review" Proposition 3.4.
³²³R. Wiegand, "Galois Theory Review" Theorem 3.8.
³²⁴Lang. p.229.
³²⁵Lang. Lma. 2.1. p.230.
³²⁶Lang. Lma. 2.2. p.230.
³²⁷Lang. Prop. 2.3. p.231.
³²⁸Lang. Cor. 2.4.p.231.
³²⁹Lang. p.231.
³³⁰Lang. Thm. 2.5. p.231.
³³¹Lang. Cor. 2.6. p.232.
³³²Lang. Thm. 2.8. p.233.
³³³Lang. Cor. 2.9. p.234.
³³⁴Lang Thm 5.1 p.246.
³³⁵Lang Cor 5.2 p.246.
³³⁶Lang Thm 5.3 p.246.
³³⁷Lang p.246.
³³⁸Lang Thm 5.4 p.246.
³³⁹Lang Thm 5.5 p.247.

5 Proofs to Know

THM: “Hilbert Basis Theorem” Let R be a commutative ring with identity. If R is Noetherian, then so is $R[x]$.³⁴⁰

Proof. Let I be an ideal in $R[x]$. Define a sequence of ideals A_i ($i \geq 0$) consisting of 0 and all the elements of R that are leading coefficients of a polynomial in I of degree i . Each A_i is an ideal since $R \subseteq R[x]$, and I has closure under multiplication and addition. Also, $A_i \subseteq A_{i+1}$ since for each $a \in A_i$ there is a polynomial $f_a \in I$ of degree i with leading coefficient a . Then $xf_a \in I$ as well, has degree $i+1$ and leading coefficient a , so $a \in A_{i+1}$.

This leads to an ascending chain of ideals $A_0 \subseteq A_1 \subseteq \dots$ in R . Since R is Noetherian, this sequence eventually stabilizes at A_m for some $m \geq 0$, that is $A_n = A_m$ for all $n \geq m$. By a theorem, these ideals are finitely generated. So, let r_1, r_2, \dots, r_{n_i} be generators for A_i , appending new generators for each ascending ideal until A_m . If $A_i = 0$, then set $n_i = 0$.

Choose polynomials $f_{j,i} \in I$ such that $f_{j,i}$ has leading coefficient r_i and is of degree j for all $0 \leq j \leq m$ and $0 < i \leq n_j$.

I claim that this finite list of polynomials generates J .

Let X be the ideal generated by the $f_{j,i}$'s. Clearly $X \subseteq J$. Given $g \in J$ with $g \neq 0$. Prove by induction on $\deg g$. Case $\deg g = 0$, then g is a constant, so its leading term is $r \in A_0$, which has $r = s_1 r_1 + \dots + s_{i_0} r_{i_0}$ with $s_1, \dots, s_{i_0} \in R$. Thus, $g = s_1 f_{0,1} + \dots + s_{i_0} f_{0,i_0} \in X$. Assume $g \in X$ for all g with $\deg g < k$.

If $k \leq m$, then the leading coefficient of g is $r = s_1 r_1 + \dots + s_{i_k} r_{i_k} \in A_k$. Then, $g - \sum_{i=1}^{i_k} s_i f_{k,i} \in J$ has degree strictly less than k , so must have $g - \sum_{i=1}^{i_k} s_i f_{k,i} \in X$ and therefore $g \in X$.

If $k > m$, then the leading coefficient of g is $r = s_1 r_1 + \dots + s_{i_m} r_{i_m} \in A_k = A_m$. Then, $g - \sum_{i=1}^{i_m} s_i f_{m,i} x^{k-m} \in J$ has degree strictly less than k , so is in X . This implies $g \in X$.

Therefore, $J \subseteq X$, so equality holds and J is finitely generated. Since every ideal of $R[x]$ is finitely generated, then $R[x]$ is Noetherian. \square

THM: “Spectral Theorem” Every normal matrix over \mathbb{C} is unitarily similar to a diagonal matrix. [Recall a square matrix P is *unitary* given $PP^* = I$. A square matrix P is *normal* if $PP^* = P^*P$. Two square matrices are *unitarily similar* if there is a unitary matrix P such that $P^*AP = B$.]

Proof. Proceed by induction on n . When $n = 1$, a normal matrix N has a single entry, so is diagonal. Assume every normal matrix over \mathbb{C} of size $n \times n$ is unitarily similar to a diagonal matrix for $n < k$ for some $k > 1$.

Let A be a $k \times k$ normal matrix. Let v be an eigenvector for an eigenvalue λ . Without loss of generality, assume v has length 1 by resizing. v can be extended to an orthonormal basis $\{v, v_2, \dots, v_k\}$. Let $Q = [v \ v_2 \ \dots \ v_k] \in U_k$, a unitary matrix. Then, define

$$A' = Q^*AQ = \begin{bmatrix} \lambda_1 & a_2 & \dots & a_k \\ 0 & & & \\ \vdots & & A_1 & \\ 0 & & & \end{bmatrix},$$

where A_1 is a $(k-1) \times (k-1)$ matrix acting as a minor of A' . Note that

$$\begin{aligned} (A')^*A' &= Q^*A^*QQ^*AQ \\ &= Q^*A^*AQ \\ &= Q^*AA^*Q && \text{(normality of } A) \\ &= Q^*AQQ^*A^*Q \\ &= A'(A')^*. \end{aligned}$$

Therefore, A' is normal. Now consider

$$\begin{aligned} \begin{bmatrix} \overline{\lambda_1}\lambda_1 & \dots \\ \vdots & A_1^*A_1 \end{bmatrix} &= (A')^*(A') \\ &= (A')(A')^* = \begin{bmatrix} \overline{\lambda_1}\lambda_1 + \overline{a_1}a_1 + \dots + \overline{a_k}a_k & \dots \\ & \vdots & & A_1A_1^* \end{bmatrix} \end{aligned}$$

Therefore, $\overline{\lambda_1}\lambda_1 + \overline{a_1}a_1 + \dots + \overline{a_k}a_k = \overline{\lambda_1}\lambda_1$. Since $\overline{a_i}a_i \in \mathbb{R}_{\geq 0}$, then each $a_i = 0$. So,

$$A' = \begin{bmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A_1 & \\ 0 & & & \end{bmatrix}.$$

Now, A_1 is a normal matrix since

$$\begin{bmatrix} \overline{\lambda_1}\lambda_1 & \dots \\ \vdots & A_1^*A_1 \end{bmatrix} = \begin{bmatrix} \overline{\lambda_1} & \\ & A_1^* \end{bmatrix} \begin{bmatrix} \lambda_1 & \\ & A_1 \end{bmatrix} = (A')^*A' = A'(A')^* = \begin{bmatrix} \overline{\lambda_1} & \\ & A_1^* \end{bmatrix} \begin{bmatrix} \lambda_1 & \\ & A_1 \end{bmatrix} = \begin{bmatrix} \overline{\lambda_1}\lambda_1 & \dots \\ \vdots & A_1A_1^* \end{bmatrix}.$$

Thus, $A_1^*A_1 = A_1A_1^*$ so A_1 is normal. By induction, there is a unitary matrix $P \in U_{k-1}$ such that $P^*A_1P = A_2$ a diagonal matrix. So, Let $P' = \begin{bmatrix} 1 & \\ & P \end{bmatrix} \in U_k$. Then $P'^*A'P' = P'^*Q^*AQP' = (QP')^*A(QP') = \begin{bmatrix} \lambda_1 & \\ & A_2 \end{bmatrix}$, a diagonal matrix. Therefore, A is unitarily similar to a diagonal matrix. \square

PROP: There are no simple groups of order pq where p and q are distinct primes.

Proof. Let G be a group of order pq where p and q are distinct primes. Assume $p < q$. Consider any Sylow q -subgroup Q . Since $[G : Q] = p$, the smallest prime divisor of G , then $Q \trianglelefteq G$. \square