Definitions

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 "Theorems" review sheet for the same class.

Contents

1 Groups

1.1 Basics

Definition 1.1. *Let $f : X \to Y$ be a map of sets. We define the* ***preimage*** *of a subset of A of Y to be $\boldsymbol{f^{-1}(A)} = \{x \in X : f(x) \in A\}$.*

Definition 1.2. *Let S be a finite set. The* ***cardinality of S****, denoted $\boldsymbol{|S|}$, is the number of elements in S.*

Definition 1.3. *The* ***trivial group*** *is the group with only one element. We often use the symbol* $\mathbf{0}$ *to refer to the trivial group. A subgroup is said to be* ***trivial*** *if it is just the identity. A homomorphism is said to be* ***trivial*** *if the image is the trivial subgroup.*

Justification for using the symbol 0 for the trivial group: We can impose a "monoid" structure on the category of groups by the binary operator $G, G' \mapsto G \times G'$. (I write monoid in quotes because the object collection in the category of groups is not actually a set.) This binary operator is associative up to isomorphism; that is,

$$G \times (G' \times G'') \cong (G \times G') \times G''$$

And the trivial group is the "unit" element of this "monoid," because

$$G \times 0 \cong 0 \times G \cong G$$

So when people use the symbol 0 to refer to the trivial group, they're thinking of this "monoid" structure.

Definition 1.4. *Let G be a group. We say that $S \subset G$* ***generates*** *G if every element of G can be written as a product of elements in S. We call S a set of* ***generators*** *for G.*

Definition 1.5. *A* ***cyclic group*** *is a group G such that every element $x \in G$ is of the form a^n for some $a \in G, n \in \mathbb{N}$. That is, a cyclic group is generated by one element.*

Definition 1.6. *Let G be an abelian group and fix $n \in \mathbb{Z}$. The* ***n-th power map*** *is the map $: G \to G$ given by $\boldsymbol{x \mapsto x^n}$. It is a group homomorphism.*

Definition 1.7. *The* ***kernel*** *of a group homomorphism $\phi : G \to G'$ is the preimage of the identity, that is,* $\ker \phi = \{g \in G : \phi(g) = e'\}$.

Definition 1.8. *An* ***automorphism*** *is an isomorphism from a group to itself. The set of automorphisms of a given group G is denoted* $\mathbf{Aut}\,\boldsymbol{(G)}$. *(It is a group under function composition.)*

Definition 1.9. *An* ***endomorphism*** *is a homomorphism from a group to itself.*

Definition 1.10. *A* ***group embedding*** *is an injective group homomorphism.*

1.2 Symmetric Group

Definition 1.11. *Let S be a nonempty set and let G be the set of bijections $S \to S$. Then G is called the* ***permutation group*** *of S. (The operation is function composition.)*

Definition 1.12. *Let $J_n = \{1, \ldots, n\}$ and let S_n be the permutation group of J_n. Then S_n is called the* ***symmetric group*** *on n elements. Note that $|S_n| = n!$.*

Definition 1.13. *A* ***transposition*** *is an element $\tau \in S_n$ such that there exists $a, b \in J_n$ so that $\tau(a) = b$ and $\tau(b) = a$ and $\tau(x) = x$ for $x \neq a, b$. (Note: The transpositions generate S_n.)*

Definition 1.14. *A permutation $\sigma \in S_n$ is* ***even*** *if it can be written as a product of an even number of 2-cycles. A permutation is* ***odd*** *if it can be written as a product of an odd number of 2-cycles.*

Definition 1.15. *The* ***alternating group*** *is the subgroup of S_n of even permutations. It is denoted $\boldsymbol{A_n}$.*

1.3 Cosets and Quotient Groups

Definition 1.16. *Let G be a group, H a subset, and $x \in G$. Then we define $\boldsymbol{xH} = \{xh : h \in H\}$.*

Definition 1.17. *Let G be a group, and H, K subsets. Then we define $\boldsymbol{HK} = \{xy : x \in H, y \in K\}$.*

Definition 1.18. *Let G be a group and H a subgroup. A* ***left coset*** *for H is a subset of G of the form $aH = \{ah : h \in H\}$ for some $a \in G$.*

Using the above notation, we get the rule for multiplying cosets:

$$(xH)(yH) = xyH$$

Definition 1.19. *Let G be a group and H a subgroup. The* ***index of H in G*** *is the number of left cosets of H in G. It is denoted $\boldsymbol{[G : H]}$ or $(G : H)$.*

Definition 1.20. *Let G be a group and H a subset. We define $\boldsymbol{xHx^{-1}} = \{xhx^{-1} : h \in H\}$.*

Definition 1.21. *A subgroup $H \subset G$ is* ***normal*** *if for all $x \in G$, $xHx^{-1} = H$ (equivalently, $xH = Hx$). We denote this by $\boldsymbol{H \triangleleft G}$.*

Definition 1.22. *A group G is* ***simple*** *if its only normal subgroups are itself and the trivial subgroup, and G is nontrivial.*

Definition 1.23. *Let G be a group and H a normal subgroup. Then the* ***quotient group $\boldsymbol{G/H}$*** *is the set of cosets $\{xH : x \in G\}$ with the operation*

$$(xH)(yH) = (xy)H$$

It is a group.

Definition 1.24. *Let G be a group and H a normal subgroup. The* ***canonical map*** *or* ***canonical projection*** *from G to G/H is the map $G \to G/H$ given by $g \mapsto gH$.*

Definition 1.25. *Let G be a group. A* ***maximal normal subgroup*** *is a normal subgroup H such that if K is a normal subgroup of G with $H \subset K$, then $K = H$ or $K = G$.*

1.4 Centralizers and Normalizers

Definition 1.26. *Let G be a group and S be a subset. The* ***normalizer of S in G*** *is* $\boldsymbol{N_G(S)} = \{x \in G : xSx^{-1} = S\}$.

Definition 1.27. *Let G be a group and S be a subset. The* ***centralizer of S in G*** *is* $\boldsymbol{C_G(S)} = \{x \in G : xsx^{-1} = s \ \forall s \in S\}$.

Definition 1.28. *Let G be a group. The* ***center*** *of G is the centralizer of G in itself, which is* $\boldsymbol{Z(G)} = \{x \in G : xy = yx \ \forall y \in G\}$.

Definition 1.29. *Let G be a group and $a \in G$. We say that m is an* ***exponent of a*** *if $a^m = e$ and $m > 0$.*

Definition 1.30. *Let G be a group. We say that m is an* ***exponent of G*** *if m is an exponent of every $g \in G$.*

Definition 1.31. *Let G, H be groups. We define the* ***direct product*** *of G and H, denoted* $\boldsymbol{G \times H}$ *by $\{(g, h) : g \in G, h \in H]\}$ and define multiplication on $G \times H$ component-wise.*

Definition 1.32. *Let N, H be groups, and let $\phi : H \to \mathrm{Aut}(N)$ be a group homomorphism. We define the* ***semidirect product*** *of N and H through ϕ to be*

$$\boldsymbol{N \rtimes_{\phi} H} = \{(n, h) : n \in N, h \in H\}$$

with a multiplication defined by

$$(n_1, h_1)(n_2, h_2) = (n_1\phi(h_1)n_2, h_1h_2)$$

Definition 1.33. *Let $G_0, G_1, \ldots G_n$ be groups and $f_1, \ldots f_n$ be group homomorphism with $f_i : G_{i-1} \to G_i$.*

$$G_0 \xrightarrow{f_1} G_1 \xrightarrow{f_2} G_2 \xrightarrow{f_3} \ldots \xrightarrow{f_n} G_n$$

We call this an ***exact sequence*** *if for each i, we have* $\ker f_{i+1} = \mathrm{im}\, f_i$.

Definition 1.34. *Let G be a group. The* ***commutator subgroup*** *of G, denoted* $\boldsymbol{[G, G]}$ *is the subgroup of G generated by all elements of the form $aba^{-1}b^{-1}$ for $a, b \in G$.*

1.5 Towers

Definition 1.35. *Let G be a group. A (finite) sequence of subgroups*

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n$$

is called a ***tower of subgroups*** *for G.*

Definition 1.36. *A tower of subgroups $G_0, G_1, \ldots G_n$ is* ***normal*** *if each G_{i+1} is normal in G_i.*

Definition 1.37. *A normal tower of subgroups $G_0, \dots G_n$ is **abelian** if each quotient G_i/G_{i+1} is an abelian group.*

Definition 1.38. *A normal tower of subgroups $G_0, \dots G_n$ is **cyclic** if each quotiet G_i/G_{i+1} is a cyclic group.*

Definition 1.39. *Let $f : G \to G'$ be a group homomorphism, and let*

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

*be a tower of G'. The **preimage** of this tower is the set of preimages of each G'_i under f, that is, $f^{-1}(G'_i)$.*

Definition 1.40. *Let*

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

*be a tower of subgroups for G. A **refinement** of this tower is another tower for G formed by inserting a finite number of subgroups in between the G_i.*

Definition 1.41. *Two towers of subgroups for G given by*

$$G = G_1 \supset \dots \supset G_n$$
$$G = H_1 \supset \dots \supset H_m$$

*are **equivalent** if $n = m$ and there is a permutation σ of $\{1 \dots, n\}$ so that $G_i/G_{i+1} \cong H_{\sigma(i)}/H_{\sigma(i+1)}$ for all i.*

Definition 1.42. *A group G is **solvable** if it has an abelian tower ending in the trivial group.*

1.6 Group actions

Definition 1.43. *Let G be a group and S a set. A **group action** of G on S is a map $G \times S \to S$ given by $(x, s) \mapsto xs$ satisfying $x(ys) = (xy)s$ for all $x, y \in G, s \in S$ and $es = s$ for all $s \in S$. This is equivalent to having a homomoprhism $\pi : G \to \mathrm{Perm}(S)$.*

Definition 1.44. *Let $\psi : G \to \mathrm{Aut}(G)$ be the map $x \mapsto \psi_x$ where $\psi_x : G \to G$ is the map $y \mapsto xyx^{-1}$. This is a group action of G on itself, and it is called **conjugation**. The image of ψ in $\mathrm{Aut}(G)$ is called the set of **inner automorphisms** of G, denoted $\mathbf{Inn}(\boldsymbol{G})$.*

Definition 1.45. *Let G be a group and let $x \in G$. The **conjugacy class of x** is the set of elements of G conjugate to x, denoted $\mathbf{cl}(\boldsymbol{x})$. More precisely, $\mathrm{cl}(x) = \{a \in G : \exists g \in G \text{ such that } gxg^{-1} = a\}$.*

Definition 1.46. *Let A, B be subsets of a group G. We say that A, B are **conjugate** if there exists $x \in G$ so that $xAx^{-1} = B$.*

Definition 1.47. *Let G be a group acting on a set S and let $s \in S$. The **stabilizer of s** (also called the **isotropy group of s**) is the set $\{x \in G : xs = s\}$. It is denoted $\boldsymbol{G_s}$.*

Definition 1.48. *Let $G \to \mathrm{Perm}(S)$ be a group action. The action is called* ***faithful*** *if the kernel of this map is trivial, that is, if the only $x \in G$ that maps to Id_S is the identity.*

Definition 1.49. *Let G act on a set S. A* ***fixed point*** *of this action is an element $s \in S$ such that $xs = s$ for all $x \in G$.*

Definition 1.50. *Let G act on a set S and let $s \in S$. The* ***orbit of s*** *is the set* $\boldsymbol{G.s} = \{gs : g \in G\}$.

Definition 1.51. *Let G act on sets S, T. A map $f : S \to T$ is called a* ***G-map*** *or an* ***equivariant map*** *or a* ***morphism of G-sets*** *if $f(g.s) = g.f(s)$ for all $g \in G, s \in S$.*

Definition 1.52. *A group action is* ***transitive*** *if there is only one orbit.*

1.7 Sylow Theory

Definition 1.53. *Let p be prime. A* ***p-group*** *is a finite group of order p^n for some $n \in \mathbb{N}$.*

Definition 1.54. *Let G be a group. A* ***p-subgroup*** *is a subgroup of G that is a p-group.*

Definition 1.55. *Let G be a group. A* ***Sylow p-subgroup*** *H (or* ***p-Sylow subgroup****) is a p-subgroup of G such that $|H|$ is the highest power of p that divides $|G|$.*

1.8 Free groups

Definition 1.56. *A* ***free group*** *on a set S is the group of all words involving elements of S and their inverses, modulo an appropriate equivalence relation by reducing out terms like aa^{-1}.*

1.9 Abelian groups

Definition 1.57. *A group is* ***abelian*** *or* ***commutative*** *if $ab = ba$ for every $a, b \in G$.*

Definition 1.58. *Let $\{A_i\}_{i \in I}$ be a family of abelian groups. We define their* ***direct sum****, $\prod_i A_i$ to be the subset of the direct product $\prod_i A_i$ consisting of all tuples (x_i) such that $x_i \neq 0$ for only finitely many i.*

Definition 1.59. *Let A be an abelian group. A set of elements $\{e_i\}$ is a* ***basis*** *for A if every element of A has a unique expression*

$$x = \sum_i x_i e_i$$

where $x_i \in \mathbb{Z}$ and only finitely many $x_i \neq 0$.

Definition 1.60. *An abelian group is* ***free*** *if it has a basis.*

Definition 1.61. *Let S be a set. Then we define $\mathbb{Z}\langle S \rangle$ to be the set of maps $\phi : S \to \mathbb{Z}$ such that $\phi(x) \neq 0$ for finitely many $x \in S$. This is called the* ***free abelian group generated by S****.*

Definition 1.62. *The* ***rank*** *of a free abelian group is the cardinality of any basis. (This is well-defined.)*

1.9.1 Finitely generated abelian groups

Definition 1.63. *Let G be a group and $a \in G$. The **order** or **period** of a is the smallest integer $n \in \mathbb{N}$ so that $a^n = e$.*

Definition 1.64. *A **torsion** element of a group is an element with finite order.*

Definition 1.65. *The **torsion subgroup** of a group is the subgroup of all torsion elements.*

Definition 1.66. *An abelian group is a **torsion group** if all elements are torsion.*

Definition 1.67. *Let A be an abelian group and p a prime number. Then we denote by $\boldsymbol{A(p)}$ the subgroup of elements of A whose period is a power of p. Then $A(p)$ is a torsion group. If $A(p)$ is finite, then it is a p-group.*

Definition 1.68. *A finite abelian p-group A is **of type** $(p^{r_1}, \ldots, p^{r_n})$ if*

$$A \cong \bigoplus_{i=1}^{n} \mathbb{Z}/p^{r_i}\mathbb{Z}$$

Definition 1.69. *A group is **torsion free** if every element except the identity has infinite period.*

Definition 1.70. *Let A be a finitely generated abelian group. The **rank** of A is the rank of the free subgroup A/A_{tor}.*

1.9.2 Bilinear pairings

Definition 1.71. *Let A, A', B be abelian groups. A **bilinear pairing** is a map $A \times A' \to B$ denoted by $(x, x') \mapsto \langle x, x' \rangle$, such that the maps*

$$x' \mapsto \langle x, x' \rangle \qquad x \mapsto \langle x, x' \rangle$$

are both homomorphisms. That is,

$$\langle x + y, x' \rangle = \langle x, x' \rangle + \langle y, x' \rangle \qquad \langle x, x' + y' \rangle = \langle x, x' \rangle + \langle x, y' \rangle$$

Definition 1.72. *Let $A \times A' \to B$ be a bilinear pairing, and $S' \subset A'$. An element $x \in A$ is **orthogonal** to S' if $\langle x, x' \rangle = 0$ for all $x' \in S'$. (Note that the set of $x \in A$ such that x is orthogonal to S' is a subgroup f A.)*

Definition 1.73. *Let $A \times A' \to B$ be a bilinear pairing. The **left kernel** is the set*

$$\{x \in A : \langle x, x' \rangle = 0,\ \forall x' \in A'\}$$

*(Note that it is a subgroup of A.) Similarly, the **right kernel** is*

$$\{x' \in A' : \langle x, x' \rangle = 0,\ \forall x \in A\}$$

1.9.3 Dual group

Definition 1.74. *Let A be an abelian group. Then we define an action $\mathbb{Z} \times A \to A$ by $nx = x + \ldots + x$ where the RHS is an n-fold sum. Whenever we write nx with $n \in \mathbb{Z}$ we are referring to this action.*

Definition 1.75. *A an abelian group A has **exponent m** for some $m \in \mathbb{Z}$ if $mx = 0$ for every $x \in A$.*

Definition 1.76. *Let A be an abelian group of exponent m. Let $\mathbb{Z}_m$ be the cyclic group of order m. The **dual group** of A is the set $A^\wedge = \mathrm{Hom}(A, \mathbb{Z}_m)$. It is a group under pointwise addition of maps.*

1.10 Inverse limit and completion

Definition 1.77. *Suppose we have a sequence $\{G_n\}_{n \geq 0}$ of groups and a sequence of surjective homomorphisms $f_n : G_n \to G_{n-1}$,*

$$\ldots \xrightarrow{f_3} G_2 \xrightarrow{f_2} G_1 \xrightarrow{f_1} G_0$$

Then for any $x_0 \in G_0$, there is an infinite sequence $x = (x_0, x_1, x_2, \ldots)$ such that $f_n(x_n) = x_{n-1}$. We define multiplication of sequences component-wise, that is,

$$(x_0, x_1, \ldots) \cdot (y_0, y_1, \ldots) = (x_0 y_0, x_1 y_1, \ldots)$$

*This satisfies $f_n(x_n y_n) = f_n(x_n) f_n(y_n) = x_{n-1} y_{n-1}$ because f_n is a homomorphism. This set of sequences is called the **inverse limit** of the family $\{(G_n, f_n)\}$. We denote it by $\varprojlim(G_n, f_n)$. It forms a group under this multiplication.*

Definition 1.78. *Let $G_n = \mathbb{Z}/p^{n+1}\mathbb{Z}$ for $n \geq 0$. Let $f_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ be the canonical homomorphism $x \mapsto x \bmod p^n$. Each f_n is surjective, so we can form the inverse limit $\varprojlim(G_n, f_n)$. This group is called the **p-adic integers** and is denoted by $\mathbb{Z}_p$.*

Definition 1.79. *A **directed set** is a partially ordered set I such that for $i, j \in I$, there exists $k \in I$ such that $i \leq k$ and $j \leq k$.*

Definition 1.80. *Let I be a directed set. A **inversely directed family** of groups is a family $\{G_i\}_{i \in I}$ and for each pair $i \leq j$ there is a homomorphism $f_i^j : G_j \to G_i$ such that for $k \leq i \leq j$ we have $f_k^i \circ f_i^j = f_k^j$ and $f_i^i = \mathrm{id}$.*

Definition 1.81. *Let $\{G_i\}_{i \in I}$ be an inversely directed family of groups. Then let $G = \prod_i G_i$ and Γ be the subset of G consisting of elements (x_i) with $x_i \in G_i$ such that $f_i^j(x_j) = x_i$ for all $j \geq i$. Then Γ is the **inverse limit** of the family. This is denoted by $\Gamma = \varprojlim G_i$. Note that Γ is a subgroup of G. Such a group Γ is called **profinite**.*

2 Categories

Definition 2.1. *A **category** is a collection of objects and a collection of morphisms. The collection of morphisms from an object A to another object B is denoted* $\mathrm{Hom}(A, B)$*. such that for every three objects A, B, C there is a map*

$$\mathrm{Hom}(B, C) \times \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, C)$$

satisfying the following: For each object A there is a unique morphism $\mathrm{Id}_A \in \mathrm{Hom}(A, A)$ which acts as right and left identity for morphisms in $\mathrm{Hom}(A, B)$ *and* $\mathrm{Hom}(B, A)$ *respectively; and the law of composition is associative.*

Definition 2.2. *A morphism $f : A \to B$ in a category is called a **isomorphism** if there is a morphism $g : B \to A$ such that $g \circ f = \mathrm{Id}_A$ and $f \circ g = \mathrm{Id}_B$.*

Definition 2.3. *Let $\mathcal{C}$ be a category. An object P is called **universally attracting** if for every object A there is a unique morphism $f : A \to P$. P is called **universally repelling** if for every object B there is a unique morphism $g : P \to B$.*

Example: The trivial group $\{0\}$ is universally repelling and universally attracting in the category of groups. For any group G, the only morphism $\{0\} \to G$ is the map $0 \mapsto 0$, and the only morphism $G \to \{0\}$ is the map $x \mapsto 0$.

Definition 2.4. *Let $\mathcal{C}$ be a category and A, B objects. A **product** of A and B is a triple (P, f, g) consisting of an object P and two morphisms $f : P \to A$ and $g : P \to B$ such that for any object C and any morphisms $\phi : C \to A$ and $\psi : C \to B$ there is a unique morphism $h : C \to P$ so that $\phi = f \circ h$ and $\psi = g \circ h$.*

3 Rings

Definition 3.1. *A **ring** is a set with two operations, called addition and multiplication. With respect to addition, the set is an abelian group. With respect to multiplication, it is a monoid. It also satisfies distributivity:*

$$(x + y)z = xy + yz \qquad z(x + y) = zx + zy$$

We denote the additive identity by 0 and the multiplicative identity by 1.

Definition 3.2. *A **ring homomorphism** is a map $f : R \to R'$ that preserves addition and multiplication.*

Definition 3.3. *A **subring** is a subset of a ring that is an additive subgroup, contains 1, and is closed under multiplication.*

Definition 3.4. *Let A be a ring. A **unit** is an element with a multiplicative inverse.*

Definition 3.5. *Two elements a and b in a ring are **associates** if $a = bu$ for some unit u.*

Definition 3.6. *A **division ring** is a ring in which all nonzero elements are units.*

Definition 3.7. *The **center** of a ring is the subset of elements that commute with every element (with respect to multiplication.)*

Definition 3.8. *A **commutative ring** is a ring in which multiplication is commutative. That is, the center is the entire ring.*

Definition 3.9. *A **field** is a commutative division ring.*

Definition 3.10. *Let A be a ring. A **zero divisor** is a nonzero element x such that $xy = 0$ for some nonzero $y \in A$.*

Definition 3.11. *A **integral domain** is a ring with no zero divisors.*

Note: A division ring has no zero divisors, but an integral domain need not be a division ring. Example: $\mathbb{Z}$.

Definition 3.12. *Let A be an integral domain. An **irreducible** element is an element a that is not a unit, and whenever $a = bc$ for $b, c \in A$, one of b, c must be a unit. That is, an irreducible element is not the product of two non-units.*

Definition 3.13. *Let A be an integral domain. A is a **unique factorization domain** if every element a can be written as*

$$a = u \prod_{i=1}^{r} p_i$$

where p_i are irreducible and u is a unit, and this factorization of a is unique up to multiplication of each p_i by units. That is, if

$$a = u \prod_{i=1}^{r} p_i = u' \prod_{j=1}^{s} q_j$$

then $r = s$ and up to a permutation of indices, $p_i = u_i q_i$ for units $u_i \in A$.

Definition 3.14. *Let A be an integral domain. We say a **divides** b and write $a|b$ if there exists c such that $ac = b$.*

Definition 3.15. *Let A be an integral domain. For $a, b \in A$, a **g.c.d** of a and b is an element d such that $d|a$, $d|b$, and*

$$x|a \text{ and } x|b \implies x|d$$

Definition 3.16. *In a unique factorization domain, irreducible elements are called **primes**.*

Definition 3.17. *Let A be a unique factorization domain. We impose an equivalence relation on the set of primes so that $p \sim q$ if $p = uq$ for a unit u, the choose one p from each equivalence class, let P be the set of chosen primes. We can then write $a \neq 0$ as*

$$a = u \prod_{p \in P} p^{k(p)}$$

*where $k(p)$ is uniquely determined for each p. $k(p)$ is the **order** of a at p, and is denoted $\operatorname{ord}_p a$.*

Definition 3.18. *Let A be a unique factorization domain. The* ***least common multiple*** *of a and b is $c \in A$ such that $\operatorname{ord}_p c = \max(\operatorname{ord}_p a, \operatorname{ord}_p b)$. Note that in a UFD, such an element always exists and is unique up to multiplication by units.*

Definition 3.19. *Let A be a unique factorization domain. Two elements a and b are* ***relatively prime*** *if $\gcd(a, b)$ is a unit.*

Definition 3.20. *Let A be a ring with unit 1_A. Define a ring homomorphism $\lambda : \mathbb{Z} \to A$ by $\lambda(1) = 1_A$. (We have defined λ on a generating set for $\mathbb{Z}$, so this determines λ.) If λ is injective, then A has* ***characteristic zero.*** *If the kernel is not trivial, then the* ***characteristic*** *of A is the smallest $n \in \mathbb{N}$ so that $n \in \ker \lambda$.*

Definition 3.21. *Let A be a subring of B, and let S be a subset of B commuting with A, that is, $sa = as$ for $a \in A, s \in S$. Define*

$$A[S] = \left\{ \sum a_{i_1} \dots a_{i_n} s_1^{i_1} \dots s_n^{i_n} : a_{i_j} \in A, s_k \in S \right\}$$

If $A[S] = B$, then S is a ***set of generators for B over A****. One should think of $A[S]$ as polynomials with elements of S as variables and elements of A as coefficients, though elements of S may not commute with each other.*

3.1 Interesting examples of rings

Definition 3.22. *Let S be a set and A be a ring. We define* $\mathbf{Map}\,(\boldsymbol{S}, \boldsymbol{A})$ *to be the set of mappings of S into A. We define addition and multiplication in $\operatorname{Map}(S, A)$ pointwise,*

$$(fg)(x) = f(x)g(x) \qquad (f + g)(x) = f(x) + g(x)$$

Definition 3.23. *Let M be an abelian group and let $A = \mathbf{End}\,(\boldsymbol{M})$ be the set of automorphisms of M. We define addition in $\operatorname{End}(M)$ pointwise, and multiplication by composition of functions. Then $\operatorname{End}(M)$ is a ring.*

Definition 3.24. *Let G be a group and K be a field. Denote by $\boldsymbol{K[G]}$ the set of formal linear combinations $\alpha = \sum a_x x$ where $x \in G$ and $a_x \in K$, where only finitely many terms are nonzero. We define a sum in $K[G]$ by*

$$\left(\sum a_x x\right) + \left(\sum b_x x\right) = \sum (a_x + b_x) x$$

We define a product in $K[G]$ by

$$\left(\sum_{x \in G} a_x x\right)\left(\sum_{y \in G} b_y y\right) = \sum_{x \in G} \sum_{y \in G} a_x b_y xy = \sum_{z \in G} \left(\sum_{xy = z} a_x b_y\right) z$$

The set $K[G]$ is called a ***group ring****. (Note that it is a ring under this addition and multiplication.)*

3.2 Ideals

Definition 3.25. *Let S be a subset of a ring R. We define*

$$\boldsymbol{SR} = \{sr : s \in S, r \in R\}$$

Definition 3.26. *A **left ideal** of a ring A is a subset $\mathfrak{a}$ such that $\mathfrak{a}A = \mathfrak{a}$.*

Definition 3.27. *A **two-sided ideal** of a ring A is a subset $\mathfrak{a}$ such that $\mathfrak{a}A\mathfrak{a} = \mathfrak{a}$.*

Definition 3.28. *Let A be a ring. For $a_1, \ldots, a_n \in A$, the **ideal generated** by $a_1, \ldots, a_n$ is the set*

$$\left\{\sum x_i a_i : x_i \in A\right\}$$

Definition 3.29. *Let A be a ring. An ideal is **principal** if it is generated by a single element.*

Definition 3.30. *A **principal ideal domain** is a ring in which every ideal is principal.*

Definition 3.31. *A commutative ring is **Noetherian** if every ideal is finitely generated.*

Definition 3.32. *Let A be a ring and $\mathfrak{a}, \mathfrak{b}$ be ideals. The **product of ideals** is*

$$\mathfrak{a}\mathfrak{b} = \left\{\sum a_i b_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\right\}$$

Note that $\mathfrak{a}\mathfrak{b}$ is an ideal.

Definition 3.33. *Let A be a ring and $\mathfrak{a}, \mathfrak{b}$ be ideals. The **sum of ideals** is*

$$\mathfrak{a} + \mathfrak{b} = \{a_i + b_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$$

Note that $\mathfrak{a} + \mathfrak{b}$ is an ideal.

Definition 3.34. *Let A be a ring and $\mathfrak{a}$ an ideal. The **quotient ring** or **factor ring**, denoted $A/\mathfrak{a}$, is the quotient group $A/\mathfrak{a}$. We define multiplication on it by*

$$(x + \mathfrak{a})(y + \mathfrak{a}) = xy + \mathfrak{a}$$

Then $A/\mathfrak{a}$ is a ring.

Definition 3.35. *Let A be a ring and $\mathfrak{a}$ an ideal. For $x, y \in A$, we say*

$$\boldsymbol{x \equiv y \pmod{\mathfrak{a}}}$$

if $x - y \in \mathfrak{a}$. If $\mathfrak{a} = (a)$, then we write

$$x \equiv y \pmod{a}$$

to mean the same thing. If $f : A \to A/\mathfrak{a}$ is the canonical homomorphism $a \mapsto a + \mathfrak{a}$, then

$$x \equiv y \pmod{\mathfrak{a}} \iff f(x) = f(y)$$

Definition 3.36. *Let A be a ring and $\mathfrak{a}$ an ideal. The* ***residue class ring*** *of $\mathfrak{a}$ is just another name for $A/\mathfrak{a}$.*

Definition 3.37. *Let A be a ring and $\mathfrak{a}$ an ideal. The* ***residue classes modulo $\mathfrak{a}$*** *are the cosets of $\mathfrak{a}$.*

Definition 3.38. *Let A be a ring and $\mathfrak{a}$ an ideal. The* ***residue class of x modulo $\mathfrak{a}$*** *is just the coset $x + \mathfrak{a}$.*

Definition 3.39. *A* ***prime ideal*** *is an ideal $\mathfrak{p}$ such that*

$$xy \in \mathfrak{p} \implies x \in \mathfrak{p} \text{ or } y \in \mathfrak{p}$$

Equivantly, $\mathfrak{p}$ is prime if $A/\mathfrak{p}$ is an integral domain.

Definition 3.40. *An ideal is* ***maximal*** *if it is a proper ideal and any ideal containing it is the whole ring.*

3.3 Localization

Definition 3.41. *A* ***multiplicative subset*** *of a ring is a subset containing 1 and closed under multiplication.*

Definition 3.42. *Let A be a commutative ring and S a multiplicative subset. The* ***localization*** *of A at S is the set of elements*

$$S^{-1}A = \left\{ \frac{a}{s} : a \in A, s \in S \right\}$$

modulo an equivalence relation. We say $\frac{a}{s} \sim \frac{a'}{s'}$ if there exists $t \in S$ so that $t(as' + s'a) = 0$. We define multiplication and addition in $S^{-1}A$ by analogy with addition and multiplication in $\mathbb{Q}$.

Definition 3.43. *Let A be an integral domain and let $S = A^*$. The* ***field of fractions*** *of A is the localization $S^{-1}A$.*

Definition 3.44. *A* ***local ring*** *is a commutative ring that has a unique maximal ideal.*

Definition 3.45. *Let A be a commutative ring and $\mathfrak{p}$ a prime ideal. Let $S = A \setminus \mathfrak{p}$. We denote $S^{-1}A$ by $A_{\mathfrak{p}}$.*

Definition 3.46. *Let A be a commutative ring and S a multiplicative subset. Let $J(A)$ be the set of ideals of A. Then $\psi_S : J(A) \to J(S^{-1}A)$ given by $\psi_S(\mathfrak{a}) = S^{-1}\mathfrak{a}$ is the* ***ideal correspondence*** *map. Note that ψ_S preserves addition, multiplication, intersection, and inclusion of ideals.*

3.4 Polynomials

Definition 3.47. *Let A be a subring of a commutative ring B and let $b \in B$. For $f = a_0 + a_1x + \ldots + a_nx^n \in A[x]$, the* ***associated polynomial function*** *is $f_B : B \to B$ by*

$$f_B(b) = a_0 + a_1b + \ldots + a_nb^n$$

Definition 3.48. *Let A be a subring of a commutative ring B. Fix $b \in B$. The* ***evaluation map*** $\mathrm{ev}_b : A[x] \to B$ *given by*

$$f \mapsto f(b)$$

Note that ev_b *is a ring homomorphism.*

Definition 3.49. *Let A be a subring of a commutative ring B and fix $b \in B$. We say that b is* ***transcendental*** *over A if the evaluation map* ev_b *is injective.*

Definition 3.50. *Let $\phi : A \to B$ be a homomorphism of commutative rings. The* ***reduction map*** *is the map $A[x] \to B[x]$ given by*

$$\sum_{i=0}^{n} a_ix^i \mapsto \sum_{i=1}^{n} \phi(a_i)x^i$$

Note that this is a ring homomorphism.

Definition 3.51. *Let k be a field. A polynomial $f \in k[x]$ is* ***irreducible*** *if it has degree greater than or equal to 1 and if whenever $f = gh$ with $g, h \in k[x]$, then one of g, h is a constant polynomial*

Definition 3.52. *Let A be a commutative ring and $f \in A[x]$. A* ***root*** *of f is an element $a \in A$ such that $f(a) = 0$.*

Definition 3.53. *Let A be a unique factorization domain. For a nonzero $a \in A$, and a prime element $p \in A$, we can write $a = p^rb$ for some $r \geq 0$, where p does not divide b. Then r is the* ***order of a at p****.*

Definition 3.54. *Let k be a field and $f \in k[x]$. The* ***content*** *of f is the* gcd *of the coefficients. A polynomial with content 1 is a* ***primitive*** *polynomial.*

4 Modules over rings

Definition 4.1. *Let A be a commutative ring. A* ***module*** *over A, also called an A-module, is an abelian group M, with a map $A \times M \to M$ satisfying*

$$(a + b)x = ax + bx \qquad a(x + y) = ax + ay$$

for $a, b \in A$ and $x, y \in M$.

Definition 4.2. *Let M be an A-module. A* ***submodule*** *is a subgroup $N \subset M$ such that $a \in A, x \in N \implies ax \in N$.*

Definition 4.3. *Let M be a A-module. If A is a field, then M is called a* ***vector space****.*

Definition 4.4. *Let A be an integral domain and M an A-module. The* ***torsion submodule*** *is the set of elements $x \in M$ such that there exists $a \in A, a \neq 0$ such that $ax = 0$.*

Definition 4.5. *Let M be an A-module and let $\mathfrak{a}$ be an ideal of A. We define $\mathfrak{a}M$ to be*

$$\mathfrak{a}M = \left\{ \sum a_i x_i : a_i \in \mathfrak{a}, x_i \in M \right\}$$

Note that $\mathfrak{a}(\mathfrak{b}M) = (\mathfrak{a}\mathfrak{b})M$ and $(\mathfrak{a} + \mathfrak{b})M = \mathfrak{a}M + \mathfrak{b}M$.

Definition 4.6. *Let M be an A-module and N a submodule. The* ***quotient module*** *M/N is M/N viewed as a quotient of abelian groups with an obvious A-module structure.*

$$A \times M/N \to M/N \qquad (a, x + N) \mapsto ax + N$$

Definition 4.7. *Let M, M' be A-modules. A* ***A-module homomorphism****, also called an A-linear map, is a map $f : M \to M'$ such that f is an abelian group homomorphism and f preserves the action of A, that is,*

$$a \cdot f(x) = f(a \cdot x)$$

for $a \in A$ and $x \in M$.

Definition 4.8. *Let $f : M \to M'$ be an A-module homomorphism. The* ***cokernel*** *of f is the quotient module $M'/\operatorname{im} f$.*

Definition 4.9. *Let M be an A-module. Then M is* ***cyclic*** *if there exists $x \in M$ such that $M = \{ax : a \in A\}$.*

4.1 Homomorphism group and hom functor

Definition 4.10. *Let A be a ring and X, X' be A-modules. We define* $\mathbf{Hom_A(X, X')}$ *to be the set of A-module homomorphisms from X to X'. It is a group under pointwise addition of maps. We define an action $A \times \operatorname{Hom}_A(X, X') \to \operatorname{Hom}_A(X, X')$ by*

$$(a \cdot \phi)(x) = a \cdot (\phi(x))$$

for $a \in A, \phi \in \operatorname{Hom}_A(X, X')$, and $x \in X$. This makes $\operatorname{Hom}_A(X, X')$ an A-module.

Definition 4.11. *Let A be a ring and Y an A-module. We define the functor* $\mathbf{Hom_A(Y, -)}$ *from the category of A-modules to itself by sending an A-module X to the A-module $\operatorname{Hom}_A(Y, X)$ and sending $f \in \operatorname{Hom}_A(X, X')$ to*

$$\begin{aligned} \operatorname{Hom}_A(Y, f) : \operatorname{Hom}_A(Y, X) &\to \operatorname{Hom}_A(Y, X') \\ \phi &\mapsto f \circ \phi \end{aligned}$$

The identity is preserved, because $\mathrm{Hom}_A(Y, \mathrm{Id}_X)$ *is given by* $\phi \mapsto \mathrm{Id} \circ \phi = \phi$*. It also preserves composition: let* $f \in \mathrm{Hom}_A(X, X')$ *and* $g \in \mathrm{Hom}_A(X', X'')$*. Then for* $\phi \in \mathrm{Hom}_A(Y, X)$*,*

$$\begin{aligned} \mathrm{Hom}_A(Y, g \circ f)(\phi) &= (g \circ f) \circ \phi = g \circ (f \circ \phi) = g \circ \mathrm{Hom}_A(Y, f)(\phi) \\ &= \mathrm{Hom}_A(Y, g) \circ \mathrm{Hom}_A(Y, f)(\phi) \\ \implies \mathrm{Hom}_A(Y, g \circ f) &= \mathrm{Hom}_A(Y, g) \circ \mathrm{Hom}_A(Y, f) \end{aligned}$$

so it is covariant.

Definition 4.12. *Let* A *be a ring and* Y *an* A*-module. We define the functor* $\mathbf{Hom_A(-, Y)}$ *from the category of* A*-modules to itself by sending an* A*-module* X *to the* A*-module* $\mathrm{Hom}_A(X, Y)$ *and sending* $f \in \mathrm{Hom}_A(X, X')$ *to*

$$\begin{aligned} \mathrm{Hom}_A(f, Y) : \mathrm{Hom}_A(X', Y) &\to \mathrm{Hom}_A(X, Y) \\ \phi &\mapsto \phi \circ f \end{aligned}$$

The identity is preserved, because $\mathrm{Hom}_A(\mathrm{Id}_X, Y)$ *is given by* $\phi \mapsto \phi \circ \mathrm{Id}_X = \phi$*. Unlike the above, this is a contravariant functor: let* $f \in \mathrm{Hom}_A(X, X')$ *and* $g \in \mathrm{Hom}_A(X', X'')$*. Then for* $\phi \in \mathrm{Hom}_A(X'', Y)$*,*

$$\begin{aligned} \mathrm{Hom}_A(Y, g \circ f)(\phi) &= \phi \circ (g \circ f) = (\phi \circ g) \circ f = \mathrm{Hom}_A(g, Y)(\phi) \circ f \\ &= \mathrm{Hom}_A(f, Y) \circ \mathrm{Hom}_A(g, Y)(\phi) \\ \implies \mathrm{Hom}_A(Y, g \circ f) &= \mathrm{Hom}_A(f, Y) \circ \mathrm{Hom}_A(g, Y) \end{aligned}$$

so it is contravariant.

Definition 4.13. *Let* A *be a ring and let*

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

be an exact sequence of A*-modules. Let* Y *be an* A*-module. The* ***induced sequence*** *is*

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

Definition 4.14. *Let* $\mathrm{Mod}(A)$ *and* $\mathrm{Mod}(B)$ *be the categories of* $A-$ *and* $B-$*modules respectively and let* $F : \mathrm{Mod}(A) \to \mathrm{Mod}(B)$ *be a functor.* F *is* ***exact*** *if for every exact sequence*

$$\ldots \xrightarrow{f} X \xrightarrow{f'} X' \xrightarrow{f''} X'' \xrightarrow{f'''} \ldots$$

the induced sequence

$$\ldots \xrightarrow{F(f)} F(X) \xrightarrow{F(f')} F(X') \xrightarrow{F(f'')} F(X'') \xrightarrow{F(f''')} \ldots$$

is exact.

Definition 4.15. *Let* M *be an* A*-module. The* ***endomorphism ring****, denoted* $\mathbf{End_A(M)}$*, is the group* $\mathrm{Hom}_A(M, M)$ *with multiplication defined by function composition. WARNING:* $\mathrm{End}_A(M)$ *and* $\mathrm{Hom}_A(M, M)$ *have very different module structures!*

4.2 Free modules

Definition 4.16. *Let M be an A-module and $S \subset M$. A **linear combination** of elements of S is a sum $\sum_{x \in S} a_x x$ where $a_x \in A$, and only finitely many a_x are nonzero. The elements a_x are the **coefficients** of the linear combination.*

Definition 4.17. *Let M be an A-module and $S \subset M$. The **submodule generated by S** is the set of linear combinations of S,*

$$N = \left\{ \sum_{x \in S} a_x x : a_x \in A, x \in S \right\}$$

*where only finitely many a_x are nonzero. This is denoted $\boldsymbol{N = A\langle S \rangle}$. If S is a single element set, this is called a **principal module**.*

Definition 4.18. *Let M be an A-module and $S \subset M$. S is **linearly independent** if*

$$\sum_{x \in S} a_x x = 0 \implies \forall x, a_x = 0$$

Definition 4.19. *Let M be an A-module and $S \subset M$. S is a **basis** of M if it is not empty, if it generates M, and it is linearly independent. (As a consequence of this, every element of M has a unique expresssion as a linear combination of elements of S.)*

Definition 4.20. *A **free module** is a module that admits a basis.*

4.3 Chain complexes

Definition 4.21. *Let A be a ring. An **chain complex** of A-modules is a sequence E^i of A-modules and a sequence $d^i : E^i \to E^{i+1}$ of A-module homomorphisms for $i \in \mathbb{Z}$ such that $d^i \circ d^{i-1} = 0$ for all i. Diagrammatically,*

$$\ldots \xrightarrow{d^{i-2}} E^{i-1} \xrightarrow{d^{i-1}} E^i \xrightarrow{d^i} E^{i+1} \xrightarrow{d^{i+1}} \ldots$$

*(Note: The sequence need not be exact.) The maps d^i are called **differentials**.*

Definition 4.22. *A chain complex is **bounded above** if $E^i = 0$ for all $i > N$ for some N. It is **bounded below** if $E^i = 0$ for all $i < M$ for some M. A chain complex is **bounded** or **finite** if it is bounded above and below.*

Definition 4.23. *Let (E^i, d^i) be a chain complex. The ith **homology** of the complex is the quotient module $(\ker d^i)/(\operatorname{im} d^{i-1})$.*

Definition 4.24. *Let M be a module. A **resolution** of M is an exact sequence*

$$\ldots \longrightarrow E_n \longrightarrow E_{n-1} \longrightarrow \ldots \longrightarrow E_0 \longrightarrow M \longrightarrow 0$$

or one of the form

$$0 \longrightarrow M \longrightarrow E_0 \longrightarrow \ldots \longrightarrow E_n \longrightarrow E_{n+1} \longrightarrow \ldots$$

Definition 4.25. *A resolution is **free** if each E_i is free. A resolution is **projective** if each E_i is projective.*

Definition 4.26. *Let S be a set. For $i = 0, 1, 2 \ldots$ let E_i be the free module over $\mathbb{Z}$ generated by $(i+1)$ tuples $(x_0, \ldots, x_i)$ where $x_j \in S$. Then define $d_{i+1} : E_{i+1} \to E_i$ by defining it on the generators as*

$$d_{i+1}(x_0, \ldots, x_{i+1}) = \sum_{j=0}^{i+1} (-1)^j (x_0, \ldots, \widehat{x}_j, x_{i+1})$$

*For $i = 0$, let $d_0 : E_0 \to \mathbb{Z}$ be the map defined by $d_0(x_0) = 1$. The **standard complex** of S is the following resolution of $\mathbb{Z}$:*

$$\ldots \xrightarrow{d_{i+2}} E_{i+1} \xrightarrow{d_{i+1}} E_i \xrightarrow{d_i} \ldots \xrightarrow{d_1} E_0 \xrightarrow{d_0} \mathbb{Z} \longrightarrow 0$$