Algebra Qualifying Exam Notes

D. Zack Garza

Friday 12^{th} June, 2020

Contents

1 Study Guide for Algebra Qualifying Exam

References:

[1]. David Dummit and Richard Foote, Abstract Algebra, Wiley, 2003.

[2]. Kenneth Hoffman and Ray Kunze, Linear Algebra, Prentice-Hall, 1971.

[3]. Thomas W. Hungerford, Algebra, Springer, 1974.

[4]. Roy Smith, Algebra Course Notes (843-1 through 845-3), `http://www.math.uga.edu/~roy/`,

As a general rule, students are responsible for knowing both the theory (proofs) and practical applications (e.g. **how to find the Jordan or rational canonical form** of a given matrix, **or the Galois group of a given polynomial**) of the topics mentioned.
A supplement to this study guide is available at:
`http://www.math.uga.edu/sites/default/files/PDFs/Graduate/QualsStudyGuides/AlgebraPhDqualremarks.pdf`

1.1 Group Theory

- Subgroups and quotient groups
- Lagrange's Theorem
- Fundamental homomorphism theorems
- Group actions with applications to the structure of groups such as
  - The Sylow Theorems
- Group constructions such as:
  - Direct and semi-direct products
- Structures of special types of groups such as:
  - p-groups
  - Dihedral,
  - Symmetric and Alternating groups
    - Cycle decompositions
- The simplicity of A_n, for $n \geq 5$
- Free groups, generators and relations
- Solvable groups

References: [1,3,4]

1.2 Linear Algebra

- Determinants

- Eigenvalues and eigenvectors
- Cayley-Hamilton Theorem
- Canonical forms for matrices
- Linear groups $(\mathrm{GL}_n, \mathrm{SL}_n, \mathrm{O}_n, \mathrm{U}_n)$
- Duality
  - Dual spaces,
  - Dual bases,
  - Induced dual map,
  - Double duals
- Finite-dimensional spectral theorem

References: [1,2,4]

1.3 Rings and Modules

- Zorn's Lemma
  - Every vector space has a basis
  - Maximal ideals exist
- Properties of ideals and quotient rings
- Fundamental homomorphism theorems for rings and modules
- Characterizations and properties of special domains such as:
  - Euclidean $\implies$ PID $\implies$ UFD
- Classification of finitely generated modules over PIDs *(with emphasis on Euclidean Domains)*
- Applications to the structure of:
  - Finitely generated abelian groups
  - Canonical forms of matrices

References: [1,3,4]

1.4 Field Theory

- Algebraic extensions of fields
- Fundamental theorem of Galois theory
- Properties of finite fields
- Separable extensions
- Computations of Galois groups of polynomials of small degree and cyclotomic
- Polynomials
- Solvability of polynomials by radicals

References: [1,3,4]

2 Remarks

Adapted from remark written by Roy Smith, August 2006

2.1 Group theory:

The first 6 chapters (220 pages) of DF are excellent.

All the definitions and proofs of these theorems on groups are given in Smith's web based lecture notes for math 843 part 1.

Key topics:

- Sylow theorems
- Simplicity of A_n for $n > 4$.
- The first isomorphism theorem,
- The Jordan Holder theorem,

The last two (one easy, one hard) are left as exercises.

The proof JH is seldom tested on the qual, but proofs are always of interest.

- Fundamental theorem of finite abelian groups

  DF Exercises 12.1.16-19

- The simple groups of order between 60 and 168 have prime order

2.2 Rings:

- DF Chapters 7,8,9.
- Gauss's important theorem on unique factorization of polynomials:
  - $\mathbb{Z}[x]$ is a UFD
  - $R[x]$ is a UFD when R is a UFD
- The fundamental isomorphism theorems for rings (easy and useful exercise)
- How to use Zorn's lemma
  - To find maximal ideals
  - Construct algebraic field closures
  - Why it is unnecessary in countable or noetherian rings.

  Smith discusses extensively in 844-1.

- Results about PIDs

  (DF Section 8.2)

  - Example of a PID that is not a Euclidean domain

    (DF p.277)
  - Proof that a Euclidean domain is a PID and hence a UFD
  - Proof that $\mathbb{Z}$ and $k[x]$ are UFDs

    (p.289 Smith, p.300 DF)
- A polynomial ring in infinitely many variables over a UFD is still a ufd

  (Easy, DF, p.305)
- Eisenstein's criterion

  (DF p.309)
  - Stated only for monic polynomials – proof of general case identical.
  - See Smith's notes for the full version.
- Cyclic product structure of $(\mathbb{Z}/n\mathbb{Z})^\times$

  (exercise in DF, Smith 844-2, section 18)
- Grobner bases and division algorithms for polynomials in several variables

  (DF 9.6.)
- Modules over pid's and Canonical forms of matrices.

  DF sections 10.1, 10.2, 10.3, and 12.1, 12.2, 12.3.
  - Constructive proof of decomposition: DF Exercises 12.1.16-19
  - Smith 845-1 and 845-2: Detailed discussion of the constructive proof.

2.3 Field Theory / Galois Theory.

- DF chapters 13,14 (about 145 pages).
- Smith:
  - 843-2, sections 11,12, and 16-21 (39 pages)
  - 844-1, sections 7-9 (20 pages)
  - 844-2, sections 10-16, (37 pages)

3 Group Theory

3.1 Random References

3.2 Big List of Notation

$$
\begin{aligned}
C(x) &= & \left\{g \in G \,\middle|\, gxg^{-1} = x\right\} &\subseteq G && \text{Centralizer} \\
C_G(h) &= & \left\{ghg^{-1} \,\middle|\, g \in G\right\} &\subseteq G && \text{Conjugacy Class} \\
\mathcal{O}_x, G \cdot x &= & \left\{g.x \,\middle|\, x \in X\right\} &\subseteq X && \text{Orbit} \\
\mathrm{Stab}_G(x), \mathrm{Stab}_G(x), G_x &= & \left\{g \in G \,\middle|\, g.x = x\right\} &\subseteq G && \text{Stabilizer} \\
X_g &= & \left\{x \in X \,\middle|\, \forall g \in G,\ g.x = x\right\} &\subseteq X && \text{Fixed Points} \\
Z(G) &= & \left\{x \in G \,\middle|\, \forall g \in G,\ gxg^{-1} = x\right\} &\subseteq G && \text{Center} \\
\mathrm{Inn}(G) &= & \left\{\varphi_g(x) = gxg^{-1}\right\} &\subseteq \mathrm{Aut}(G) && \text{Inner Aut.} \\
\mathrm{Out}(G) &= & \mathrm{Aut}(G)/\mathrm{Inn}(G) &\hookrightarrow \mathrm{Aut}(G) && \text{Outer Aut.} \\
N(H) &= & \left\{g \in G \,\middle|\, gHg^{-1} = H\right\} &\subseteq G && \text{Normalizer}
\end{aligned}
$$

3.3 Basics

Definition (Centralizer):

$$C_G(H) = \left\{g \in G \,\middle|\, ghg^{-1} = h \ \forall h \in H\right\}$$

Definition (Normalizer):

$$N_G(H) = \left\{g \in G \,\middle|\, gHg^{-1} = H\right\}$$

Lemma: $C_G(H) \trianglelefteq N_G(H)$

Lemma: The size of the conjugacy class of H is the index of its centralizer, i.e.

$$\left|\left\{gHg^{-1} \,\middle|\, g \in G\right\}\right| = [G : C_G(H)].$$

Proof: Orbit-stabilizer.

Lemma ("The Fundamental Theorem of Cosets"):

$$aH = bH \iff a^{-1}b \in H \text{ or } aH \bigcap bH = \emptyset$$

Definition: $[x, y] = x^{-1}y^{-1}xy$ is the **commutator**, and $[G, G] \coloneqq \left\{[x, y] \,\middle|\, x, y \in G\right\}$ is the **commutator subgroup**.

Lemma:

$$[G, G] \leq H \text{ and } H \trianglelefteq G \implies G/H \text{ is abelian.}$$

Lemmas:

- Every subgroup of a cyclic group is itself cyclic.
- Intersections of subgroups are still subgroups
  - Intersections of distinct coprime-order subgroups are trivial
  - Intersections of subgroups of the same prime order are either trivial or equality
- The Quaternion group has only one element of order 2, namely -1.
  - They also have the presentation

$$\begin{aligned} Q &= \left\langle x, y, z \;\middle|\; x^2 = y^2 = z^2 = xyz = -1 \right\rangle \\ &= \left\langle x, y \;\middle|\; x^4 = y^4 = e, x^2 = y^2, yxy^{-1} = x^{-1} \right\rangle. \end{aligned}$$

- A dihedral group always has a presentation of the form

$$D_n = \left\langle x, y \;\middle|\; x^n = y^2 = (xy)^2 = e \right\rangle,$$

  yielding at least 2 distinct elements of order 2.

3.4 Finitely Generated Abelian Groups

Invariant factor decomposition:

$$G \cong \mathbb{Z}^r \times \prod_{j=1}^{m} \mathbb{Z}/(n_j) \quad \text{where } n_1 \;\Big|\; \cdots \;\Big|\; n_m.$$

Going from invariant divisors to elementary divisors:

- Take prime factorization of each factor
- Split into coprime pieces

Example:

$$\begin{aligned} &\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2^3 \cdot 5^2 \cdot 7) \\ \cong &\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2^3) \oplus \mathbb{Z}/(5^2) \oplus \mathbb{Z}/(7) \\ . \end{aligned}$$

Going from elementary divisors to invariant factors:

- Bin up by primes occurring (keeping exponents)
- Take highest power from each prime as *last* invariant factor
- Take highest power from all remaining primes as next, etc

Example: Given the invariant factor decomposition

$$G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}, .$$

$p=2$	$p=3$	$p=5$
$2,2,2$	$3,3$	5^2

$\implies n_m = 5^2 \cdot 3 \cdot 2$

$p=2$	$p=3$	$p=5$
$2,2$	3	$\emptyset$

$\implies n_{m-1} = 3 \cdot 2$

$p=2$	$p=3$	$p=5$
2	$\emptyset$	$\emptyset$

$\implies n_{m-2} = 2$

and thus

$$G \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(3 \cdot 2) \oplus \mathbb{Z}/(5^2 \cdot 3 \cdot 2).$$

Classifying Abelian Groups of a Given Order:

> Let $p(x)$ be the integer partition function.
> Example: $p(6) = 11$, given by $6, 5+1, 4+2, \cdots$.

Write $G = p_1^{k_1} p_2^{k_2} \cdots$; then there are $p(k_1)p(k_2)\cdots$ choices, each yielding a distinct group.

3.5 The Symmetric Group

Definitions:

- A cycle is **even** $\iff$ product of an *even* number of transpositions.
  - A cycle of even *length* is **odd**
  - A cycle of odd *length* is **even**

Definition The **alternating group** is the subgroup of **even** permutations, i.e. $A_n \coloneqq \left\{ \sigma \in S_n \,\middle|\, \operatorname{sign}(\sigma) = 1 \right\}$ where $\operatorname{sign}(\sigma) = (-1)^m$ where m is the number of cycles of even length.

> *Corollary:* Every $\sigma \in A_n$ has an even number of *odd* cycles (i.e. an even number of *even-length* cycles).

Example:

$$\begin{aligned} A_4 = \{&\mathrm{id}, \\ &(1,3)(2,4), (1,2)(3,4), (1,4)(2,3), \\ &(1,2,3), (1,3,2), \\ &(1,2,4), (1,4,2), \\ &(1,3,4), (1,4,3), \\ &(2,3,4), (2,4,3)\}. \end{aligned}$$

Lemmas:

- The transitive subgroups of S_3 are S_3, A_3
- The transitive subgroups of S_4 are $S_4, A_4, D_4, \mathbb{Z}_2^2, \mathbb{Z}_4$.
- S_4 has two normal subgroups: $A_4, \mathbb{Z}_2^2$.
- $S_{n\geq 5}$ has one normal subgroup: A_n.
- $Z(S_n) = 1$ for $n \geq 3$
- $Z(A_n) = 1$ for $n \geq 4$
- $[S_n, S_n] = A_n$
- $[A_4, A_4] \cong \mathbb{Z}_2^2$
- $[A_n, A_n] = A_n$ for $n \geq 5$, so $A_{n\geq 5}$ is nonabelian.
- $A_{n\geq 5}$ is *simple*.

3.6 Counting Theorems

Lagrange's Theorem:

$$H \leq G \implies |H| \,\Big|\, |G|.$$

Corollary: The order of every element divides the size of G, i.e.

$$g \in G \implies o(g) \,\Big|\, o(G) \implies g^{|G|} = e.$$

Warning: There does **not** necessarily exist $H \leq G$ with $|H| = n$ for every $n \,\Big|\, |G|$.
Counterexample: $|A_4| = 12$ but has no subgroup of order 6.

Cauchy's Theorem:

For every prime p dividing $|G|$. there is an element (and thus a subgroup) of order p.

This is a partial converse to Lagrange's theorem, and strengthened by Sylow's theorem.

Notation: For a group G acting on a set X,

- $G \cdot x = \left\{ g \curvearrowright x \,\middle|\, g \in G \right\} \subseteq X$ is the orbit
- $G_x = \left\{ g \in G \,\middle|\, g \curvearrowright x = x \right\} \subseteq G$ is the stabilizer
- $X/G \subset \mathcal{P}(X)$ is the set of orbits

- $X^g = \left\{x \in X \;\middle|\; g \curvearrowright x = x\right\} \subseteq X$ are the fixed points

Orbit-Stabilizer:

$$|G \cdot x| = [G : G_x] = |G|/|G_x| \quad \text{if } G \text{ is finite}$$

Mnemonic: $G/G_x \cong G \cdot x$.

3.6.1 Examples of Orbit-Stabilizer

1. Let G act on itself by conjugation.

- $G \cdot x$ is the **conjugacy class** of x
- $G_x = Z(x) \coloneqq C_G(x) = \left\{g \;\middle|\; [g,x] = e\right\}$, the **centralizer** of x.
- G^g (the fixed points) is the **center** $Z(G)$.

Corollary: The number of conjugates of an element (i.e. the size of its conjugacy class) is the index of its centralizer, $[G : C_G(x)]$.
Corollary: the **Class Equation**:

$$|G| = |Z(G)| + \sum_{\substack{\text{One } x_i \text{ from} \\ \text{each conjugacy} \\ \text{class}}} [G : Z(x_i)]$$

1. Let G act on S, its set of *subgroups*, by conjugation.

- $G \cdot H = \left\{gHg^{-1}\right\}$ is the **set of conjugate subgroups** of H
- $G_H = N_G(H)$ is the **normalizer** of in G of H
- S^G is the set of **normal subgroups** of G

Corollary: Given $H \leq G$, the number of conjugate subgroups is $[G : N_G(H)]$.

1. For a fixed proper subgroup $H < G$, let G act on its cosets $G/H = \left\{gH \;\middle|\; g \in G\right\}$ by left-multiplication.

- $G \cdot gH = G/H$, i.e. this is a *transitive* action.
- $G_{gH} = gHg^{-1}$ is a *conjugate subgroup* of H
- $(G/H)^G = \emptyset$

Application: If G is simple, $H < G$ proper, and $[G : H] = n$, then there exists an injective map $\varphi : G \hookrightarrow S_n$.
Proof: This action induces φ; it is nontrivial since $gH = H$ for all g implies $H = G$; $\ker \varphi \trianglelefteq G$ and G simple implies $\ker \varphi = 1$.

Burnside's Formula:

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

3.6.2 Sylow Theorems

Notation: For any p, let $\mathrm{Syl}_p(G)$ be the set of Sylow-p subgroups of G.

Write

- $|G| = p^n m$ where $(m,p) = 1$,
- S_p a Sylow-p subgroup, and
- n_p the number of Sylow-p subgroups.

Definition: A p-group is a group G such that every element is order p^k for some k. If G is a finite p-group, then $|G| = p^j$ for some j.

Lemma: p-groups have nontrivial centers.

Some useful facts:

- Coprime order subgroups are disjoint, or more generally $\mathbb{Z}_p, \mathbb{Z}_q \subset G \implies \mathbb{Z}_p \bigcap \mathbb{Z}_q = \mathbb{Z}_{(p,q)}$.
- The Chinese Remainder theorem: $(p,q) = 1 \implies \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$

3.6.3 Sylow 1 (Cauchy for Prime Powers)

$$\forall p^n \text{ dividing } |G| \quad \text{there exists a subgroup of size } p^n.$$

If $|G| = \prod p_i^{\alpha_i}$, then there exist subgroups of order $p_i^{\beta_i}$ for every i and every $0 \leq \beta_i \leq \alpha_i$. In particular, Sylow p-subgroups always exist.

3.6.4 Sylow 2 (Sylows are Conjugate)

All sylow-p subgroups S_p are conjugate, i.e.

$$S_p^1, S_p^2 \in \mathrm{Syl}_p(G) \implies \exists g \text{ such that } gS_p^1 g^{-1} = S_p^2.$$

Corollary: $n_p = 1 \iff S_p \trianglelefteq G$

3.6.5 Sylow 3 (Numerical Constraints)

1. $n_p \mathrel{\Big|} m$ (in particular, $n_p \leq m$),
2. $n_p \equiv 1 \mod p$,
3. $n_p = [G : N_G(S_p)]$ where N_G is the normalizer.

Corollary: p does not divide n_p.

Lemma: Every p-subgroup of G is contained in a Sylow p-subgroup.

Proof: Let $H \leq G$ be a p-subgroup. If H is not *properly* contained in any other p-subgroup, it is a Sylow p-subgroup by definition.
Otherwise, it is contained in some p-subgroup H^1. Inductively this yields a chain $H \subsetneq H^1 \subsetneq \cdots$, and by Zorn's lemma $H := \bigcup_i H^i$ is maximal and thus a Sylow p-subgroup.

Fratini's Argument: If $H \trianglelefteq G$ and $P \in \mathrm{Syl}_p(G)$, then $HN_G(P) = G$ and $[G : H]$ divides $|N_G(P)|$.

3.7 Products

Characterizing direct products: $G \cong H \times K$ when

- $G = HK = \left\{ hk \;\middle|\; h \in H, k \in K \right\}$
- $H \bigcap K = \{e\} \subset G$
- $H, K \trianglelefteq G$

Can relax to only $H \trianglelefteq G$ to get a semidirect product instead

Characterizing semidirect products: $G = N \rtimes_\psi H$ when

- $G = NH$
- $N \trianglelefteq G$
- $H \curvearrowright N$ by conjugation via a map

$$\begin{aligned} \psi : H &\longrightarrow \mathrm{Aut}(N) \\ h &\mapsto h(\,\cdot\,)h^{-1}. \end{aligned}$$

Useful Facts

- If $\sigma \in \mathrm{Aut}(H)$, then $N \rtimes_\psi H \cong N \rtimes_{\psi\circ\sigma} H$.
- $\mathrm{Aut}((\mathbb{Z}/(p)^n) \cong \mathrm{GL}(n, \mathbb{F}_p)$, which has size \$- $|\mathrm{Aut}(\mathbb{Z}/(p)^n)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.
  - If this occurs in a semidirect product, it suffices to consider similarity classes of matrices (i.e. just use canonical forms)
- $\mathrm{Aut}(\mathbb{Z}/(n)) \cong \mathbb{Z}/(n)^\times \cong \mathbb{Z}/(\varphi(n))$ where φ is the totient function.
  - $\varphi(p^k) = p^{k-1}(p-1)$
- If G, H have coprime order then $\mathrm{Aut}(G \oplus H) \cong \mathrm{Aut}(G) \oplus \mathrm{Aut}(H)$.

3.8 Isomorphism Theorems

Lemma: If $H, K \leq G$ and $H \leq N_G(K)$ (or $K \trianglelefteq G$) then $HK \leq G$ is a subgroup.

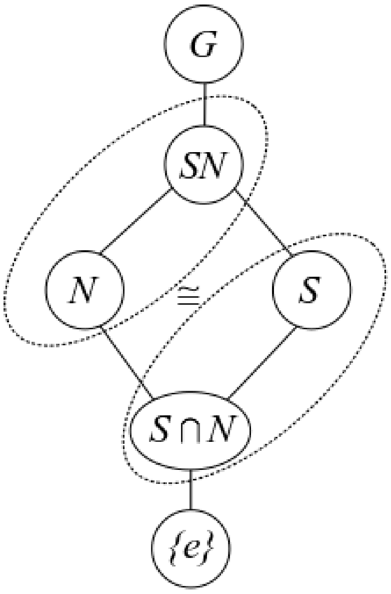
Note that this implies that HK is not always a subgroup.

Diamond Theorem / 2nd Isomorphism Theorem:

If $S \leq G$ and $N \trianglelefteq G$, then

$$\frac{SN}{N} \cong \frac{S}{S \bigcap N} \quad \text{and} \quad |SN| = \frac{|S||N|}{|S \bigcap N|}$$

Mnemonic:



> Note: for this to make sense, we also have
>
> - $SN \leq G$,
> - $S \bigcap N \trianglelefteq S$,

Cancellation / 3rd Isomorphism Theorem

If $H, K \trianglelefteq G$ with $H \trianglelefteq K$, then

$$\frac{G/H}{G/K} \cong \frac{G}{K}$$

> Note: for this to make sense, we also have $G/K \trianglelefteq G/H$.

The Correspondence Theorem / 4th Isomorphism Theorem: Suppose $N \trianglelefteq G$, then there exists a correspondence:

$$\left\{H < G \;\middle|\; N \subseteq H\right\} \iff \left\{H \;\middle|\; H < \frac{G}{N}\right\}$$
$$\left\{\begin{matrix}\text{Subgroups of } G \\ \text{containing } N\end{matrix}\right\} \iff \left\{\begin{matrix}\text{Subgroups of the} \\ \text{quotient } G/N\end{matrix}\right\}.$$

In words, subgroups of G containing N correspond to subgroups of the quotient group G/N. This is given by the map $H \mapsto H/N$.

> Note: $N \trianglelefteq G$ and $N \subseteq H < G \implies N \trianglelefteq H$.

3.9 Special Classes of Groups

Definition: The **"2 out of 3 property"** is satisfied by a class of groups $\mathcal{C}$ iff whenever $G \in \mathcal{C}$, then $N, G/N \in \mathcal{C}$ for any $N \trianglelefteq G$.

Definition: If $|G| = p^k$, then G is a **p-group.**

Facts about p-groups:

- If $k = 1$ then G is cyclic
- If $k = 2$, then $G \cong \mathbb{Z}/(p)^2$ or $\mathbb{Z}/(p^2)$.
- p-groups have nontrivial centers
  - Proof: Use class equation.
- Every normal subgroup is contained in the center
- Normalizers grow
- Every maximal is normal
- Every maximal has index p
- p-groups are *nilpotent*
- p-groups are *solvable*

Facts about other special order groups:

General strategy: find a normal subgroup (usually a Sylow) and use recognition of semidirect products.

- $|G| = pq$: Two possibilities. By cases:
  - If p divides $q - 1$, two cases:
    - $G \cong \mathbb{Z}/(pq)$ or $\mathbb{Z}(p) \times \mathbb{Z}/(q)$
  - Otherwise, $G \cong \mathbb{Z}/(pq)$

  Proof: Sylow theorems. Note: Such groups are never simple.
- $|G| = p^2 q$:
  - $q \mid p^2 - 1$: Two abelian possibilities, $\mathbb{Z}/(p) \times \mathbb{Z}/(q^2)$, or $\mathbb{Z}/(pq) \times \mathbb{Z}/(q)$.
  - Otherwise, the sylow-q subgroup H is normal and order q^2, so either $\mathbb{Z}/(q)^2$ or $\mathbb{Z}/(q^2)$.
    - Case 2: $\left|\mathrm{Aut}(\mathbb{Z}/(q)^2)\right| = q(q-1)$, so only trivial action
    - Case 1: $\left|\mathrm{Aut}(\mathbb{Z}/(q^2))\right| = q(q-1)^2(q+1)$
      - If p doesn't divide $q + 1$, noting new
      - Otherwise, a nontrivial semidirect product.

Definition: A group G is **simple** iff $H \trianglelefteq G \implies H = \{e\}, G$, i.e. it has no non-trivial proper subgroups.

> **Lemma:** If G is *not* simple, then for any $N \trianglelefteq G$, it is the case that $G \cong E$ for an extension of the form $N \longrightarrow E \longrightarrow G/N$. >

Definition: A group G is **solvable** iff G has a terminating normal series with abelian factors, i.e.

$$G \longrightarrow G^1 \longrightarrow \cdots \longrightarrow \{e\} \text{ with } G^i/G^{i+1} \text{ abelian for all } i.$$

Lemmas:

- G is solvable iff G has a terminating *derived series.*

- Solvable groups satisfy the 2 out of 3 property
- Abelian $\implies$ solvable
- Every group of order less than 60 is solvable.

Definition: A group G is **nilpotent** iff G has a terminating central series, upper central series, or lower central series.

> Moral: the adjoint map is nilpotent.

Lemma: For G a finite group, TFAE:

- G is nilpotent
- Normalizers grow (i.e.$H < N_G(H)$ whenever H is proper)
- Every Sylow-p subgroup is normal
- G is the direct product of its Sylow p-subgroups
- Every maximal subgroup is normal
- G has a terminating *Lower* Central Series
- G has a terminating *Upper* Central Series

Lemmas:

- G nilpotent $\implies$ G solvable
- Nilpotent groups satisfy the 2 out of 3 property.
- G has normal subgroups of order d for *every* d dividing $|G|$
- G nilpotent $\implies$ $Z(G) \neq 0$
- Abelian $\implies$ nilpotent
- p-groups $\implies$ nilpotent

3.10 Series of Groups

Definition: A **normal series** of a group G is a sequence $G \longrightarrow G^1 \longrightarrow G^2 \longrightarrow \cdots$ such that $G^{i+1} \trianglelefteq G_i$ for every i.

Definition A **composition series** of a group G is a finite normal series such that G^{i+1} is a *maximal proper* normal subgroup of G^i.

Theorem (Jordan-Holder): Any two composition series of a group have the same length and isomorphic factors (up to permutation).1

Definition A **derived series** of a group G is a normal series $G \longrightarrow G^1 \longrightarrow G^2 \longrightarrow \cdots$ where $G^{i+1} = [G^i, G^i]$ is the commutator subgroup.

> The derived series terminates iff G is *solvable*.

Definition: A **central series** for a group G is a terminating normal series $G \longrightarrow G^1 \longrightarrow \cdots \longrightarrow \{e\}$ such that each quotient is **central**, i.e. $[G, G^i] \leq G^{i-1}$ for all i.

Definition: A **lower central series** is a terminating normal series $G \longrightarrow G^1 \longrightarrow \cdots \longrightarrow \{e\}$ such that $G^{i+1} = [G^i, G]$

> Moral: Iterate the adjoint map $[\,\cdot\,, G]$.

> G is nilpotent $\iff$ the LCS terminates.

Definition: An **upper central series** is a terminating normal series $G \longrightarrow G^1 \longrightarrow \cdots \longrightarrow \{e\}$ such that $G^1 = Z(G)$ and G^{i+1} is defined such that $G^{i+1}/G^i = Z(G^i)$.

> Moral: Iterate taking "higher centers".

3.11 Classification of Groups

- Keith Conrad: Classifying Groups of Order 12
- Order p: cyclic.
- Order pq: ?
- Order p^2q: ?

4 Rings

4.1 Definitions

Lemma: Intersections, products, and sums (but not necessarily unions) of ideals are ideals.

Theorem (Krull): Every ring has proper maximal ideals, and any proper ideal is contained in a maximal ideal.

Definition: A ring R is **simple** iff every ideal $I \trianglelefteq R$ is either 0 or R.

Definition: An element $r \in R$ is **irreducible** iff $r = ab \implies a$ is a unit or b is a unit.

Definition: An element $r \in R$ is **prime** iff $ab \mathrel{\Big|} r \implies a \mathrel{\Big|} r$ or $b \mathrel{\Big|} r$ whenever a, b are nonzero and not units.

Definition: $\mathfrak{p}$ is a **prime** ideal $\iff ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Definition: $\operatorname{Spec}(R) = \left\{\mathfrak{p} \trianglelefteq R \mathrel{\Big|} \mathfrak{p} \text{ is prime}\right\}$ is the **spectrum** of R.

Definition: $\mathfrak{m}$ is **maximal** $\iff I \ntrianglelefteq R \implies I \subseteq \mathfrak{m}$.

> Example: Maximal ideals of $R[x]$ are of the form $I = (x - a_i)$ for some $a_i \in R$.

Definition: $\operatorname{Spec}_{\max}(R) = \left\{\mathfrak{m} \trianglelefteq R \mathrel{\Big|} \mathfrak{m} \text{ is maximal}\right\}$ is the **max-spectrum** of R.

> Note: nonstandard notation / definition.

Lemmas (Quotients of Rings):

- R/I is a domain $\iff I$ is prime,
- R/I is a field $\iff I$ is maximal.
- For R a PID, I is prime $\iff I$ is maximal.

Lemma (Characterizations of Rings):

- R a commutative division ring $\implies R$ is a field
- R a finite integral domain $\implies R$ is a field.
- $\mathbb{F}$ a field $\implies \mathbb{F}[x]$ is a Euclidean domain.
- $\mathbb{F}$ a field $\implies \mathbb{F}[x]$ is a PID.
- $\mathbb{F}$ is a field $\iff \mathbb{F}$ is a commutative simple ring.

- R is a UFD $\iff$ $R[x]$ is a UFD.
- R a PID $\implies$ $R[x]$ is a UFD
- R a PID $\implies$ R Noetherian
- $R[x]$ a PID $\implies$ R is a field.

Lemma: Fields $\subset$ Euclidean domains $\subset$ PIDs $\subset$ UFDs $\subset$ Integral Domains $\subset$ Rings

- A Euclidean Domain that is not a field: $\mathbb{F}[x]$ for $\mathbb{F}$ a field
  - *Proof*: Use previous lemma, and x is not invertible
- A PID that is not a Euclidean Domain: $\mathbb{Z}\left[\dfrac{1+\sqrt{-19}}{2}\right]$.
  - *Proof*: complicated.
- A UFD that is not a PID: $\mathbb{F}[x, y]$.
  - *Proof*: $\langle x, y\rangle$ is not principal
- An integral domain that is not a UFD: $\mathbb{Z}[\sqrt{-5}]$
  - *Proof*: $(2+\sqrt{-5})(2-\sqrt{-5}) = 9 = 3 \cdot 3$, where all factors are irreducible (check norm).
- A ring that is not an integral domain: $\mathbb{Z}/(4)$
  - *Proof*: $2 \mod 4$ is a zero divisor.

Lemma: In R a UFD, an element $r \in R$ is prime $\iff$ r is irreducible.

> Note: For R an integral domain, prime $\implies$ irreducible, but generally not the converse.
> *Example of a prime that is not irreducible:* $x^2 \mod (x^2 + x) \in \mathbb{Q}[x]/(x^2 + x)$. Check that x is prime directly, but $x = x \cdot x$ and x is not a unit.
> *Example of an irreducible that is not prime:* $3 \in \mathbb{Z}[\sqrt{-5}]$. Check norm to see irreducibility, but $3 \,\Big|\, 9 = (2+\sqrt{-5})(2-\sqrt{-5})$ and doesn't divide either factor.

Lemma: If R is a PID, then every element in R has a unique prime factorization.

Definition: A nonzero unital ring R is **semisimple** iff $R \cong \displaystyle\bigoplus_{i=1}^{n} M_i$ with each M_i a simple module.

Theorem (Artin-Wedderubrn): If R is a nonzero, unital, *semisimple* ring then $R \cong \displaystyle\bigoplus_{i=1}^{m} \mathrm{Mat}(n_i, D_i)$, a finite sum of matrix rings over division rings.

> *Corollary:* If M is a simple ring over R a division ring, the M is isomorphic to a matrix ring.

4.2 Nontrivial Properties

Lemma: Every $a \in R$ for a finite ring is either a unit or a zero divisor.

> *Proof:* Let $a \in R$ and define $\varphi(x) = ax$. If φ is injective, then it is surjective, so $1 = ax$ for some $x \implies x^{-1} = a$. Otherwise, $ax_1 = ax_2$ with $x_1 \neq x_2 \implies a(x_1 - x_2) = 0$ and $x_1 - x_2 \neq 0$, so a is a zero divisor.

4.3 Ideals

4.3.1 Maximal and Prime Ideals

Lemma: Maximal $\implies$ prime, but generally not the converse.

Counterexample: $(0) \in \mathbb{Z}$ is prime since $\mathbb{Z}$ is a domain, but not maximal since it is properly contained in any other ideal.

Proof: Suppose $\mathfrak{m}$ is maximal, $ab \in \mathfrak{m}$, and $b \notin \mathfrak{m}$. Then there is a containment of ideals $\mathfrak{m} \subsetneq \mathfrak{m} + (b) \implies \mathfrak{m} + (b) = R$.
So

$$1 = m + rb \implies a = am + r(ab),$$

but $am \in \mathfrak{m}$ and $ab \in \mathfrak{m} \implies a \in \mathfrak{m}$.

■

Lemma: If x is not a unit, then x is contained in some maximal ideal $\mathfrak{m}$.

Proof: Zorn's lemma.

Lemma: $R/\mathfrak{m}$ is a field $\iff$ $\mathfrak{m}$ is maximal.

Lemma: $R/\mathfrak{p}$ is an integral domain $\iff$ $\mathfrak{p}$ is prime.

4.3.2 Nilradical and Jacobson Radical

Definition: $\mathfrak{N} := \left\{ x \in R \;\middle|\; x^n = 0 \text{ for some } n \right\}$ is the **nilradical** of R.

Lemma: The nilradical is the intersection of all **prime** ideals, i.e.

$$\mathfrak{N}(R) = \bigcap_{\mathfrak{p} \in \operatorname{Spec}(R)} \mathfrak{p}$$

Proof:
$\mathfrak{N} \subseteq \bigcap \mathfrak{p}$: $x \in \mathfrak{N} \implies x^n = 0 \in \mathfrak{p} \implies x \in \mathfrak{p}$ or $x^{n-1} \in \mathfrak{p}$.
$\mathfrak{N}^c \subseteq \bigcup \mathfrak{p}^c$: Define $S = \left\{ I \trianglelefteq R \;\middle|\; a^n \notin I \text{ for any } n \right\}$. Then apply Zorn's lemma to get a maximal ideal $\mathfrak{m}$, and maximal $\implies$ prime.

Lemma: $R/\mathfrak{N}(R)$ has no nonzero nilpotent elements.

Proof:

$$\begin{aligned} a + \mathfrak{N}(R) \text{ nilpotent } &\implies (a + \mathfrak{N}(R))^n := a^n + \mathfrak{N}(R) = \mathfrak{N}(R) \\ &\implies a^n \in \mathfrak{N}(R) \\ &\implies \exists \ell \text{ such that } (a^n)^\ell = 0 \\ &\implies a \in \mathfrak{N}(R). \end{aligned}$$

Definition: The **Jacobson radical** is the intersection of all **maximal** ideals, i.e.

$$J(R) = \bigcap_{\mathfrak{m} \in \operatorname{Spec}_{\max}} \mathfrak{m}$$

Lemma: $\mathfrak{N}(R) \subseteq J(R)$.

Proof: Maximal $\implies$ prime, and so if x is in every prime ideal, it is necessarily in every maximal ideal as well.

4.3.3 Zorn's Lemma

Lemma: A field has no nontrivial proper ideals.

Lemma: If $I \trianglelefteq R$ is a proper ideal $\iff$ I contains no units.

Proof: $r \in R^\times \bigcap I \implies r^{-1}r \in I \implies 1 \in I \implies x \cdot 1 \in I \quad \forall x \in R$.

Lemma: If $I_1 \subseteq I_2 \subseteq \cdots$ are ideals then $\bigcup_j I_j$ is an ideal.

Example Application of Zorn's Lemma: Every proper ideal is contained in a maximal ideal.

Proof: Let $0 < I < R$ be a proper ideal, and consider the set

$$S = \left\{ J \;\middle|\; I \subseteq J < R \right\}.$$

Note $I \in S$, so S is nonempty. The claim is that S contains a maximal element M.
S is a poset, ordered by set inclusion, so if we can show that every chain has an upper bound, we can apply Zorn's lemma to produce M.
Let $C \subseteq S$ be a chain in S, so $C = \{C_1 \subseteq C_2 \subseteq \cdots\}$ and define $\widehat{C} = \bigcup_i C_i$.

$\widehat{C}$ is an upper bound for C:
This follows because every $C_i \subseteq \widehat{C}$.
$\widehat{C}$ is in S:
Use the fact that $I \subseteq C_i < R$ for every C_i and since no C_i contains a unit, $\widehat{C}$ doesn't contain a unit, and is thus proper.

■