Theorems
Algebra qualifying course
MSU, Fall 2016

Joshua Ruiter

October 15, 2019

This document was made as a way to study the material from the fall semester algebra qualifying course at Michigan State University, in fall of 2016. It serves as a companion document to the "Definitions" review sheet for the same class.

Contents

1 Groups **3**
- 1.1 Monoids and sets . . . 3
- 1.2 Basic properties of groups . . . 3
- 1.3 Normal subgroups . . . 4
- 1.4 Exact sequences of groups . . . 5
- 1.5 Group isomorphism theorems . . . 5
- 1.6 Cyclic groups . . . 6
- 1.7 Towers and solvability . . . 6
- 1.8 Group actions . . . 7
- 1.9 Symmetric group . . . 8
- 1.10 Sylow theory . . . 8
- 1.11 Abelian groups . . . 9
  - 1.11.1 Finitely generated abelian groups . . . 10
  - 1.11.2 Dual group . . . 10

2 Categories **11**

3 Rings **11**

4 Localization **12**
- 4.1 Polynomials . . . 13

5 Modules **14**
- 5.1 The hom functor . . . 15
- 5.2 Free modules . . . 15

1 Groups

1.1 Monoids and sets

Proposition 1.1. *Let I, J be sets and let G be a commutative monoid. Let $f : I \times J \to G$ such that $f(i,j) = 1$ for all but finitely many pairs (i,j). Then*

$$\prod_{i\in I}\left(\prod_{j\in J} f(i,j)\right) = \prod_{j\in J}\left(\prod_{i\in I} f(i,j)\right)$$

Proposition 1.2. *Let S, T be finite sets. Let $M = \{f : S \to T\}$ be the set of maps from S to T. Then $|M| = |T|^{|S|}$.*

1.2 Basic properties of groups

Proposition 1.3. *Inverses are unique in groups. That is, if G is a group with identity e and $x \in G$ and y, y' satisfy $xy = yx = e$ and $xy' = y'x = e$, then $y = y'$.*

Theorem 1.4. *The intersection of subgroups is a subgroup.*

Note: The union of subgroups need to be a subgroup in general. However, the next theorem gives a decisive criterion for the union of subgroups to be a subgroup.

Theorem 1.5. *Let G be a group and H, K subgroups. Then $H \cup K$ is a subgroup if and only if $H \subset K$ or $K \subset H$.*

Theorem 1.6. *Two group homomophisms that agree on a generating set are the same. More precisely, if $f, f' : G \to G'$ are group homomorphisms and S is a set of generators for G and $f(x) = f'(x)$ for $x \in S$, then $f = f'$.*

Theorem 1.7. *The composition of group homomorphisms is a homomorphism.*

Theorem 1.8. *A group homomorphism is injective if and only if its kernel is trivial.*

Theorem 1.9. *If $\phi : G \to G'$ is a group homomorphism and $g \in G$ has finite order, then the order of $\phi(g)$ divides the order of g. In particular, the order of $\phi(g)$ is less than or equal to the order of g.*

Theorem 1.10 (Basic Properties of Cosets)**.** *Let G be a group and H a subgroup and let $a, b \in G$. Then*

$$|aH| = |bH|$$
$$h \in H \iff hH = H$$
$$aH = bH \iff aH \cap bH \neq \emptyset$$

Theorem 1.11. *Let G be a group and H a subgroup. Then $|G| = [G : H]|H|$.*

Corollary 1.12. *The order of a subgroup divides the order of the group.*

Corollary 1.13. *Every finite group of prime order is cyclic.*

1.3 Normal subgroups

Corollary 1.14. *Let G be a finite group and let H be a normal subgroup. Then* $|G| = |G/H||H|$

Theorem 1.15. *The intersection of normal subgroups is a normal subgroup. More precisely, if $\{H_i\}_{i\in I}$ is a family of normal subgroups of G, then $\cap_{i\in I} H_i$ is a normal subgroup of G.*

Theorem 1.16. *The kernel of a group homomorphism is a normal subgroup and the image of a group homomorphism is a subgroup.*

Theorem 1.17. *Let $f : G \to G'$ be a group homomorphism and H' a normal subgroup of G'. Then $f^{-1}(H')$ is a normal subgroup of G.*

Theorem 1.18. *Every normal subgroup is the kernel of some group homomorphism.*

Theorem 1.19. *The centralizer of a subset is a subgroup.*

Theorem 1.20. *The normalizer of a subset is a subgroup.*

Theorem 1.21. *The centralizer of a given set is a normal subgroup of the normalizer of that set. Symbolically, if S is a subset of a group G, then $C_G(S)$ is normal in $N_G(S)$.*

Theorem 1.22 (Proposition 2.1)**.** *Let G be a group and let H, K be subgroups such that $H \cap K = \{e\}$ and $HK = G$ and $xy = yx$ for $x \in H, y \in K$. Then the map*

$$\begin{aligned} H \times K &\to G \\ (x, y) &\mapsto xy \end{aligned}$$

is an isomorphism.

Theorem 1.23. *Let G be a group and H a subgroup. Then H is a normal subgroup of $N_G(H)$. Furthermore, $N_G(H)$ is the largest subgroup of G in which H is normal. That is, if K is a subgroup of G such that H is normal in K, then $K \subset N_G(H)$.*

Theorem 1.24. *Let G be a group with a subgroup H. If K is a subgroup of $N_G(H)$, then KH and HK are groups and $H \triangleleft KH$ and $H \triangleleft HK$.*

Theorem 1.25. *Let G be a group with subgroups H, K. If either of H, K is normal, then $HK = KH$ and HK is a subgroup (of G).*

Theorem 1.26. *Let G be a group with normal subgroups H, K. Then HK is normal.*

Theorem 1.27. *Let G be a group. A normal subgroup H is a maximal normal subgroup if and only if G/H is simple.*

Lemma 1.28. *Let G be a group and H, K be subgroups. We define $\phi : H/(H\cap K) \to HK/K$ by $g(H \cap K) \mapsto gK$. Then ϕ is a bijection. (Note that HK may not be a group.)*

Proposition 1.29. *Let H, K be subgroups of a finite group G with $K \subset N_G(H)$. Then*

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Proposition 1.30. *Let G be a group and H a subgroup of finite index. Then there is a finite number of right cosets of H, and the number of right cosets is equal to the number of left cosets.*

1.4 Exact sequences of groups

Theorem 1.31. *Let G_1, G_2, G_3 be groups and f_1, f_2 be group homomorphisms so that the sequence*

$$0 \xrightarrow{i} G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \xrightarrow{j} 0$$

is exact (where $i : 0 \to G_1$ is the map $0 \mapsto 0$ and $j : G_3 \to 0$ is the trivial map). Then f_1 is injective and f_2 is surjective.

Theorem 1.32. *Let G be a group and H a normal subgroup. Let $\iota : H \hookrightarrow G$ be the inclusion map and $\pi : G \to G/H$ be the canonical projection. Then the sequence*

$$0 \longrightarrow H \xrightarrow{\iota} G \xrightarrow{\pi} G/H \longrightarrow 0$$

is exact.

Theorem 1.33. *Let*

$$0 \longrightarrow G' \xrightarrow{\psi} G \xrightarrow{\phi} G'' \longrightarrow 0$$

be an exact sequence of groups. Then there is an isomorphism θ so that the following diagram commutes and has exact rows. Note that all the vertical maps are isomorphisms.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G' & \xrightarrow{\psi} & G & \xrightarrow{\phi} & G'' & \longrightarrow & 0 \\ & & \psi\downarrow & & \mathrm{Id}_G\downarrow & & \theta\downarrow & & \\ 0 & \longrightarrow & \ker\phi & \xrightarrow{\iota} & G & \xrightarrow{\pi} & G/\ker\phi & \longrightarrow & 0 \end{array}$$

1.5 Group isomorphism theorems

Theorem 1.34 (First Isomorphism Theorem)**.** *The image of a group homomorphism is isomorphic to the quotient by the kernel. More precisely, if $\phi : G \to G'$ is a group homomorphism, then $\operatorname{im}\phi \cong G/\ker\phi$.*

Theorem 1.35 (Second Isomorphism Theorem)**.** *Let G be a group with subgroups H, N where N is normal. Then HN is a subgroup of G, and $H \cap N$ is a normal subgroup of H, and $HN/N \cong H/(H \cap N)$.*

Theorem 1.36 (Third Isomorphism Theorem)**.** *Let G be a subgroup with normal subgroups H, K such that $K \subset H$. Then K is normal in H, so we can define a map $G/K \to G/H$ by $xK \mapsto xH$. This is a homomorphism, and the kernel is $\{xK : x \in H\}$. Therefore,*

$$(G/K)/(G/H) \cong G/H$$

Theorem 1.37. *Let $f : G \to G'$ be a group homomorphism and let $H = \ker f$. Let $\phi : G/H \to G$ be the canonical map. Then there exists a unique homomorphism $f_* : G/H \to G'$ such that $f = f_* \circ \phi$ and f_* is injective. In particular, f_* is the map $xH \mapsto f(x)$.*

Theorem 1.38. *Let G be a group and H a subgroup. Let N be the intersection of all normal subgroups containing H. Let $f : G \to G'$ be a homomorphism with $H \subset \ker f$, and let $\phi : G/N \to N$ be the canonical map. Then $N \subset \ker f$ and there exists a unique homomorphism $f_* : G/N \to G$ such that $f_* \circ \phi = f$. In particular, f_* is the map $xN \mapsto f(x)$.*

1.6 Cyclic groups

Theorem 1.39. *Let H be a nontrivial subgroup of $\mathbb{Z}$. Then $H = n\mathbb{Z}$ for some $n \in \mathbb{Z}$.*

Theorem 1.40. *Every subgroup of a cyclic group is cyclic.*

Theorem 1.41. *Two finite cyclic groups of the same order are isomorphic.*

Theorem 1.42. *Let G be a finite cyclic group of order n, and let x be a generator of G. Then $g \in G$ is a generator if and only if $g = x^k$ where $\gcd(k, n) = 1$. That is, the generators of $\mathbb{Z}/n\mathbb{Z}$ are precisely those numbers that are relatively prime to n.*

Theorem 1.43. *Let G be a cyclic group and let a, b be generators of G. Then there exists a unique automorphism of G mapping a to b.*

Theorem 1.44. *Let G be a cyclic group of order n and let d be a positive integer dividing n. Then there exists a unique subgroup of G of order d.*

Theorem 1.45. *The direct sum of cyclic groups is cyclic if and only if the groups have relatively prime orders. More precisely, if G_1, G_2 are cyclic groups, then $G_1 \times G_2$ is cyclic if and only if $\gcd(|G_1|, |G_2|) = 1$.*

1.7 Towers and solvability

Theorem 1.46. *The preimage of a normal tower under a group homomorphisms is a normal towers. More precisely, let $f : G \to G'$ be a group homomorphism, and*

$$G' = G'_0 \supset G'_1 \supset \ldots \supset G'_n$$

be a normal tower for G'. Define $G_i = f^{-1}(G'_i)$. Then

$$G = G_0 \supset G_1 \supset \ldots \supset G_n$$

is a normal tower for G.

Theorem 1.47. *Every abelian group is solvable.*

Proof. Let G be abelian. Then $G \supset \{e\}$ is an abelian tower ending in the trivial group, so G is solvable. □

Theorem 1.48. *The preimage of an abelian tower (under a group homomorphism) is an abelian tower.*

Theorem 1.49. *The preimage of a cyclic tower (under a group homomorphism) is a cyclic tower.*

Theorem 1.50. *Let G be a finite group with an abelian tower. Then there is a refinement of that tower that is cyclic.*

Theorem 1.51. *Let G be a finite solvable group. Then G has a cylic tower ending in the trivial group.*

Theorem 1.52. *Let G be a group and H a normal subgroup. Then G is solvable if and only if H and G/H are solvable.*

Theorem 1.53. *The commutator subgroup is normal, and the quotient by the commutator subgroup gives an abelian group. More precisely, if G is a group, then $[G,G]$ is normal in G and $G/[G,G]$ is abelian.*

Theorem 1.54. *An abelian group is simple if and only if it is cyclic of prime order.*

Theorem 1.55 (Butterfly Lemma)**.** *Let U, V be subgroups of a group. Let u, v be normal subgroups of U and V respectively. Then*

$$u(U \cap v) \lhd u(U \cap V)$$
$$(u \cap V)v \lhd (U \cap V)v$$
$$u(U \cap V)/u(U \cap v) \cong (U \cap V)v/(u \cap V)v$$

Theorem 1.56 (Schreier's Theorem)**.** *Two normal towers of subgroups ending with the trivial group have equivalent refinements.*

Theorem 1.57 (Jordan-Holder)**.** *Let G be a group and let*

$$G = G_1 \supset G_2 \supset \ldots \supset G_n = \{e\}$$

be a normal tower so that each group G_i/G_{i+1} is simple and $G_i \neq G_{i+1}$. Then any other normal tower of G having these properties is equivalent to this tower.

1.8 Group actions

Theorem 1.58. *Let G act on a set S and let $s \in S$. The stabilizer of s is a subgroup of G.*

Theorem 1.59. *Let G act on a set S and let $s, t \in S$. Then G_s and G_t are conjugate.*

Theorem 1.60. *Let G act on a set S and let $s \in S$. Let G also act on G/G_s by $g.xG_s = (gx)G_s$. Define $f : G/G_s \to S$ by $xG_s \mapsto xs$. Then f is well-defined and f is a morphism of G-sets. Furthermore, f is injective and the image of f is the orbit $G.s$. Therefore, f induces a bijection between G/G_s and $G.s$.*

Theorem 1.61 (Orbit-Stabilizer Theorem)**.** *Let G be a group acting on a set S and let $s \in S$. Then the order of the orbit $G.s$ is equal to the index of G_s, that is, $|G.s| = [G : G_s]$. If G is finite, then we get $|G.s| = |G|/|G_s|$.*

Theorem 1.62. *Let G be a group and let it act on itself by conjugation. Let $x \in G$. Then the stabilizer of x is the normalizer of x.*

Theorem 1.63. *Let G be a group and let it act on the set of subgroups by conjugation. Let H be a subgroup. Then the stabilizer of H is the normalizer of H.*

Theorem 1.64. *Let G act on its subgroups by conjugation and let H be a subgroup. By the Orbit-Stabilizer Theorem, the order of the orbit of H is equal to the index of the stabilizer of H. The order of the orbit of H is equal to the number of subgroups conjugate to H, and the index of the stabilizer is equal to the index of the normalizer of H.*

Theorem 1.65 (Orbit Decomposition Formula)**.** *Let G act on a set S. The orbits of the group action form a partition of S. Thus*

$$|S| = \sum_{i \in I} [G : G_{s_i}]$$

where I is an indexing set so that each s_i is a representative of a distinct orbit.

Theorem 1.66 (Class Equation)**.** *Let G act on itself by conjugation. Then for $x \in G$, we have $x \in Z(G)$ if and only if the orbit of x is just $\{x\}$. Thus*

$$|G| = |Z(G)| + \sum_{i \in I} [G : G_{x_i}] = |Z(G)| + \sum_{i \in I} |\operatorname{cl}(x_i)|$$

where I is an indexing set so that $x_i \notin Z(G)$ and each x_i is a representative of a distinct conjugacy class.

1.9 Symmetric group

Theorem 1.67. *There exists a unique homomorphism $\epsilon : S_n \to \{-1, 1\}$ such that for every transposition τ, we have $\epsilon(\tau) = -1$. For $\sigma \in S_n$, we call $\epsilon(\sigma)$ the **sign** of σ.*

Theorem 1.68. *S_n is generated by transpositions.*

Theorem 1.69. *S_n is generated by $(1\ 2)$ and $(1\ 2 \ldots n)$.*

Theorem 1.70. *If n is prime and σ is an n-cycle and τ is a transposition, then σ, τ generate S_n.*

Theorem 1.71. *If $n \geq 5$, then S_n is not solvable.*

Theorem 1.72. *If $n \geq 5$, then A_n is simple.*

1.10 Sylow theory

Lemma 1.73. *Let G be a finite abelian group of order m and let p be a prime dividing m. Then G has a subgroup of order p. (Note: This is true for non-abelian groups as well.)*

Lemma 1.74. *Let H be a p-group acting on a finite set S. Then*

1. *The number of fixed points of H is congruent to $|S| \pmod p$.*
2. *If H has exactly one fixed point, then $|S|$ is congruent to $1 \pmod p$.*
3. *If p divides $|S|$, then the number of fixed points of H is congruent to $0 \pmod p$.*

Theorem 1.75 (First Sylow Theorem)**.** *Let G be a finite group and p a prime dividing $|G|$. Then there exists a Sylow p-subgroup of G.*

Theorem 1.76 (Second Sylow Theorem)**.** *Let G be a finite group and p a prime dividing $|G|$. Then all Sylow p-subgroups of G are conjugate.*

Theorem 1.77. *Let G be a finite group, and H a p-subgroup. Then H is contained in some Sylow p-subgroup.*

Theorem 1.78 (Third Sylow Theorem)**.** *Let G be a finite group, and p a prime dividing $|G|$. Let n_p be the number of distinct Sylow p-subgroups of G and let P be a Sylow p-subgroup of G. Then $n_p \equiv 1 \bmod p$ and $n_p = [G : N_G(P)]$ and n_p divides $[G : P]$. Hence, n_p divides $|G|/|P|$. Thus n_p divides $|G|/p^\alpha$, where α is the highest power of p that divides $|G|$.*

Theorem 1.79. *Let G be a finite group and p a prime dividing $|G|$. If there is a unique p-Sylow subgroup, then it is normal.*

Proof. Let P be the unique p-Sylow subgroup and n_p the number of p-Sylow subgroups. We have $n_p = 1 = [G : N_G(P)]$, so $|N_G(P)| = |G|$ so $N_G(P) = G$. So the normalizer of P is all of G. Every subgroup is normal in its normalizer, so P is normal in G. □

Theorem 1.80. *Every (nontrivial) p-group has a nontrivial center.*

Theorem 1.81. *Every p-group is solvable.*

Theorem 1.82. *Let G be a nontrivial p-group. Then there exists a sequence of subgroups*

$$G = G_n \supset G_{n-1} \supset \ldots \supset G_1 \supset G_0 = \{e\}$$

such that G_i is normal in G and G_{i+1}/G_i is cyclic of order p.

Theorem 1.83. *Let G be a finite group and let p be the smallest prime dividing the order of G. Then any subgroup of index p is normal in G.*

Proposition 1.84. *Let G be a group, and let P be a p-subgroup and Q be a q-subgroup, where p, q are distinct primes. Then $P \cap Q = \{e\}$.*

Theorem 1.85. *Let p, q be distinct primes and let G be a group of order pq. Then G is solvable.*

Lemma 1.86. *Let P, P' be p-Sylow subgroups of G with $|P| = |P'| = p$. Then $P = P'$ or $P \cap P' = \{e\}$.*

1.11 Abelian groups

Theorem 1.87. *Let $\{A_i\}_{i \in I}$ be a family of abelian groups. Define the map $\lambda_i : A_i \to \oplus_i A_i$ by $x \mapsto (0, \ldots, x, \ldots, 0)$. Then λ_i is an injective group homomorphism.*

Theorem 1.88 (Universal Property of Direct Sum)**.** *Let $f_i : A_i \to B$ be a family of homomorphisms into an abelian group. Then there is a unique homomorphism $f : \oplus_i A_i \to B$ so that $f \circ \lambda_i = f_i$ for each i. In particular, f is given by*

$$(x_i) \mapsto \sum_{i \in I} f_i(x_i)$$

Theorem 1.89. *If $\lambda : S \to S'$ is a map of sets, there is a unique homomorphism $\widetilde{\lambda}$ so that the following diagram commutes:*

$$\begin{array}{ccc} S & \xrightarrow{f_S} & \mathbb{Z}\langle S \rangle \\ \lambda \big\downarrow & & \widetilde{\lambda} \big\downarrow \\ S' & \xrightarrow{F_{S'}} & \mathbb{Z}\langle S' \rangle \end{array}$$

Theorem 1.90. *Let $f : A \to A'$ be a surjective homomorphism of abelian groups and assume that A' is free. Let $B = \ker f$. Then there exists a subgroup C of A such that $f|_C : C \to A'$ is an isomorphism, and $A = B \oplus C$.*

Theorem 1.91. *Let A be a free abelian group an let B be a subgroup. Then B is also a free abelian group, and the cardinality of a basis of B is less than or equal to the cardinality of a basis of A.*

Theorem 1.92. *Let A be a free abelian group. Then any two bases of A have the same cardinality.*

1.11.1 Finitely generated abelian groups

Theorem 1.93 (Bezout's Identity)**.** *Let $a, b \in \mathbb{N}$ and $d = \gcd(a, b)$. Then there exist integers x, y so that $ax + by = d$.*

Theorem 1.94. *Let A be a torsion abelian group. Then A is the direct sum of its subgroups $A(p)$ for all primes p such that $A(p) \neq 0$.*

Theorem 1.95. *Every finite abelian p-group is isomorphic to a product of cyclic p-groups. If it is of type $(p^{r_1}, \ldots, p^{r_n})$ with $1 \leq r_1 \leq \ldots \leq r_n$ then the sequence of (positive) integers $r_1, \ldots, r_n$ are unique.*

Theorem 1.96. *Let A be a finitely generated, torsion-free, abelian group. Then A is free.*

Theorem 1.97. *Let A be a finitely generated abelian group, and let A_{tor} be the torsion subgroup. Then A_{tor} is finite and A/A_{tor} is free. There exists a free subgroup B of A such that $A = B \oplus A_{\text{tor}}$.*

1.11.2 Dual group

Theorem 1.98. *Let $f : A \to B$ be an abelian group homomorphism and suppose A, B both have exponent m. Then the map $f^\wedge : B^\wedge \to A^\wedge$ defined by $f^\wedge(\psi) = \psi \circ f$ is a homomorphism. Note that $\text{id}^\wedge = \text{id}$ and $(f \circ g)^\wedge = g^\wedge \circ f^\wedge$.*

Theorem 1.99. *Let A, B be finite abelian groups. Then $(A \times B)^\wedge \cong A^\wedge \times B^\wedge$.*

Theorem 1.100. *A finite abelian group is isomorphic to its own dual.*

Theorem 1.101. *Let A and C be abelian groups. Then the map $A \times \text{Hom}(A, C) \to C$ given by $(a, f) \mapsto f(a)$ is a bilinear pairing.*

2 Categories

Theorem 2.1. *Let $\mathcal{C}$ be a category and let A be an object. The set of automorphisms of A forms a group.*

Theorem 2.2. *The usual direct product of groups is a product in the category of groups. More precisely, if A, B are groups, then the triple $(A \times B, \pi_A, \pi_B)$ is a product, where $\pi_A : A \times B \to A$ and $\pi_B : A \times B \to B$ are given by $\pi_A(a, b) = a$ and $\pi_B(a, b) = b$. Specifically, given a group C and morphisms $\phi : C \to A$ and $\psi : C \to B$, the unique morphism $h : C \to A \times B$ is $c \mapsto (\phi(c), \psi(c))$.*

3 Rings

Theorem 3.1. *Let A be a ring. The set of units, denoted A^*, forms a group.*

Theorem 3.2. *Let A be a commutative ring and $\mathfrak{a}, \mathfrak{b}$ be ideals. Then*

$$\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$$

If $\mathfrak{a} + \mathfrak{b} = A$, then equality holds.

Theorem 3.3. *The kernel of a ring homomorphism is an ideal.*

Theorem 3.4. *A ring homomorphism is completely determined by its effect on a set of generators.*

Theorem 3.5. *A bijective ring homomorphism is an isomorphism.*

Theorem 3.6. *The image of a ring (or subring) under a ring homomorphism is a subring.*

Theorem 3.7. *The preimage of an ideal under a ring homomorphism is an ideal.*

Theorem 3.8. *Products exist in the category of rings. More specifically, the product is just the product as abelian groups, with an obvious multiplication structure.*

Theorem 3.9. *Let A be an integral domain and let $a, b \in A$ be nonzero. Then a and b generate the same ideal if and only if a and b are associates.*

Theorem 3.10. *If an ideal contains a unit, then it is the whole ring.*

Theorem 3.11. *Every maximal ideal is prime.*

Theorem 3.12. *Every proper ideal is contained in some maximal ideal.*

Theorem 3.13. *Let A be a commutative ring and $\mathfrak{m}$ an ideal. $\mathfrak{m}$ is maximal if and only if $A/\mathfrak{m}$ is a field.*

Theorem 3.14. *The preimage of a prime ideal under a ring homomorphism of commutative rings is a prime ideal.*

Theorem 3.15. *Let $f : A \to A'$ be a surjective ring homomorphism of commutative rings. If $\mathfrak{m}'$ is maximal in A', then $f^{-1}(m')$ is maximal in A.*

Theorem 3.16. *The integers are a principal ideal domain.*

Theorem 3.17 (Chinese Remainder Theorem)**.** *Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals of A such that $\mathfrak{a}_i + \mathfrak{a}_j = A$ for all $i \neq j$. Then if $x_1, \dots, x_n \in A$, there exists $x \in A$ such that $x \equiv x_i \pmod{\mathfrak{a}_i}$ for all i.*

Theorem 3.18. *Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals of A such that $\mathfrak{a}_i + \mathfrak{a}_j = A$ for $i \neq j$. Define $f : A \to \prod_{i=1}^n A/\mathfrak{a}_i$ be the map*

$$x \mapsto (x + \mathfrak{a}_1, x + \mathfrak{a}_2, \dots, x + \mathfrak{a}_n)$$

Then $\ker f = \bigcap_{i=1}^n \mathfrak{a}_i$ and f is surjective. Hence there is an isomorphism

$$A/\bigcap \mathfrak{a}_i \cong \prod A/\mathfrak{a}_i$$

Theorem 3.19. *Let $m \in \mathbb{N}$, and write m as a product of prime powers, $m = \prod_i p_i^{r_i}$. Then*

$$\mathbb{Z}/m\mathbb{Z} \cong \prod_i \mathbb{Z}/p_i^{r_i}\mathbb{Z}$$

This induces an isomorphism

$$(\mathbb{Z}/m\mathbb{Z})^* \cong \prod_i (\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*$$

Theorem 3.20. *If p is a prime number and $r \in \mathbb{N}$, then*

$$\phi(p^r) = p^{r-1}(p-1)$$

Theorem 3.21. *Let f, g be polynomials over an integral domain. Then $\deg(fg) = \deg f + \deg g$. We also have $\deg(f+g) \leq \max(\deg f, \deg g)$.*

Theorem 3.22. *If A is an integral domain, then $A[x]$ is an integral domain.*

4 Localization

Theorem 4.1. *Let A be an integral domain and S a multiplicative subset not containing zero. Then $\phi : A \to S^{-1}A$ given by $a \mapsto \frac{a}{1}$ is injective.*

Theorem 4.2. *Let $\mathfrak{p}$ be a prime ideal of a commutative ring A. Then $S = A \setminus \mathfrak{p}$ is a multiplicative subset.*

Theorem 4.3. *Let $\mathfrak{p}$ be a prime ideal of a commutative ring A. Then $A_{\mathfrak{p}}$ is a local ring.*

Theorem 4.4. *Let $a \in A$ such that (a) is a prime ideal. Then a is irreducible.*

Theorem 4.5. *Let A be a commutative ring. Then left and right cancellation hold in A if and only if A is an integral domain.*

Theorem 4.6. *Let A be a commutative ring. If $p \in A$ is irreducible and u is a unit, then up is irreducible.*

Theorem 4.7. *Every principal ideal domain is a unique factorization domain.*

Theorem 4.8. *Greatest common denominators exist in unique factorization domains. That is, if $a, b \in A$, there exists $d \in A$ such that d is a* gcd *of a and b.*

Theorem 4.9. *Let A be a principal ideal domain and a, b be nonzero elements. If $(a)+(b) = (c)$, then c is a* gcd *of a and b.*

Theorem 4.10. *Let A be a unique factorization domain and p be an irreducible element. Then (p) is prime.*

Theorem 4.11. *Let $f : A \to A'$ be a surjective ring homomorphism. If A is local and $A' \neq 0$, then A' is local.*

Theorem 4.12. *Let A be a principal ideal domain and S a multiplicative subset not containing zero. Then $S^{-1}A$ is a principal ideal domain.*

Theorem 4.13. *Let A be a unique factorization domain and S a multiplicative subset not containing zero. Then $S^{-1}A$ is a unique factorization domain.*

4.1 Polynomials

Theorem 4.14. *Let A be a commutative ring and let $f, g \in A[x]$ be polynomials with nonzero degree, where the leading coefficient of g is a unit. Then there exist unique polynomials $q, r \in A[x]$ such that*

$$f = gq + r$$

and $\deg r < \deg g$.

Theorem 4.15. *Let k be a field. Then $k[x]$ is a principal ideal domain. Consequently, $k[x]$ is a unique factorization domain.*

Theorem 4.16. *Let k be a field and $f \in k[x]$ with* $\deg f = n \geq 0$. *Then f has at most n roots in k. If $a \in k$ is a root of f, then $(x - a)$ divides $f(x)$.*

Theorem 4.17. *Let k be a field and $f \in k[x]$. If there is an infinite subset S of k such that $f(s) = 0$ for $s \in S$, then $f(a) = 0$ for all $a \in K$.*

Theorem 4.18. *Let k be an infinite field and f a polynomial in n variables over k. If f induces the zero function on k^n, then $f = 0$.*

Theorem 4.19. *Let k be a field and U a finite multiplicative subgroup. The U is cyclic.*

Theorem 4.20. *If k is a finite field, then k^* is cyclic.*

Theorem 4.21. *Let A be a unique factorization domain and K its quotient field. Let $a, b \in K$ such that $ab \neq 0$. Then* $\operatorname{ord}_p(ab) = \operatorname{ord}_p a + \operatorname{ord}_p b$.

Theorem 4.22 (Gauss's Lemma)**.** *Let A be a unique factorization domain and K its quotient field. Let $f, g \in k[x]$. Then the content of fg is the content of f times the content of g.*

Theorem 4.23. *The product of primitive polynomials is primitive.*

Theorem 4.24. *Let A be a unique factorization domain with quotient field K.. Then $A[x]$ is a unique factorization domain. The prime elements of $A[x]$ are primes of A and primitive polynomials that are irreducible in $K[x]$.*

Theorem 4.25 (Eisenstein's Criterion)**.** *Let A be a unique factorization domain with quotient field K. Let $f(x) = a_n x^n + \ldots + a_0 \in A[x]$. If there is a prime $p \in A$ such that*

$$a_n \not\equiv 0 \pmod{p} \qquad a_i \equiv 0 \pmod{p} \qquad a_0 \not\equiv \pmod{p^2}$$

for $i < n$, then f is irreducible in $k[x]$.

Theorem 4.26 (Reduction Criterion)**.** *Let A, B be integral domains with quotient fields K, L and $\phi : A \to B$ a homomorphism. Let $f \in A[x]$ such that $\phi f \neq 0$ and $\deg \phi f = \deg f$. If ϕf is irreducible in $L[x]$, then f is irreducible in $A[x]$. If A is a unique factorization domain, then f is irreducible in $K[x]$.*

Theorem 4.27 (Integral Root Test)**.** *Let A be a unique factorization domain with quotient field K. If $f(x) = a_n x^n + \ldots + a_0 \in A[x]$. If $\alpha = b/d \in K$ is a root of f with $\gcd(b, d) = 1$, then $b|a_0$ and $d|a_n$.*

Theorem 4.28. *Let A be a commutative Noetherian ring. Then $A[x]$ is Noetherian.*

Theorem 4.29. *Let k be a field and $f \in k[x]$ a non-zero polynomial. The following are equivalent: the ideal generated by f is prime, the ideal generated by f is maximal, and f is irreducible.*

Theorem 4.30. *Let k be a field. A polynomial of degree 2 or 3 in $k[x]$ is reducible if and only if it has a root in k.*

Theorem 4.31. *Let R be an integral domain containing a field k as a subring, such that R is a finite-dimensional vector space over k. Then R is a field.*

Theorem 4.32. *Let R be a commutative ring with unity. Then $f = a_0 + a_1 x + \ldots a_n x^n \in R[x]$ is a unit if and only if a_0 is a unit in R and a_i is nilpotent for $i \geq 1$.*

5 Modules

Theorem 5.1. *The kernel, image, and cokernel of a module homomorphism are submodules.*

Theorem 5.2. *Direct products exist in the category of A-modules. In particular, they are simply direct products of abelian groups, with obvious actions from A.*

Theorem 5.3. *Let R be a commutative ring and M be an R-module. M is cylic if and only if there exists an ideal $I \subset R$ such that $M \cong R/I$. (Note that this is an isomorphism of R-modules.)*

5.1 The hom functor

Theorem 5.4. *Let A be a ring and let*

$$X' \xrightarrow{f} X \xrightarrow{g} X'' \longrightarrow 0$$

be a sequence of A-modules. This sequence is exact if and only if, for every A-module Y, the the induced sequence

$$\mathrm{Hom}_A(X',Y) \xleftarrow{\mathrm{Hom}_A(f,Y)} \mathrm{Hom}_A(X,Y) \xleftarrow{\mathrm{Hom}_A(g,Y)} \mathrm{Hom}_A(X'',Y) \longleftarrow 0$$

is exact.

Theorem 5.5. *Let A be a ring and let*

$$0 \longrightarrow Y' \xrightarrow{f} Y \xrightarrow{g} Y''$$

be a sequence of A-modules. This sequence is exact if and only if, for every A-module X, the the induced sequence

$$0 \longrightarrow \mathrm{Hom}_A(X,Y') \xrightarrow{\mathrm{Hom}_A(X,f)} \mathrm{Hom}_A(X,Y) \xrightarrow{\mathrm{Hom}_A(X,g)} \mathrm{Hom}_A(X,Y'')$$

is exact.

5.2 Free modules

Theorem 5.6. *Let A be a ring with unit 1. Then as a module over itself, A is free, with basis $\{1\}$.*

Theorem 5.7. *Let I be a nonempty set and let A be a ring. Let $A_i = A$ for $i \in I$. Then $\oplus_{i\in I} A_i$ is a free A-module. A basis is given by $\{e_i\}_{i\in I}$ where e_i has a one in the ith component and zero elsewhere.*

Theorem 5.8. *Let M be a free A-module with basis $\{x_i\}_{i\in I}$. Let N be an A-module with a subset $\{y_i\}_{i\in I}$. There exists a unique A-module homomorphism $f : M \to N$ such that $f(x_i) = y_i$ for $i \in I$.*

Theorem 5.9. *Let M, N be free A modules with bases $\{x_i\}_{i\in I}$ and $\{y_i\}_{i\in I}$ respectively. Then there is a unique A-module isomorphism $f : M \to N$ defined by $f(x_i) = y_i$.*