

Abstract Algebra– Terms for Qualifying Examination

Elisha Peterson

November 6, 2003

1 Linear Algebra

Basis: given some subspace, it is a smallest set of elements which generate that subspace; its size is unique, called the dimension of the subspace.

Rank: given a matrix M , it is the dimension of $\text{im } M$.

Null Space: the subspace K with $M(K) = 0$; the rank of a matrix plus the dimension of the null space equals the dimension of the overall space.

Similar Matrices: matrices A, B for which there exists an invertible matrix P with $A = PBP^{-1}$; basically means they're the same up to a change of basis.

Trace: the sum of diagonal elements of a matrix.

Determinant:

Eigenvalue: a value λ such that $Ax = \lambda x$ for some x , which is called an **Eigenvector**.

2 Groups

2.1 Basics

Group: a set G with associativity ($a(bc) = (ab)c$), an identity ($\exists e \in G$ s.t. $ae = ea = a$), and an inverse a^{-1} for all elements s.t. $aa^{-1} = a^{-1}a = e$.

Abelian group: a group which is also commutative ($ab = ba$).

Index $[G : H]$: the number of cosets of H in G , equal to $|G|/|H|$ by **Lagrange's Theorem**.

Normal Subgroup: a subgroup $K \leq G$ with $gkg^{-1} \in K$ for all $g \in G, k \in K$, denoted by $K \triangleleft G$.

Quotient Group: the group of cosets of a *normal* subgroup K , denoted G/K . By Lagrange's Theorem, the order of a quotient group is $|G/K| = |G|/|K|$.

Cyclic Group: a group which is generated by a single element, and therefore isomorphic to either the finite \mathbb{Z}_m (integers modulo m) or the integers \mathbb{Z} .

Symmetric Group S_n : the group formed from the set of all permutations of the letters $\{1, 2, \dots, n\}$. The even permutations form the **Alternating Group A_n** .

Cayley's Theorem: every group is isomorphic to a subgroup of a symmetric group; this is either S_n where $|G| = n$ or S_G (the permutations on elements of G) if the order is infinite. This result is most useful in the classification of groups.

First Isomorphism Theorem: for a homomorphism $f : G \rightarrow H$, the kernel $\ker f$ is a normal subgroup, and $G/\ker f \cong \text{im } f$. Alternately, if $K = \ker f$ and $\pi : G \rightarrow G/K$ is the natural map, then there exists an isomorphism ϕ with $f = \phi \circ \pi$. The next two results are consequences of this theorem.

Second Isomorphism Theorem: if H, K are subgroups of G with $H \triangleleft G$ normal, then the set of products HK is a group, $H \cap K$ is a normal subgroup of K , and $K/(H \cap K) \cong HK/H$.

Third Isomorphism Theorem: if H, K are normal subgroups with $K \leq H$, then $H/K \triangleleft G/K$ and $(G/K)/(H/K) \cong G/H$ (allowing us to ‘cancel factors’).

2.2 Examples

Dihedral Group D_n : the group of symmetries of an n -polygon, consisting of n rotations and n reflections.

Group of Units $U(n)$: the set of elements of \mathbb{Z}_n which are relatively prime to n ; forms a group under multiplication.

Matrix Group: matrices $GL(n, \mathbb{R})$ and $GL(n, \mathbb{C})$ with nonzero determinant and entries in \mathbb{R} or \mathbb{C} form a group; with extra conditions, $GL(n, R)$ for a general ring may also form a group.

Automorphism Group $\text{Aut}(G)$: automorphisms of G .

Inner Automorphism Group $\text{Inn}(G)$: the automorphisms of the form $\phi_a(x) = axa^{-1}$, also forming a group.

2.3 Solvability

Normal series: a sequence of groups $H_0 \subset H_1 \subset \dots \subset H_k$ with $H_i \triangleleft H_{i+1}$ for all i .

Composition series: a normal series with all nontrivial factor groups simple (called **composition factors**).

Jordan-Holder theorem: Any two composition series of a group are equivalent; thus, the length is an invariant of the group.

Solvable group: there is a normal series $\{e\} = H_0 \subset H_1 \subset \dots \subset H_k = G$ with factor groups H_{i+1}/H_i abelian for all i .

Simple group: a group with no nontrivial normal subgroups.

Solvability of S^n : for $n \geq 5$, the symmetric group S^n is nonsimple. Since it is also nonabelian, it is not solvable.

2.4 Special Groups/Subgroups

Cyclic Subgroup $\langle a \rangle$: given $a \in G$, the elements $\langle a \rangle = \{1, a, a^2, \dots\}$.

Center $Z(G)$: the elements which commute with all others; it is normal and $G/Z(G) \cong \text{Inn}(G)$.

G/Z Theorem: states that $Z(G)$ is cyclic (trivial) iff G is abelian.

Centralizer $C(a)$: given $a \in G$, the elements $C(a) = \{g \in G : ga = ag\}$; also defined for subgroups.

Normalizer $N(H)$: given $H < G$, the elements $x \in G$ with $xHx^{-1} \in H$.

N/C Theorem: $N(H)/C(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$.

Stabilizer $\text{stab}(a)$: given $a \in G$ and a permutation group (or group action), the permutations of G which fix a .

Orbit $\text{orb}(a)$: given $a \in G$, the elements $\phi(a)$ for ϕ in a given permutation group (or group action).

Orbit-Stabilizer Theorem: $|G| = |\text{orb}(a)| \cdot |\text{stab}(a)|$.

2.5 Group actions/Sylow Theory

Group action: a group G acts on a set X if there is a function $G \times X \rightarrow X$ with $(g, x) \mapsto gx$, such that $(gh)x = g(hx)$ and $1x = x$.

Left/Right/Conjugation Actions: an element $g \in G$ provides a left action $x \mapsto gx$, a right action $x \mapsto xg$, and a conjugation action $x \mapsto gxg^{-1}$ on the group G .

Conjugacy class: given $a \in G$, it is the elements $\text{cl}(a) = \{gag^{-1} : g \in G\}$. Its size is $|\text{cl}(a)| = |G : C(a)|$.

Class Formula: $|G| = \sum |G : C(a)|$, the sum taken over conjugacy classes. Alternately, $|G| = |Z(G)| + \sum |G : C(a)|$.

Sylow's First Theorem: if p^k divides $|G|$, then G has a subgroup of order p^k ; the maximal such subgroup is the **Sylow p -subgroup**.

Sylow's Second Theorem: every subgroup $H < G$ with $|H| = p^k$ is contained in some Sylow p -subgroup.

Sylow's Third Theorem: any two Sylow p -subgroups are conjugate; the number n_p of such is $\equiv_p 1$ and also divides $|G|$. The subgroup is unique iff it is normal.

Solvability of p -groups: every finite p -group is solvable, since it has a nontrivial center.

2.6 Free Groups

Free group: a group generated by a set of symbols S consisting of formal finite sequences (called words) of elements in S and their inverses.

Universal mapping property: Every group is a homomorphic image of a free group.

Existence of generators/relations in category of groups: every group is a factor group of a free group, hence is definable by a set of generators and relations.

Free abelian group: given generators x_i , it is the group $\langle x_1 \rangle \oplus \cdots \oplus \langle x_k \rangle$.

Torsion subgroup: the subgroup of an abelian group consisting of all finite-order elements.

Internal direct sums in abelian groups: a group G may be written $G = H \times K$ if $G = HK$ for (normal) subgroups H, K and $H \cap K = \{e\}$. In this case, $H \oplus K \cong H \times K$, so the internal product is isomorphic to the external product.

Primary decomposition of abelian torsion groups: a free abelian group has torsion subgroup isomorphic to $\mathbb{Z}_{p_1}^{n_1} \oplus \cdots \oplus \mathbb{Z}_{p_k}^{n_k}$ where the primes p_i and coefficients n_i are unique up to reordering. The remainder of the group will then be $\mathbb{Z}^{n_{k+1}}$.

3 Categories

Category: consists of a set of **objects**, a set of **morphisms** $\text{Hom}(A, B)$ between every ordered pair (A, B) of objects, and a **composition** $\text{Hom}(A, B) \times \text{Hom}(B, C) \rightarrow \text{Hom}(A, C)$ for every triple of objects which is associative. Moreover, the $\text{Hom}(A, B)$ sets are disjoint and there exists an **identity morphism** $1_A \in \text{Hom}(A, A)$.

Examples of categories: Sets with functions, groups with homomorphisms, commutative rings with ring homomorphisms, etc. are all categories.

Equivalence morphism: a morphism $f : A \rightarrow B$ such that there exists a morphism $g \in \text{Hom}(B, A)$ with $gf = 1_A$ and $fg = 1_B$; essentially an isomorphism.

Functor: a functor is a map T between objects and maps in two categories which (i) takes objects to objects; (ii) takes maps to maps; (iii) preserves composition of maps; (iv) preserves the identity morphism.

The Hom functor: given an object A in a category \mathcal{C} , it is the functor $T_A : \mathcal{C} \rightarrow \mathcal{S}$ to the category \mathcal{S} of sets with $B \mapsto \text{Hom}(A, B)$ and the map $f \in \text{Hom}(B, B')$ taken to the map $\text{Hom}(A, B) \rightarrow \text{Hom}(A, B')$ with $h \mapsto fh$.

Coproducts (direct sums): also called the **free product** and denoted by $A_1 \sqcup A_2$ or $A_1 \oplus A_2$; formally, one has **injection morphisms** $\alpha_i : A_i \rightarrow A_1 \sqcup A_2$ such that for every object X and morphisms $f_i \in \text{Hom}(A_i, X)$, there exists a unique morphism $\theta : A_1 \sqcup A_2 \rightarrow X$ such that $\theta\alpha_i = f_i$.

Products: formally, it is the object $P = A_1 \sqcap A_2$ together with morphisms $p_i \in \text{Hom}(P, A_i)$ such that for every object X and morphisms $f_i : X \rightarrow A_i$, there exists a unique morphism $\theta : X \rightarrow P$ such that $p_i\theta = f_i$; different just in that the ‘arrows are reversed’; often coincides with the coproduct.

4 Rings

4.1 Basics

Ring: a set R with two operations with $(R, +)$ an abelian group, associative under \cdot , and distributive $(a(b + c) = ab + ac)$. The additive identity is denoted 0.

Commutative Ring: a ring R with \cdot commutative.

Ring with unity: a ring R with multiplicative identity 1.

Field: a ring R with (R^*, \cdot) also an abelian group.

Left Ideal: a subring $A \subset R$ with $ar \in A$ for all $a \in A, r \in R$. A **right ideal** is similarly defined.

(2-Sided) Ideal: a subring $A \subset R$ which is both a left and right ideal.

Quotient Ring: the set of cosets of an ideal $A \subset R$, denoted R/A .

Isomorphism Theorems: completely analogous to those for groups.

4.2 Examples

Matrix Ring: given a ring R , one can form a ring of matrices $M_n(R)$ consisting of $n \times n$ matrices with entries in R , using matrix addition and multiplication.

Group Ring: also called a **Group Algebra** and denoted kG , where k is a ring and G a group; it is the set of formal sums $\sum_{g_i \in G} \alpha_i g_i$ with $\alpha_i \in k$, multiplication given by $\alpha_i g_i \cdot \alpha_j g_j = \alpha_i \alpha_j g_i g_j$, and the obvious addition. Thus, it is essentially a vector space over k with G as basis, equipped with a multiplication.

Real Quaternions:

4.3 Integral Domains

Zero Divisors: nontrivial elements $a, b \in R$ with $ab = 0$.

Integral Domain: a commutative ring with unity and no zero divisors; equivalently, with a cancellation law $ab = ac \implies b = c$.

Prime Ideal: an ideal $A \subset R$ with $ab \in A$ implying either $a \in A$ or $b \in A$. In this case, R/A is an integral domain.

Maximal Ideal: an ideal $A \subset R$ contained in no other nontrivial ideal of R . In this case, R/A is a field.

Zorn's Lemma: equivalent to the axiom of choice; states that every nonempty partially ordered set in which every chain has an upper bound has a maximal element.

Chinese Remainder Theorem: for rings, states that if I_1, \dots, I_n are pairwise coprime ideals, and $a_1, \dots, a_n \in R$, then there exists a single $r \in R$ such that $r + I_i = a_i + I_i$ for all i .

4.4 Factorization

Principal Ideal: an ideal $A \subset R$ of the form $\langle a \rangle = \{ra : r \in D\}$ for some $a \in R$; thus, the smallest subring containing a .

Principal Ideal Domain (PID): a ring where every ideal is principal.

Prime Element: an element $a \in D$ of an integral domain with $a|bc$ implies either $a|b$ or $a|c$.

Irreducible Element: an element $a \in D$ with $a = bc$ implies either b or c is a unit.

Unique Factorization Domain (UFD): a ring where unique factorization into irreducibles (up to units) holds. Every PID is a UFD.

Euclidean Ring/Domain (ED): an integral domain with a division algorithm; there is some function $d : D^* \rightarrow \mathbb{Z}_0^+$ such that $d(a) \leq d(ab)$, $b \neq 0$ implies there are $q, r \in D$ such that $a = bq + r$ and $d(r) < d(b)$. Every ED is a PID.

Polynomial Ring: given a ring R , it is the formal set $R[x]$ consisting of $a_0 + a_1x + \dots + a_nx^n$ with $a_i \in R$. If R is an integral domain, so is $R[x]$; if R is a field, $R[x]$ is a PID; if R is a UFD, so is $R[x]$.

4.5 Artinian/Noetherian Rings

Simple Ring: a ring with no nontrivial (2-sided) ideals.

Semisimple Ring: a ring which is a direct sum of minimal ideals.

Division Ring (Skew Field): a ring with every nonzero element having an inverse, but not necessarily commutative; the matrix ring $\text{Mat}_n(\Delta)$ over a division ring Δ is a simple ring.

Artinian Ring: a ring where every descending chain of ideals $I_1 \supset I_2 \supset \dots$ stops.

Noetherian Ring: a ring where every ascending chain of ideals $I_1 \subset I_2 \subset \dots$ stops; more simply, every ideal is finitely generated.

Wedderburn's Theorem for Simple Artinian Rings: a simple artinian ring is isomorphic to $\text{Mat}_n(\Delta)$ for some division ring Δ .

Hilbert Basis Theorem: if R is a commutative noetherian ring, then so is $R[x]$.

4.6 Localization

Multiplicative Set: a subset of a ring including the unity and closed under multiplication.

Fraction Field (Field of Quotients): given an integral domain D , it is the set of pairs (or quotients) of elements of D modulo an appropriate equivalence relation; like constructing the rationals from the integers.

Quotient Field:

Local Rings: rings with a unique maximal ideal; the other elements are precisely the units of the ring.

5 Modules

5.1 Basics

Module: given a ring R , an R -module is an abelian group M with scalar multiplication $R \times M \rightarrow M$ satisfying the expected laws (similar to those for vector fields).

Examples: vector spaces over a field F are F -modules; abelian groups are \mathbb{Z} -modules (looking at the exponents); a commutative ring R is an S -module for any subring $S \subset R$, including itself.

Exact Sequence: a sequence $\cdots \rightarrow M_{n+1} \rightarrow M_n \rightarrow M_{n-1} \rightarrow \cdots$ of R -modules and R -maps $f_i : M_i \rightarrow M_{i-1}$ with $\text{im } f_{i+1} = \text{ker } f_i$ for all i .

Exactness Properties of Hom:

Modules over Matrix Rings: one can form a module over a matrix ring $M_n(R)$ as the set of n -tuples of elements of R , using standard matrix multiplication.

Modules over Group Rings: one can form a module over a group ring kG just as for any other ring.

5.2 Free/Generated Modules

Free Module: an R -module M which is isomorphic to a direct sum of copies of R ; every R -module is a quotient of a free R -module.

Invariance of Rank: for a commutative ring R , every free R -module has the same rank, the same number of elements in any basis; not true for non-commutative rings.

Presentation of a Module: every R -module is a quotient of a free R -module; this provides the basis (generators) for a presentation, with the relations given by the factor submodule.

Finitely Generated Module over a PID: when R is a PID, a finitely generated R -module M is a direct sum $M = tM \oplus F$, where F is a free module.

Applications: this implies primary decomposition theorems for both abelian groups and torsion R -modules.

Applications to Canonical Forms of Matrices and Abelian Groups:

5.3 Tensor Products

Tensor Product: formally, given R -modules A, B , it is the space $A \otimes_R B$ and a map $A \times B \rightarrow_f A \otimes_R B$ such that for all bilinear maps $A \times B \rightarrow_g G$ into an abelian group G , there exists a map $h : A \otimes_R B \rightarrow G$ which commutes with the previous two; informally, it is the unique space such that all maps into and out of it are linear.

Localization:

Algebras and Base Change:

Exactness Properties of Tensor Products:

Exterior Algebra:

5.4 Projective/Injective Modules

Projective Module: a module P for which every short exact sequence $0 \rightarrow A \rightarrow^i B \rightarrow^p P \rightarrow 0$ is split; equivalently, given a surjection $A \rightarrow B$ and a map $P \rightarrow B$, there exists a pullback map $P \rightarrow A$ commuting with the other two.

Injective Module: a module E for which every short exact sequence $0 \rightarrow E \rightarrow^i A \rightarrow^p B \rightarrow 0$ is split; equivalently, given an injection $A \rightarrow B$ and a map $E \rightarrow A$, there exists a map $E \rightarrow B$ which commutes.

Homology:

The Snake Lemma:

Facts on derived functors including Tor and Ext:

6 Field Theory

Field: a set R with $(R, +)$ and (R^*, \cdot) both abelian groups.

6.1 Field extensions

Field Extension: a field $E \supset F$ containing F .

Algebraic Element (Extension): an element $a \in E \supset F$ of an extension field which is the zero of a polynomial in $F[x]$ (an extension with every element algebraic).

Transcendental Element/Extension: an element (extension) which is not algebraic.

Characteristic: the additive order of the unity 1 in a field, or 0 if the order is infinite.

Finite Field: must have order p^n , denoted $GF(p^n)$, with $(GF(p^n)^*, \cdot)$ cyclic and $(GF(p^n), +)$ isomorphic to $\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$.

Algebraic Closure: the smallest extension field of F containing all algebraic elements over F , so every polynomial splits.

Transcendence Basis: given a field extension $E \supset F$, it is a maximal algebraically independent subset $B \subset E$, with **transcendence degree** defined to be $|B|$, basically the number of elements which must be adjoined to F to obtain E .

6.2 Splitting fields/normal extensions

Splitting Field: an extension field $E \supset F$ which contains all the zeros of a specified polynomial $p(x)$.

Normal Extension: an extension which is the splitting field of some set of polynomials.

Extension of Isomorphisms:

Separable Polynomial: a polynomial with no repeated roots.

Separable Extension: an extension with every element separable, meaning either transcendental or with minimal polynomial separable.

6.3 Galois Theory

Galois Extension: an extension $E \supset F$ which is the splitting field of a polynomial in $F[x]$; a separable extension.

Galois Group: the group $\text{Gal}(E/F)$ of automorphisms of E which fix F ; isomorphic to a subgroup of S^n where n is the degree of the polynomial with splitting field E (since its elements must permute the roots of the polynomial).

Galois Correspondence: given a Galois extension $E \supset F$, there is a 1 : 1 correspondence between intermediate fields K ($E \supset K \supset F$) and subgroups of $\text{Gal}(E/F)$, given by the map $K \mapsto \text{Gal}(E/K)$.

Cyclic Extensions: first, in a Galois extension E/F of prime degree p , where F includes a primitive root of $x^p = 1$, then the Galois group is \mathbb{Z}_p and $E = F(\beta)$ for some $\beta^p \in F$.

Roots of Unity: for ω a primitive n th root of unity, we have $\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong U(n)$.

Ruler and Compass Constructions: an n -gon is constructible iff a primitive n th root of unity is constructible; the only possible choices are $2^k \prod p_i$, where the p_i are primes of the form $2^m + 1$.

Solvable by Radicals: $f(x) \in F[x]$ which splits in some extension $F(a_1, \dots, a_n)$ and there exist $k_i \in \mathbb{Z}^+$ such that $a_i^{k_i} \in F(a_1, \dots, a_{i-1})$. In this case, the Galois group of the extension $F(a_1, \dots, a_n)$ is solvable.

Norms:

Traces:

Computations of Galois Groups:

7 Representations

Representation (of a Group): a homomorphism $\sigma : G \rightarrow M_n(\mathbb{C})$ from a group into a complex matrix ring.

Trivial Representation: the representation taking G to the identity matrix I .

Faithful Representation: a representation carrying the full group structure; hence, $\ker \sigma = 0$.

Module Correspondence: there is a bijective correspondence between $\mathbb{C}G$ -modules and complex representations.

Regular Representation: the representation corresponding to the group algebra $\mathbb{C}G$ acting on itself to form a $\mathbb{C}G$ -module.

Equivalent Representations: two representations $\sigma, \tau : G \rightarrow M_n(\mathbb{C})$ for which there exists a matrix $P \in M_n(\mathbb{C})$ such that $\sigma(g)P = P\tau(g)$ for all $g \in G$; equivalent representations come from the same module.

Irreducible Representation: a representation with no nontrivial invariant subspaces; in terms of modules, there are no nontrivial submodules.

Reducible Representation: may be written in block-triangular form; for finite groups this implies **Completely Irreducible**, which is simply block diagonal form.

Character: basically, the trace of a representation: given $\sigma : G \rightarrow M_n(\mathbb{C})$, it is the function $\chi_\sigma : G \rightarrow \mathbb{C}$ given by $\chi(g) = \text{tr}(\sigma(g))$; constant on conjugacy classes.

Irreducible Character: the character of an irreducible representation.

Class function: a function, like the character, which is constant on conjugacy classes; actually, the irreducible characters form the basis for the class functions of a group.