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

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

- $[g,h] = ghg^{-1}h^{-1}$
- $[G,H] = \langle [g,h] : g \in G, h \in H \rangle$ (Subgroup generated by commutators)

Definition 3.0.1 (Normal Closure of a subgroup)**.**

- $H^G = \{gHg^{-1} : g \in G\}$
- Equivalently,

$$H^G = \bigcap \{N : H \leq N \trianglelefteq G\}$$

  - (The smallest normal subgroup of G containing H)

Definition 3.0.2 (Normal Core of a subgroup)**.**

- $$H_G = \bigcap_{g \in G} gHg^{-1}$$
- Equivalently, $H_G = \langle N : N \trianglelefteq G \ \&\ N \leq H \rangle$
  - Largest normal subgroup that contains H
- Equivalently, $H_G = \ker\psi$ where $\psi : G \to Sym(G/H);\ g \sim (xH) = (gx)H$

- Facts:
  - $H_G \trianglelefteq G$ and is an idempotent operation

Definition 3.0.3 (Characteristic subgroup)**.**

- H char $G \iff \forall \varphi \in Aut(G), \varphi(H) = H$
  - i.e., H is fixed by all automorphisms of G.

3.3 Basics

Definition 3.0.4 (Centralizer):)**.**

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

Definition 3.0.5 (Normalizer)**.**

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

- Equivalently, $\bigcup\{K : H \trianglelefteq K \leq G\}$ (the largest $K \leq G$ for which $H \trianglelefteq K$)
- Equivalently, the stabilizer of H under G acting on its subgroups via conjugation

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 $[G, G] := \left\{ [x, y] \;\middle|\; x, y \in G \right\}$ 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:

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

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. $A_n \coloneqq \left\{ \sigma \in S_n \;\middle|\; \mathrm{sign}(\sigma) = 1 \right\}$ where $\mathrm{sign}(\sigma) = (-1)^m$ 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

Theorem 3.1 ***(Lagrange's Theorem).***
$H \leq G \implies |H| \,\Big|\, |G|$.

Corollary 3.2.
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.

Theorem 3.3 ***(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.

3.6.1 Group Actions

Definition 3.3.1 (Group Action)**.**
An action of G on X is a group morphism

$$\begin{aligned} \varphi : G \times X &\to X \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

or equivalently

$$\begin{aligned} \varphi : G &\longrightarrow \operatorname{Aut}(X) \\ g \mapsto (x \mapsto \varphi_g(x) &:= g \cdot x) \end{aligned}$$

satisfying
1. $e \cdot x = x$
2. $g \cdot (h \cdot x) = (gh) \cdot x$

Note that $\ker \psi = \bigcap_{x \in X} G_x$ is the intersection of all stabilizers.

Definition 3.3.2 (Transitive)**.**
A group action $G \curvearrowright X$ is *transitive* iff for all $x, y \in X$ there exists a $g \in G$ such that $g \cdot x = x$. Equivalently, the action has a single orbit.

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

Note that being in the same orbit is an equivalence relation which partitions X, and G acts transitively if restricted to any single orbit.

Orbit-Stabilizer:

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

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

3.6.2 Examples of Orbit-Stabilizer

1. Let G act on itself by left translation, where $g \mapsto (h \mapsto gh)$.

- The orbit $G \cdot x = G$ is the entire group
- The stabilizer G_x is only the identity.
- The fixed points X^g are only the identity.

1. Let G act on *itself* by conjugation.

- $G \cdot x$ is the **conjugacy class** of x (so not generally transitive)
- $G_x = Z(x) \coloneqq C_G(x) = \left\{ g \;\middle|\; [g, x] = e \right\}$, 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 X, 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
- X^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 translation.

- $G \cdot gH = G/H$, 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:

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

3.6.3 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 3.3.3.
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.

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: $(p, q) = 1 \implies \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$

3.6.4 Sylow 1 (Cauchy for Prime Powers)

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

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.

3.6.5 Sylow 2 (Sylows are Conjugate)

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

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

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

3.6.6 Sylow 3 (Numerical Constraints)

1. $n_p \mid m$ (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.

Theorem 3.4 ***(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

Theorem 3.5 ***(Recognizing Direct Products).***
We have $G \cong H \times K$ when

- $H, K \trianglelefteq G$
- $G = HK$.
- $H \bigcap K = \{e\} \subset G$

Note: can relax to $[h, k] = 1$ for all h, k.

Theorem 3.6 ***(Recognizing Generalized Direct Products).***
We have $G = \prod_{i=1}^{n} H_i$ when

- $H_i \trianglelefteq G$ for all i.
- $G = H_1 \cdots H_n$
- $H_k \bigcap H_1 \cdots \widehat{H_k} \cdots H_n = \emptyset$

Note on notation: intersect H_k with the amalgam *leaving out* H_k.

Theorem 3.7 ***(Recognizing Semidirect Products).***
We have $G = N \rtimes_\psi H$ when

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

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

> Note relaxed conditions compared to direct product: $H \trianglelefteq G$ and $K \leq G$ to get a semidirect product instead

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.

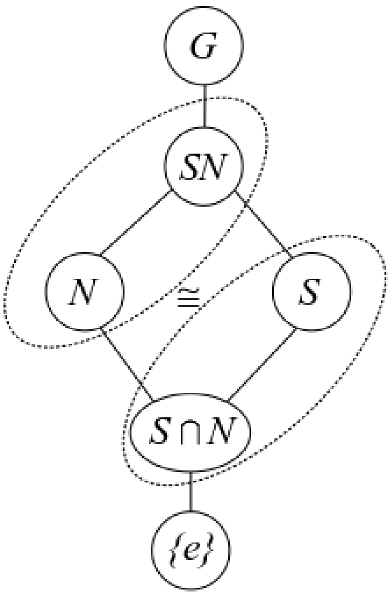
> Note that this implies that HK is not always a subgroup.

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

- $SN \leq G$,
- $S \bigcap N \trianglelefteq S$,

Corollary 3.8.
If we relax the conditions to $S, N \leq G$ with $S \in N_G(N)$, then $S \bigcap N \trianglelefteq S$ (but is not normal in G) and the theorem still applies.

Cancellation / 3rd Isomorphism Theorem

Suppose $N, K \leq G$ with $N \trianglelefteq G$ and $N \subseteq K \subseteq G$.

1. If $K \leq G$ then $K/N \leq G/N$ is a subgroup
2. If $K \trianglelefteq G$ then $K/N \trianglelefteq G/N$.
3. Every subgroup of G/N is of the form K/N for some such $K \leq G$.
4. Every *normal* subgroup of G/N is of the form K/N for some such $K \trianglelefteq G$.
5. If $K \trianglelefteq G$, then we can cancel normal subgroups:

$$\frac{G/N}{K/N} \cong \frac{G}{K}.$$

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.
- $|G| = p^2 q$:
  - $q \,\Big|\, p^2 - 1$: 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 3.8.1 (Simple Groups)**.**
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 $ab \mid r \implies a \mid r$ or $b \mid r$ 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: $\operatorname{Spec}(R) = \left\{ \mathfrak{p} \trianglelefteq R \;\middle|\; \mathfrak{p} \text{ is prime} \right\}$ 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: $\operatorname{Spec}_{\max}(R) = \left\{ \mathfrak{m} \trianglelefteq R \;\middle|\; \mathfrak{m} \text{ is maximal} \right\}$ 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 $3 \mid 9 = (2+\sqrt{-5})(2-\sqrt{-5})$ 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 $R \cong \bigoplus_{i=1}^{n} M_i$ with each M_i a simple module.

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

■

5 Fields

Let k denote a field.

Lemmas:

- The characteristic of any field k is either 0 or p a prime.
- All fields are simple rings (no proper nontrivial ideals).
- If L/k is algebraic, then $\min(\alpha, L)$ divides $\min(\alpha, k)$.
- Every field morphism is either zero or injective.

Theorem 5.1.
Every finite extension is algebraic.

Proof .
Todo?

■

Theorem 5.2 *(Gauss' Lemma)*.
Let R be a UFD and F its field of fractions. Then a primitive $p \in R[x]$ is irreducible in $R[x] \iff p$ is irreducible in $F[x]$.

Corollary 5.3.
A primitive polynomial $p \in \mathbb{Q}[x]$ is irreducible $\iff$ p is irreducible in $\mathbb{Z}[x]$.

Theorem 5.4 *(Eisenstein's Criterion)*.
If $f(x) = \sum_{i=0}^{n} \alpha_i x^i \in \mathbb{Q}[x]$ and $\exists p$ such that

- p divides every coefficient *except* a_n and
- p^2 does not divide a_0,

then f is irreducible over $\mathbb{Q}[x]$, and by Gauss' lemma, over $\mathbb{Z}[x]$.

Definition 5.4.1 (Primitive)**.**
For R a UFD, a polynomial $p \in R[x]$ is **primitive** iff the greatest common divisors of its coefficients is a unit.

5.1 Finite Fields

Definition 5.4.2.
The **prime subfield** of a field F is the subfield generated by 1.

Lemma 5.5 ***(Characterization of Prime Subfields).***
The prime subfield of any field is isomorphic to either $\mathbb{Q}$ or $\mathbb{F}_p$ for some p.

Proposition 5.6 ***(Freshman's Dream).***
If char $k = p$ then $(a+b)^p = a^p + b^p$ and $(ab)^p = a^p b^p$.

Proof .
Todo

■

Theorem 5.7 ***(Construction of Finite Fields).***
$\mathbb{GF}(p^n) \cong \dfrac{\mathbb{F}_p}{(f)}$ where $f \in \mathbb{F}_p[x]$ is any irreducible of degree n, and $\mathbb{GF}(p^n) \cong \mathbb{F}[\alpha] \cong \operatorname{span}_{\mathbb{F}} \left\{1, \alpha, \cdots, \alpha^{n-1}\right\}$ for any root α of f.

Lemma 5.8 ***(Prime Subfields of Finite Fields).***
Every finite field F is isomorphic to a unique field of the form $\mathbb{GF}(p^n)$ and if char $F = p$, it has prime subfield $\mathbb{F}_p$.

Lemma 5.9 ***(Containment of Finite Fields).***
$\mathbb{GF}(p^\ell) \leq \mathbb{GF}(p^k) \iff \ell$ divides k.

Lemma 5.10 ***(Identification of Finite Fields as Splitting Fields).***
$\mathbb{GF}(p^n)$ is the splitting field of $\rho(x) = x^{p^n} - x$, and the elements are exactly the roots of ρ.

Proof .
Todo. Every element is a root by Cauchy's theorem, and the p^n roots are distinct since its derivative is identically -1.

■

Lemma 5.11 ***(Splits Product of Irreducibles).***
Let $\rho_n := x^{p^n} - x$. Then $f(x) \mathrel{\Big|} \rho_n(x) \iff \deg f \mathrel{\Big|} n$ and f is irreducible.

Corollary 5.12.
$x^{p^n} - x = \prod f_i(x)$ over all irreducible monic $f_i \in \mathbb{F}_p[x]$ of degree d dividing n.

Proof .

$\Longleftarrow$: Suppose f is irreducible of degree d. Then $f \mid x^{p^d} - x$ (consider $F[x]/\langle f \rangle$) and $x^{p^d} - x \mid x^{p^n} - x \iff d \mid n$.

$\Longrightarrow$:

- $\alpha \in \mathbb{GF}(p^n) \iff \alpha^{p^n} - \alpha = 0$, so every element is a root of φ_n and $\deg \min(\alpha, \mathbb{F}_p) \mid n$ since $\mathbb{F}_p(\alpha)$ is an intermediate extension.
- So if f is an irreducible factor of φ_n, f is the minimal polynomial of some root α of φ_n, so $\deg f \mid n$. $\varphi_n'(x) = p^n x^{p^{n-1}} \neq 0$, so φ_n has distinct roots and thus no repeated factors. So φ_n is the product of all such irreducible f.

■

Lemma 5.13.
No finite field is algebraically closed.

Proof .
Todo?

■

5.2 Galois Theory

Definition 5.13.1.
A field extension L/k is **algebraic** iff every $\alpha \in L$ is the root of some polynomial $f \in k[x]$.

Definition 5.13.2.
Let L/k be a finite extension. Then TFAE:

- L/k is **normal**.
- Every irreducible $f \in k[x]$ that has one root in L has *all* of its roots in L
  - i.e. every polynomial splits into linear factors
- Every embedding $\sigma : L \hookrightarrow \overline{k}$ that is a lift of the identity on k satisfies $\sigma(L) = L$.
- If L is separable: L is the splitting field of some irreducible $f \in k[x]$.

Definition 5.13.3.
Let L/k be a field extension, $\alpha \in L$ be arbitrary, and $f(x) := \min(\alpha, k)$. TFAE:

- L/k is **separable**
- f has no repeated factors/roots
- $\gcd(f, f') = 1$, i.e. f is coprime to its derivative
- $f' \not\equiv 0$

Lemma 5.14.
If char $k = 0$ or k is finite, then every *algebraic* extension L/k is separable.

Definition 5.14.1.
$\mathrm{Aut}(L/k) = \left\{\sigma : L \longrightarrow L \;\middle|\; \sigma|_k = \mathrm{id}_k\right\}$.

Lemma 5.15.
If L/k is algebraic, then $\mathrm{Aut}(L/k)$ permutes the roots of irreducible polynomials.

Lemma 5.16.
$|\mathrm{Aut}(L/k)| \leq [L : k]$ with equality precisely when L/k is normal.

Definition 5.16.1.
If L/k is Galois, we define $\mathrm{Gal}(L/k) := \mathrm{Aut}(L/k)$.

5.2.1 Lemmas About Towers

Let $L/F/k$ be a finite tower of field extensions

- Multiplicativity: $[L : k] = [F : L][F : k]$
- L/k normal/algebraic/Galois $\implies$ L/F normal/algebraic/Galois.
  - *Proof (normal):* $\min(\alpha, F) \;\Big|\; \min(\alpha, k)$, so if the latter splits in L then so does the former.
  - *Corollary:* $\alpha \in L$ algebraic over $k \implies \alpha$ algebraic over F.
  - *Corollary:* E_1/k normal and E_2/k normal $\implies E_1E_2/k$ normal and $E_1 \bigcap E_2/k$ normal.

$$\begin{tikzcd} L \arrow[d, dotted, bend right] \arrow[dd, bend left] \\ F \\ k \end{tikzcd}$$

- F/k algebraic and L/F algebraic $\implies$ L/k algebraic.
- If L/k is algebraic, then F/k separable and L/F separable $\iff$ L/k separable

$$\begin{tikzcd} L \arrow[d, bend right] \arrow[dd, dashed, bend left] \\ F \arrow[d, bend right] \\ k \end{tikzcd}$$

- F/k Galois and L/K Galois $\implies$ F/k Galois **only if** $\mathrm{Gal}(L/F) \trianglelefteq \mathrm{Gal}(L/k)$
  - $\implies \mathrm{Gal}(F/k) \cong \dfrac{\mathrm{Gal}(L/k)}{\mathrm{Gal}(L/F)}$

$$\begin{tikzcd}
L \arrow[d, dotted, bend right] \arrow[dd, bend left] \\
F \arrow[d, bend right] \\
k
\end{tikzcd}$$

Common Counterexamples:

- $\mathbb{Q}(\zeta_3, 2^{1/3})$ is normal but $\mathbb{Q}(2^{1/3})$ is not since the irreducible polynomial $x^3 - 2$ has only one root in it.

Definition 5.16.2 (Characterizations of Galois Extensions)**.**
Let L/k be a finite field extension. TFAE:
- L/k is **Galois**
- L/k is finite, normal, and separable.
- L/k is the splitting field of a separable polynomial
- $|\mathrm{Aut}(L/k)| = [L : k]$
- The fixed field of $\mathrm{Aut}(L/k)$ is exactly k.

Theorem 5.17 ***(Fundamental Theorem of Galois Theory).***
Let L/k be a Galois extension, then there is a correspondence:

$$\left\{\text{Subgroups } H \leq \mathrm{Gal}(L/k)\right\} \iff \left\{\substack{\text{Fields } F \text{ such} \\ \text{that } L/F/k}\right\}$$

$$H \to \left\{E^H := \text{ The fixed field of } H\right\}$$

$$\left\{\mathrm{Gal}(L/F) := \left\{\sigma \in \mathrm{Gal}(L/k) \;\middle|\; \sigma(F) = F\right\}\right\} \leftarrow F.$$

- This is contravariant with respect to subgroups/subfields.
- $[F : k] = [G : H]$, so degrees of extensions over the base field correspond to indices of subgroups.
- $[K : F] = |H|$
- L/F is Galois and $Gal(K/F) = H$
- F/k is Galois $\iff$ H is normal, and $\mathrm{Gal}(F/k) = \mathrm{Gal}(L/k)/H$.
- The compositum F_1F_2 corresponds to $H_1 \bigcap H_2$.
- The subfield $F_1 \bigcap F_2$ corresponds to H_1H_2.

5.2.2 Examples

1. $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}/(n)^\times$ and is generated by maps of the form $\zeta_n \mapsto \zeta_n^j$ where $(j, n) = 1$.

   I.e., the following map is an isomorphism:

$$\begin{aligned} \mathbb{Z}/(n)^\times &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_n), \mathbb{Q}) \\ r \mod n &\mapsto (\varphi_r : \zeta_n \mapsto \zeta_n^r). \end{aligned}$$

2. $\mathrm{Gal}(\mathbb{GF}(p^n)/\mathbb{F}_p) \cong \mathbb{Z}/(n)$, a cyclic group generated by powers of the Frobenius automorphism:

$$\begin{aligned} \varphi_p : \mathbb{GF}(p^n) &\longrightarrow \mathbb{GF}(p^n) \\ x &\mapsto x^p. \end{aligned}$$

Lemma 5.18.
Every quadratic extension is Galois.

Lemma 5.19.
If K is the splitting field of an irreducible polynomial of degree n, then $\mathrm{Gal}(K/\mathbb{Q}) \leq S_n$ is a transitive subgroup.

Corollary 5.20.
n divides the order $|\mathrm{Gal}(K/\mathbb{Q})|$.

Definition 5.20.1.
TFAE:

- k is a **perfect** field.
- Every irreducible polynomial $p \in k[x]$ is separable
- Every finite extension F/k is separable.
- If char $k > 0$, the Frobenius is an automorphism of k.

Theorem 5.21.

- If char $k = 0$ or k is finite, then k is perfect.
- $k = \mathbb{Q}, \mathbb{F}_p$ are perfect, and any finite normal extension is Galois.
- Every splitting field of a polynomial over a perfect field is Galois.

Proposition 5.22 ***(Composite Extensions).***
If F/k is finite and Galois and L/k is arbitrary, then FL/L is Galois and

$$\mathrm{Gal}(FL/L) = \mathrm{Gal}(F/F \bigcap L) \subset \mathrm{Gal}(F/k).$$

5.3 Cyclotomic Polynomials

Definition 5.22.1 (Cyclotomic Polynomials)**.**
Let $\zeta_n = e^{2\pi i/n}$, then the n**th cyclotomic polynomial** is given by

$$\Phi_n(x) = \prod_{\substack{k=1 \\ (j,n)=1}}^{n} \left(x - \zeta_n^k\right),$$

which is a product over primitive roots of unity. It is the unique irreducible polynomial which is a divisor of $x^n - 1$ but *not* a divisor of $x^k - 1$ for any $k < n$.

Proposition 5.23.
$\deg \Phi_n(x) = \varphi(n)$ for φ the totient function.

Proof .
$\deg \Phi_n(x)$ is the number of nth primitive roots, which is the number of numbers less than and coprime to n.

∎

Computing Φ_n:

1.
$$\Phi_n(z) = \prod_{d \mid n, d>0} \left(z^d - 1\right)^{\mu\left(\frac{n}{d}\right)}$$
where
$$\mu(n) \equiv \begin{cases} 0 & \text{if } n \text{ has one or more repeated prime factors} \\ 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes,} \end{cases}$$

2.
$$x^n - 1 = \prod_{d \mid n} \Phi_d(x) \implies \Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d \mid n \\ d<n}} \Phi_d(x)},$$
so just use polynomial long division.

Lemma 5.24.
$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$
$$\Phi_{2p}(x) = x^{p-1} - x^{p-2} + \cdots - x + 1.$$

Lemma 5.25.
$$k \mid n \implies \Phi_{nk}(x) = \Phi_n\left(x^k\right)$$

Definition 5.25.1.
An extension F/k is **simple** if $F = k[\alpha]$ for a single element α.

Theorem 5.26 ***(Primitive Element).***
Every finite separable extension is simple.

Corollary 5.27.
$\mathbb{GF}(p^n)$ is a simple extension over $\mathbb{F}_p$.

6 Modules

6.1 General Modules

Definition: A module is **simple** iff it has no nontrivial proper submodules.

Definition: A **free** module is a module with a basis (i.e. a spanning, linearly independent set).

Example: $\mathbb{Z}/(6)$ is a $\mathbb{Z}$-module that is *not* free.

Definition: A module M is **projective** iff M is a direct summand of a free module $F = M \oplus \cdots$.

Free implies projective, but not the converse.

Definition: A sequence of homomorphisms $0 \xrightarrow{d_1} A \xrightarrow{d_2} B \xrightarrow{d_3} C \longrightarrow 0$ is *exact* iff $\operatorname{im} d_i = \ker d_{i+1}$.

Lemma: If $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ is a short exact sequence, then

- C free $\implies$ the sequence splits
- C projective $\implies$ the sequence splits
- A injective $\implies$ the sequence splits

Moreover, if this sequence splits, then $B \cong A \oplus C$.

6.2 Classification of Modules over a PID

Let M be a finitely generated modules over a PID R. Then there is an invariant factor decomposition

$$M \cong F \bigoplus R/(r_i) \quad \text{where } r_1 \mathrel{\Big|} r_2 \mathrel{\Big|} \cdots,$$

and similarly an elementary divisor decomposition.

6.3 Minimal / Characteristic Polynomials

Fix some notation:

$$\begin{aligned} \min_A(x) :& \quad \text{The minimal polynomial of } A \\ \chi_A(x) :& \quad \text{The characteristic polynomial of } A. \end{aligned}$$

Definition: The minimal polynomial is the unique polynomial $\min_A(x)$ of minimal degree such that $\min_A(A) = 0$.

Definition: The **characteristic polynomial** of A is given by

$$\chi_A(x) = \det(A - xI)) = \det(SNF(A - xI)).$$

> *Useful lemma:* If A is upper triangular, then $\det(A) = \prod_i a_{ii}$

Theorem (Cayley-Hamilton): The minimal polynomial divides the characteristic polynomial, and in particular $\chi_A(A) = 0$.

Lemma: Writing

$$\min_A(x) = \prod (x - \lambda_i)^{a_i}$$
$$\chi_A(x) = \prod (x - \lambda_i)^{b_i}$$

- $a_i \leq b_i$
- The roots both polynomials are precisely the eigenvalues of A.

> *Proof*: By Cayley-Hamilton, $\min_A$ divides χ_A. Every λ_i is a root of μ_M:
> Let $(\mathbf{v}_i, \lambda_i)$ be a nontrivial eigenpair. Then by linearity,
>
> $$\min_A(\lambda_i)\mathbf{v}_i = \min_A(A)\mathbf{v}_i = \mathbf{0},$$
>
> which forces $\min_A(\lambda_i) = 0$.

Definition: Two matrices A, B are **similar** (i.e. $A = PBP^{-1}$) $\iff$ A, B have the same Jordan Canonical Form (JCF).

Definition: Two matrices A, B are **equivalent** (i.e. $A = PBQ$) $\iff$

- They have the same rank,
- They have the same invariant factors, *and*
- They have the same (JCF)

Finding the minimal polynomial:

Let $m(x)$ denote the minimal polynomial A.

1. Find the characteristic polynomial $\chi(x)$; this annihilates A by Cayley-Hamilton. Then $m(x) \mid \chi(x)$, so just test the finitely many products of irreducible factors.
2. Pick any $\mathbf{v}$ and compute $T\mathbf{v}, T^2\mathbf{v}, \cdots T^k\mathbf{v}$ until a linear dependence is introduced. Write this as $p(T) = 0$; then $\min_A(x) \mid p(x)$.

Definition: Given a monic $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1} + x^n$, the **companion matrix** of p is given by

$$C_p := \begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{bmatrix}.$$

6.4 Canonical Forms

6.4.1 Rational Canonical Form

Corresponds to the **Invariant Factor Decomposition** of T.

Lemma: $RCF(A)$ is a block matrix where each block is the companion matrix of an invariant factor of A.

Derivation:

- Let $k[x] \curvearrowright V$ using T, take invariant factors a_i,
- Note that $T \curvearrowright V$ by multiplication by x
- Write $\overline{x} = \pi(x)$ where $F[x] \xrightarrow{\pi} F[x]/(a_i)$; then span $\{\overline{x}\} = F[x]/(a_i)$.
- Write $a_i(x) = \sum b_i x^i$, note that $V \longrightarrow F[x]$ pushes $T \curvearrowright V$ to $T \curvearrowright k[x]$ by multiplication by $\overline{x}$
- WRT the basis $\overline{x}$, T then acts via the companion matrix on this summand.
- Each invariant factor corresponds to a block of the RCF.

6.4.2 Jordan Canonical Form

Corresponds to the **Elementary Divisor Decomposition** of T.

Lemma: The elementary divisors of A are the minimal polynomials of the Jordan blocks.

Lemma: Writing

$$\min_A(x) = \prod (x - \lambda_i)^{a_i}$$
$$\chi_A(x) = \prod (x - \lambda_i)^{b_i}$$

- $a_i \leq b_i$
- a_i tells you the size of the **largest** Jordan block associated to λ_i,
- b_i is the **sum of sizes** of all Jordan blocks associated to λ_i
- $\dim E_{\lambda_i}$ is the **number of Jordan blocks** associated to λ_i

6.5 Using Canonical Forms

Lemma: The characteristic polynomial is the *product of the invariant factors*, i.e.

$$\chi_A(x) = \prod_{j=1}^{n} f_j(x).$$

Lemma: The minimal polynomial of A is the *invariant factor of highest degree*, i.e.

$$\min_A(x) = f_n(x).$$

Lemma: For a linear operator on a vector space of nonzero finite dimension, TFAE:

- The minimal polynomial is equal to the characteristic polynomial.
- The list of invariant factors has length one.
- The Rational Canonical Form has a single block.
- The operator has a matrix similar to a companion matrix.
- There exists a *cyclic vector* $\mathbf{v}$ such that $\operatorname{span}_k \left\{ T^j \mathbf{v} \;\middle|\; j = 1, 2, \cdots \right\} = V$.
- T has $\dim V$ distinct eigenvalues

6.6 Diagonalizability

Notation: A^* denotes the conjugate tranpose of A.

Lemma: Let V be a vector space over k an algebraically closed and $A \in \operatorname{End}(V)$. Then if $W \subseteq V$ is an invariant subspace, so $A(W) \subseteq W$, the A has an eigenvector in W.

Theorem (The Spectral Theorem):

1. Hermitian matrices (i.e. $A^* = A$) are diagonalizable over $\mathbb{C}$.
2. Symmetric matrices (i.e. $A^t = A$) are diagonalizable over $\mathbb{R}$.

Proof: Suppose A is Hermitian. Since V itself is an invariant subspace, A has an eigenvector $\mathbf{v}_1 \in V$. Let $W_1 = \operatorname{span}_k \{\mathbf{v}_1\}^\perp$. Then for any $\mathbf{w}_1 \in W_1$,

$$\langle \mathbf{v}_1,\ A\mathbf{w}_1 \rangle = \langle A\mathbf{v}_1,\ \mathbf{w}_1 \rangle = \lambda \langle \mathbf{v}_1,\ \mathbf{w}_1 \rangle = 0,$$

so $A(W_1) \subseteq W_1$ is an invariant subspace, etc.
Suppose now that A is symmetric. Then there is an eigenvector of norm 1, $\mathbf{v} \in V$.

$$\lambda = \lambda \langle \mathbf{v},\ \mathbf{v} \rangle = \langle A\mathbf{v},\ \mathbf{v} \rangle = \langle \mathbf{v},\ A\mathbf{v} \rangle = \overline{\lambda} \implies \lambda \in \mathbb{R}.$$

Lemma: $\{A_i\}$ pairwise commute $\iff$ they are all simultaneously diagonalizable.

Proof: By induction on number of operators

- A_n is diagonalizable, so $V = \bigoplus E_i$ a sum of eigenspaces
- Restrict all $n-1$ operators A to E_n.
- The commute in V so they commute in E_n
- **(Lemma)** They were diagonalizable in V, so they're diagonalizable in E_n
- So they're simultaneously diagonalizable by I.H.
- But these eigenvectors for the A_i are all in E_n, so they're eigenvectors for A_n too.
- Can do this for each eigenspace. ■

Full details here

Theorem (Characterizations of Diagonalizability)

M is diagonalizable over $\mathbb{F}$ $\iff$ $\min_M(x, \mathbb{F})$ splits into distinct linear factors over $\mathbb{F}$, or equivalently iff all of the roots of $\min_M$ lie in $\mathbb{F}$.

Proof: $\Longrightarrow$: If $\min_A$ factors into linear factors, so does each invariant factor, so every elementary divisor is linear and $JCF(A)$ is diagonal.
$\Longleftarrow$: If A is diagonalizable, every elementary divisor is linear, so every invariant factor factors into linear pieces. But the minimal polynomial is just the largest invariant factor.

6.7 Matrix Counterexamples

1. A matrix that is:

- Not diagonalizable over $\mathbb{R}$ but diagonalizable over $\mathbb{C}$
- No eigenvalues in $\mathbb{R}$ but distinct eigenvalues over $\mathbb{C}$
- $\min_M(x) = \chi_M(x) = x^2 + 1$

$$M = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \sim \left[\begin{array}{r|r} -1\sqrt{-1} & 0 \\ \hline 0 & 1\sqrt{-1} \end{array}\right].$$

2.

$$M = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

- Not diagonalizable over $\mathbb{C}$
- Eigenvalues $[1, 1]$ (repeated, multiplicity 2)
- $\min_M(x) = \chi_M(x) = x^2 - 2x + 1$

3. Non-similar matrices with the same characteristic polynomial

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

4. A full-rank matrix that is not diagonalizable:

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

5. Matrix roots of unity:

$$\sqrt{I_2} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

$$\sqrt{-I_2} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

6.8 Miscellaneous

Lemma: $I \trianglelefteq R$ is a free R-module iff I is a principal ideal.

Proof: $\implies$:
Suppose I is free as an R-module, and let $B = \{\mathbf{m}_j\}_{j\in J} \subseteq I$ be a basis so we can write $M = \langle B \rangle$.
Suppose that $|B| \geq 2$, so we can pick at least 2 basis elements $\mathbf{m}_1 \neq \mathbf{m}_2$, and consider

$$\mathbf{c} = \mathbf{m}_1\mathbf{m}_2 - \mathbf{m}_2\mathbf{m}_1,$$

which is also an element of M .
Since R is an integral domain, R is commutative, and so

$$\mathbf{c} = \mathbf{m}_1\mathbf{m}_2 - \mathbf{m}_2\mathbf{m}_1 = \mathbf{m}_1\mathbf{m}_2 - \mathbf{m}_1\mathbf{m}_2 = \mathbf{0}_M$$

However, this exhibits a linear dependence between $\mathbf{m}_1$ and $\mathbf{m}_2$, namely that there exist $\alpha_1, \alpha_2 \neq 0_R$ such that $\alpha_1\mathbf{m}_1 + \alpha_2\mathbf{m}_2 = \mathbf{0}_M$; this follows because $M \subset R$ means that we can take $\alpha_1 = -m_2, \alpha_2 = m_1$. This contradicts the assumption that B was a basis, so we must have $|B| = 1$ and so $B = \{\mathbf{m}\}$ for some $\mathbf{m} \in I$. But then $M = \langle B \rangle = \langle \mathbf{m} \rangle$ is generated by a single element, so M is principal.
$\impliedby$:
Suppose $M \trianglelefteq R$ is principal, so $M = \langle \mathbf{m} \rangle$ for some $\mathbf{m} \neq \mathbf{0}_M \in M \subset R$.
Then $x \in M \implies x = \alpha\mathbf{m}$ for some element $\alpha \in R$ and we just need to show that $\alpha\mathbf{m} = \mathbf{0}_M \implies \alpha = 0_R$ in order for $\{\mathbf{m}\}$ to be a basis for M, making M a free R-module.
But since $M \subset R$, we have $\alpha, m \in R$ and $\mathbf{0}_M = 0_R$, and since R is an integral domain, we have $\alpha m = 0_R \implies \alpha = 0_R$ or $m = 0_R$.
Since $m \neq 0_R$, this forces $\alpha = 0_R$, which allows $\{m\}$ to be a linearly independent set and thus a basis for M as an R-module.

■

7 Extra Problems

7.1 Group Theory

7.1.1 Basic Structure

15. Show that any cyclic group is abelian.
16. Show that if $G/Z(G)$ is cyclic then G is abelian.
17. Show that the intersection of two subgroups is again a subgroup.
18. Show that if $G \curvearrowright X$ is a group action, then the stabilizer G_x of a point is a subgroup.
19. Show that $G = H \times K$ iff the conditions for recognizing direct products hold.
20. Show that if $H, K \trianglelefteq G$ and $H \bigcap K = \emptyset$, then $hk = kh$ for all $h \in H, k \in K$.
21. Show that every normal subgroup of G is contained in $Z(G)$.
22. Show that $|G|/|H| = [G : H]$.
23. Show that the order of any element in a group divides the order of the group.
24. Show that $\varphi(n) = n \prod p \mid n\left(1 - \frac{1}{p}\right)$.
25. Show that $Z(G) \subseteq C_G(H) \subseteq N_G(H)$.
26. Show that G/N is abelian iff $[G, G] \leq N$.
27. Give a counterexample where $H, K \leq G$ but HK is not a subgroup of G.
28. Show that if $H, K \trianglelefteq G$ are normal subgroups that intersect trivially, then $[H, K] = 1$ (so $hk = kh$ for all k and h).

29. Give an example showing that normality is not transitive: i.e. $H \trianglelefteq K \trianglelefteq G$ with H *not* normal in G.

7.1.2 Primes in Group Theory

14. Show that any group of prime order is cyclic and simple.
15. Analyze groups of order p^2.
16. Analyze groups of order pq.
17. Show that a group of order pq with $q < p$ and q not dividing $p - 1$ is cyclic of order pq.
18. Analyze groups of order p^2q.
19. Show that no group of order p^2q^2 is simple for $p < q$ primes.
20. Show that a group of order p^2q^2 has a normal Sylow subgroup.
21. Show that a group of order p^2q^2 where q does not divide $p^2 - 1$ and p does not divide $q^2 - 1$ is abelian.
22. Show that every group of order pqr with $p < q < r$ primes contains a normal Sylow subgroup.
23. Show that every p-group is nilpotent.
24. Show that every p-group is solvable.
25. Show that p-groups have nontrivial centers.
26. Show that any normal p- subgroup is contained in every Sylow p-subgroup of G.

7.1.3 p-Groups

- Let $O_P(G)$ be the intersection of all Sylow p-subgroups of G. Show that $O_p(G) \trianglelefteq G$, is maximal among all normal p-subgroups of G
- Let $P \in \mathrm{Syl}_p(H)$ where $H \trianglelefteq G$ and show that $P \bigcap H \in \mathrm{Syl}_p(H)$.
- Show that Sylow p_i-subgroups S_{p_1}, S_{p_2} for distinct primes $p_1 \neq p_2$ intersect trivially.

7.1.4 Classification

10. Show that no group of order 36 is simple.
11. Show that no group of order 90 is simple.
12. Show that all groups of order 45 are abelian.

7.1.5 Group Actions

1. Show that the stabilizer of an element G_x is a subgroup of G.
2. Show that if x, y are in the same orbit, then their stabilizers are conjugate.

7.1.6 Series

6. Show that A_n is simple for $n \geq 5$
7. Give a necessary and sufficient condition for a cyclic group to be solvable.
8. Prove that every simple abelian group is cyclic.

7.1.7 Misc

- Show that the size of a conjugacy class divides the order of a group.

- Show that $\text{Inn}(G) \trianglelefteq Aut(G)$
- Show that $\text{Inn}(G) \cong G/Z(G)$
- Show that the kernel of the map $G \longrightarrow \text{Aut}(G)$ given by $g \mapsto (h \mapsto ghg^{-1})$ is $Z(G)$.
- Show that $C_G(H) \subseteq N_G(H) \leq G$.
- Show that $N_G(H)/C_G(H) \cong A \leq Aut(H)$
- Given $H \subseteq G$, let $S(H) = \bigcup_{g \in G} gHg^{-1}$, so $|S(H)|$ is the number of conjugates to H. Show that $|S(H)| = [G : N_G(H)]$.
  - That is, the number of subgroups conjugate to H equals the index of the normalizer of H.
- Show that $Z(G) = \bigcap_{a \in G} C_G(a)$.
- Show that the centralizer $G_G(H)$ of a subgroup is again a subgroup.
- Show that $C_G(H) \trianglelefteq N_G(H)$ is a normal subgroup.
- Show that $C_G(G) = Z(G)$.
- Show that for $H \leq G$, $C_H(x) = H \bigcap C_G(x)$.

7.1.8 Nonstandard Topics

- Show that H char $G \Rightarrow H \trianglelefteq G$

  Thus "characteristic" is a strictly stronger condition than normality

- Show that H char K char $G \Rightarrow H$ char G

  So "characteristic" is a transitive relation for subgroups.

- Show that if $H \leq G$, $K \trianglelefteq G$ is a normal subgroup, and H char K then H is normal in G.

  So normality is not transitive, but strengthening one to "characteristic" gives a weak form of transitivity.

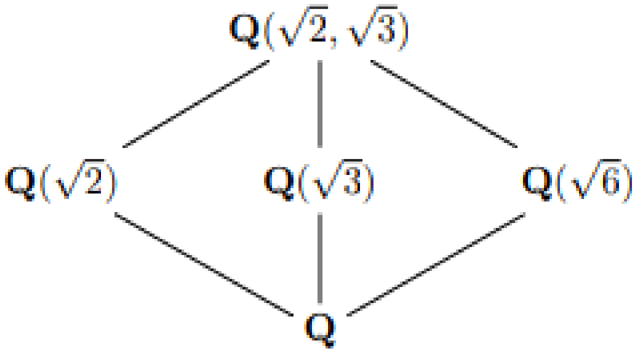
7.2 Ring Theory

1. Show that if $x \in R$ a PID, then x is irreducible $\iff$ $\langle x \rangle \trianglelefteq R$ is maximal.

7.3 Field Theory

1. What is $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}]$?
2. What is $[\mathbb{Q}(2^{\frac{3}{2}}) : \mathbb{Q}]$?
3. Show that every field is simple.
4. Show that any field morphism is either 0 or injective.
5. Show that if $p \in \mathbb{Q}[x]$ and $r \in \mathbb{Q}$ is a rational root, then in fact $r \in \mathbb{Z}$.
6. If $\{\alpha_i\}_{i=1}^n \subset F$ are algebraic over K, show that $K[\alpha_1, \cdots, \alpha_n] = K(\alpha_1, \cdots, \alpha_n)$.
7. Show that the Galois group of $x^n - 2$ is D_n, the dihedral group on n vertices.

8. Compute all intermediate field extensions of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, show it is equal to $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, and find a corresponding minimal polynomial.



9. Compute all intermediate field extensions of $\mathbb{Q}(2^{\frac{1}{4}}, \zeta_8)$.
10. Show that $\mathbb{Q}(2^{\frac{1}{3}})$ and $\mathbb{Q}(\zeta_3 2^{\frac{1}{3}})$
11. Show that if L/K is separable, then L is normal $\iff$ there exists a polynomial $p(x) = \prod_{i=1}^{n} x - \alpha_i \in K[x]$ such that $L = K(\alpha_1, \cdots, \alpha_n)$ (so L is the splitting field of p).
12. Is $\mathbb{Q}(2^{\frac{1}{3}})/\mathbb{Q}$ normal?
13. Show that any finite integral domain is a field.
14. Prove that if R is an integral domain, then $R[t]$ is again an integral domain.
15. Show that $ff(R[t]) = ff(R)(t)$.
16. Prove that $x^{p^n} - x$ is the product of all monic irreducible polynomials in $\mathbb{F}_p[x]$ with degree dividing n.
17. Prove that an irreducible $\pi(x) \in \mathbb{F}_p[x]$ divides $x^{p^n} - x \iff \deg \pi(x)$ divides n.
18. Show that a field with p^n elements has exactly one subfield of size p^d for every d dividing n.
19. Show that $\mathbb{GF}(p^n)$ is the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$.
20. Show that $x^{p^d} - x \mid x^{p^n} - x \iff d \mid n$
21. Show that $\mathbb{GF}(p^d) \leq \mathbb{GF}(p^n) \iff d \mid n$
22. Show that $x^{p^n} - x = \prod f_i(x)$ over all irreducible monic f_i of degree d dividing n.
23. Compute the Galois group of $x^n - 1 \in \mathbb{Q}[x]$ as a function of n.
24. Identify all of the elements of the Galois group of $x^p - 2$ for p an odd prime (note: this has a complicated presentation).
25. Classify the five groups of order 12.
26. Classify the four groups of order 28.
27. Show if G is finite, then G is solvable $\iff$ all of its composition factors are of prime order.
28. Show that if N and G/N are solvable, then G is solvable.
29. Show that S_n is generated by disjoint cycles.
30. Show that S_n is generated by transpositions.
31. Show that an m-cycle is an odd permutation iff m is an even number.
32. Show that a permutation is odd iff it has an odd number of even cycles.
33. Prove Burnside's theorem.
34.

7.4 Modules and Linear Algebra

1. Prove the Cayley-Hamilton theorem.
2. Prove that the minimal polynomial divides the characteristic polynomial.
3. Prove that the cokernel of $A \in \mathrm{Mat}(n \times n, \mathbb{Z})$ is finite $\iff$ $\det A \neq 0$, and show that in this case $|\mathrm{coker}(A)| = |\det(A)|$.
4. Show that a nilpotent operator is diagonalizable.
5. Show that if A, B are diagonalizable and $[A, B] = 0$ then A, B are simultaneously diagonalizable.
6. Does diagonalizable imply invertible? The converse?

7.5 Commutative Algebra

1. Show that a finitely generated module over a Noetherian local ring is flat iff it is free using Nakayama and Tor.

8 List of Topics

Chapters 1-9 of Dummit and Foote

- Left and right cosets
- Lagrange's theorem
- Isomorphism theorems
- Group generated by a subset
- Structure of cyclic groups
- Composite groups
  - HK is a subgroup iff $HK = KH$
- Normalizer
  - $HK \leq H$ if $H \leq N_G(K)$
- Symmetric groups
  - Conjugacy classes are determined by cycle types
- Group actions
  - Actions of G on X are equivalent to homomorphisms from G into Sym(X)
- Cayley's theorem
- Orbits of an action
- Orbit stabilizer theorem
- Orbits act on left cosets of subgroups
- Subgroups of index p, the smallest prime dividing $|G|$, are normal
- Action of G on itself by conjugation
- Class equation
- p-groups
  - Have non trivial center
- p^2 groups are abelian
- Automorphisms, the automorphism group
  - Inner automorphisms
  - $Inn(G) \cong Z/Z(G)$
  - $Aut(S_n) = Inn(S_n)$ unless $n = 6$
  - $Aut(G)$ for cyclic groups

- $G \cong Z_p^n$, then $Aut(G) \cong GL_n(Z_p)$
- Proof of Sylow theorems
- A_n is simple for $n \geq 5$
- Recognition of internal direct product
- Recognition of semi-direct product
- Classifications:
    - pq
- Free group & presentations
- Commutator subgroup
- Solvable groups
    - S_n is solvable for $n \leq 4$
- Derived series
    - Solvable iff derived series reaches e
- Nilpotent groups
    - Nilpotent iff all sylow-p subgroups are normal
    - Nilpotent iff all maximal subgroups are normal
- Upper central series
    - Nilpotent iff series reaches G
- Lower central series
    - Nilpotent iff series reaches e
- Fratini's argument
- Rings
    - I maximal iff R/I is a field
    - Zorn's lemma
    - Chinese remainer theorem
    - Localization of a domain
    - Field of fractions
    - Factorization in domains
    - Euclidean algorithm
    - Gaussian integers
    - Primes and irreducibles
    - Domains
        - Primes are irreducible
    - UFDs
        - Have GCDs
        - Sometimes PIDs
    - PIDs
        - Noetherian
        - Irreducibles are prime
        - Are UFDs
        - Have GCDs
    - Euclidean domains
        - Are PIDs
    - Factorization in $Z[i]$
    - Polynomial rings
    - Gauss' lemma
    - Remainder and factor theorem
    - Polynomials

- Reducibility
- Rational root test
- Eisenstein's criterion

9 Groups

9.1 Definitions

9.1.1 Subgroup Generated by a set A

- $\langle A \rangle = \{a_1^{\pm 1}, a_2^{\pm 1}, \cdots a_2^{\pm 1} : a_i \in A, n \in \mathbb{N}\}$
- Equivalently, the intersection of all H such that $A \subseteq H \leq G$

9.2 Numeric Results

9.2.1 Cauchy's Theorem

- For any p dividing $|G|$, there is a subgroup of order p.

9.2.2 Sylow Theorems: $|G| = p^k m$ where $p \not| m$

- At least one Sylow-p subgroup always exists: $\exists P \leq G$ with $|P| = p^k$
- All such subgroups are conjugate: $\forall P, P', \exists g \in G : gPg^{-1} = P'$
- n_p satisfies:
  - n_p divides $m = [G : P]$
  - $n_p = 1 \bmod p$
  - $n_p = [G : N_G(P)]$ (Not as useful)
- Every p-subgroup of G is a p-subgroup of P (i.e. P is maximal and contains all subgroups of order p^l with $l \leq k$)

9.2.3 Orbit-stabilizer Theorem

- Given a group action, $G/G_x \cong \mathcal{O}_x$
- Gives the numeric result $|\mathcal{O}_x| = |G/G_x| = [G : G_x] = \dfrac{|G|}{|G_x|}$
- Also useful in the form $|G| = |\mathcal{O}_x||G_x|$
- Proof:
  - Use the map

$$\begin{aligned} \varphi : G &\to X \\ g &\mapsto g \sim x \end{aligned}$$

  Where $\mathrm{im}\varphi = \mathcal{O}_x$ and $\ker\varphi = G_x$.

9.2.4 Burnside's Lemma

- $$|X_G| = \frac{1}{|G|}\sum_{g\in G}|X^g|$$
  - $|X_G|$ is the number of orbits
  - $X^g = \{x \in X : g \sim x = x\}$

9.2.5 The class equation

- $$|G| = |Z(G)| + \sum_{a\in A}[G : C_G(a)]$$
  - Where $A = \{a_1, a_2, \ldots, a_n : a_1 \in [a_1], a_2 \in [a_2], \ldots\}$ is a set containing one element from each conjugacy class
  - $[G : C_G(a)]$ is the number of elements in $[a]$
  - Each element in $Z(G)$ has a singleton conjugacy class

9.2.6 General facts

- $|G| = p \Rightarrow G$ is cyclic
- $|G| = p^e \Rightarrow Z(G) \neq e$
- $|G| = p^e$ (P-groups)
  - $Z(G) \neq \{e\}$ (Use class equation)
- $|G| = p$
  - Always cyclic
    - Proof: Any nontrivial cyclic subgroup's order is > 1 and divides p, so equals p.
- $|G| = p^2$
  - Always abelian
    - Proof: $|G/Z(G)| = 1, p$. If p, it's cyclic, and G is abelian. Otherwise it's 1, so $G = Z(G)$.
  - Two possibilities:
    - Z_{p^2} (cyclic)
    - $Z_p \times Z_p$
- $|G| = pq$
  - $p \not\Big| \, q - 1 (q \neq 1 \mod p)$:
    - One possibility:
      - $G \cong Z_{pq}$ (cyclic)
    - Facts:
      - $\exists P \trianglelefteq G$ (A Sylow-P subgroup)

- p divides $q-1$ ($q = 1 \bmod p$):
  - Two possibilities:
    - $G \cong Z_{pq}$ (cyclic)
    - $G \cong Z_q \rtimes Z_p$
- Never simple

- $|G| = p^2q$
  - $\exists P \trianglelefteq G$ (A Sylow-P subgroup)
- $|G| = p_1p_2p_3$ (distinct)
  - Not simple

9.3 Common Groups

9.3.1 S_3

$S_3 = \langle (12), (23), (13) \rangle$

- $Z(S_3) = e$
- $Aut(S_3) = Inn(S_3)$, since

$$\begin{aligned} Z(G) = e = \ker\psi \\ \Rightarrow Out(S_3) = Inn(S_3) \\ \Rightarrow Aut(S_3) \cong S_3 \end{aligned}$$

9.3.2 S_n

$S_n, n \geq 4$

- $Z(S_n) = e$
  - Let $\sigma(a) = b$, choose $\tau = (bc)$ so $\tau\sigma(a) = \tau(b) = c \neq b = \sigma(a0 = \sigma\tau(a)$
- Conjugacy classes are determined entirely by cycle structure
  - There are exactly $p(n)$ of them (partition function)
- Disjoint cycles commute
- $\sigma \circ (a_1 \cdots a_k) \circ \sigma^{-1} = (\sigma(a_1), \cdots \sigma(a_k))$
- Every element is a product of disjoint cycles
- Every element is a product of transpositions
  - A cycle of length k can be written as $k-1$ transpositions
  - Parity of the cycle equals the parity of $k-1$.
- The order of an element is the lcm of the size of the cycles.

9.3.3 A_n

- Simple for $n \geq 5$
- Index 2 in S_n, so $A_n \trianglelefteq Sn$

9.3.4 D_n

- $\left\langle a, b \,\middle|\, a^n = b^2 = 1, bab^{-1} = a^{-1} \right\rangle \cong \langle r, s \rangle$
- D_n/N is always another dihedral group for any $N \trianglelefteq D_n$
- All subgroups:
  - $\left\langle r^d \right\rangle \cong Z_{n/d}$ where d divides n (index $2d$)
  - $\left\langle r^d, r^i s \right\rangle \cong D_{\frac{n}{d}}$ where d divides n and $0 \leq i \leq d-1$ (index d)
    * All dihedral

10 Rings

10.1 Facts about ideals:

- Intersections, products, and sums of ideals are ideals
- Not necessarily unions
- Every ring has proper maximal ideals
- Apply Z.L. to $\{I \trianglelefteq R : I \neq R\}$
- Every proper ideal is contained in a maximal ideal

10.2 Maximal ideals

$I \trianglelefteq R$ *maximal* if $\nexists J \trianglelefteq R : I \subset J \subset R$

- Every nonzero ring has a maximal ideal (Krull's Theorem)
- R commutative $\implies R/I$ a field
- Union of maximal ideals $= R - R^\times$
- $(X - a) \trianglelefteq R[X]$ is maximal for $a \in R$

10.3 Prime ideals

$I \trianglelefteq R$ *prime* when $pq \in I \implies p \in I \vee q \in I$

- I prime $\iff R/I$ an integral domain,
- (maximal $\implies$ prime)
- $\text{rad}(I^n) = I$

10.4 Radicals

$I \trianglelefteq R$ *radical* when $\forall a \in R, a^n \in I \implies a \in I$

- The nilradical: $\text{nilrad}(I) = \bigcap P$ such that $P \trianglelefteq R$ is prime
- $\text{rad}(I) = \{x \in \,\Big|\, \exists n : x^n \in I\}$
- $\text{rad}(0) = \text{nilrad}(R)$
- $\text{rad}(IJ) = \text{rad}(I) \bigcap \text{rad}(J)$
- $\text{rad}(I) = \bigcap J$ such that $I \subset J, J$ prime (i.e. intersection of all prime ideals containing I)

10.5 Other ideals

- $I \trianglelefteq R$ *primary* when $pq \in I \implies a \in I \vee \exists n \in \mathbb{N} : b^n \in I$
- Prime $\implies$ primary
- $I \trianglelefteq R$ *principal* when $\exists a \in R : I = \langle a \rangle$
- $I \trianglelefteq R$ *irreducible* when $\nexists \{J \trianglelefteq R : I \subset J\} : I = \bigcap J$
- $I \subset R \iff 1, u \notin I \; (u \in R^{\times})$
- $\{I : I \trianglelefteq R\}$ is a poset
- Zorn's lemma can be applied to $\{I \trianglelefteq R : 1 \notin I\}$
- Every proper ideal is contained in a maximal ideal.
- Facts about units
- $R^{\times}$ is closed under multiplication, but *not* under addition.
- $R - R^{\times}$ an additive group $\iff$ R is a local ring
- Integral Domain
- Principal Ideal Domain
- (Prime $\implies$ maximal) $\implies$ UFD
- Unique Factorization Domain
- Field
- When (0) is the only proper ideal
- R/M a field $\iff$ M maximal
- Localization
- Zorn's Lemma: For every poset P, every chain in P has an upper bound $\implies$ P has a maximal element.
- Noetherian: Every ideal is finitely generated
- iff the ascending chain condition for ideals holds

10.6 Orders less than 16:

(Normal: Diamond, grouped by conjugacy class)

- 1 (The trivial group)
  - $Z_1 = \{e\}$
- 2 (One group)
  - $Z_2 \cong Z_3^{\times} \cong Z_4^{\times} \cong Z_6^{\times}$
    $= \{e, a\}$
    * Cyclic

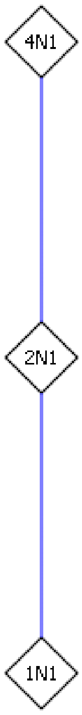


Figure 1: img

    * One element of order 2

- 3 (One group)
  - $Z_3 \cong A_3$
    $\cong \{(), (123), 132)\}$
    * Cyclic
    * One element of order 3
- 4 *(Two groups, both abelian)*
  - $Z_4 \cong Z_5^\times \cong Z_8^\times \cong Z_{10}^\times \cong Z_{12}^\times$
    * Cyclic
    * One element of order 4
  - $Z_2 \times Z_2 \cong V_4 \cong D_2 \cong Z_8^\times$, which are all isomorphic to $\left\langle a, b \,\middle|\, a^2 = b^2 = (ab)^2 = e \right\rangle \cong \langle (12)(34), (13)(24), (14)(23) \rangle$
    * Not cyclic, but abelian
    * All elements have order 2
    * $V_4 \trianglelefteq A_4 \leq S_4$
- 5 (One group)

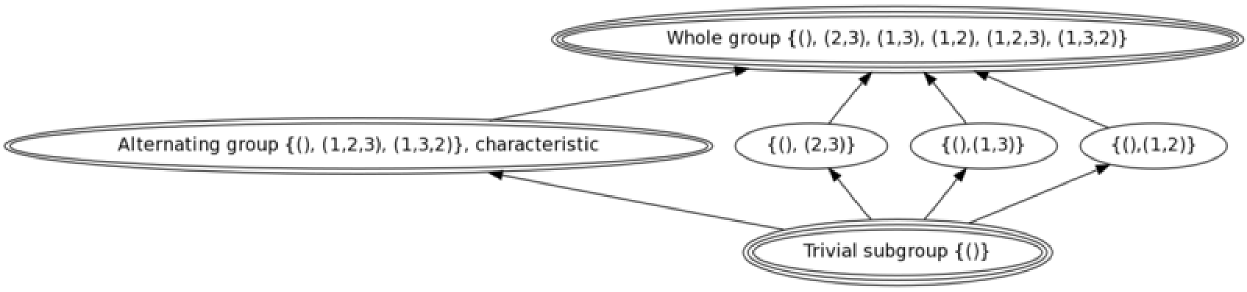


Figure 2: File:S3latticeofsubgroups.png

- Z_5
  - Cyclic, one element of order 5
- 6 *(Two groups)*
  - $Z_6 \cong Z_7^\times \cong Z_9^\times \cong Z_{14}^\times$
    - Cyclic, one element of order 6
  - $S_3 \cong D_6$ $\cong \left\langle a, b, c \,\middle|\, a^2 = b^2 = c^3 = abc = e \right\rangle$
    - Non-abelian (smallest one)
- 7 (One group)
  - Z_7
    - Cyclic, one element of order 7
- 8 **(Five groups)**

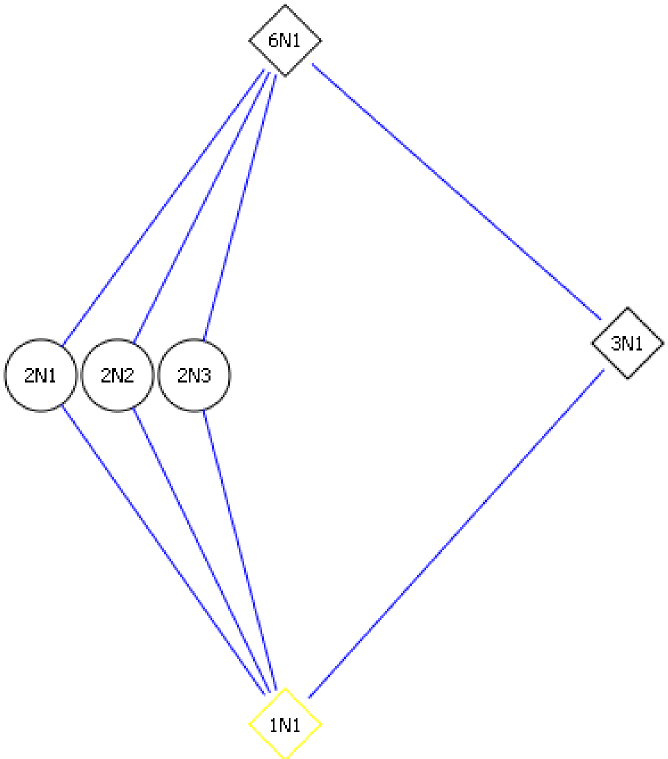
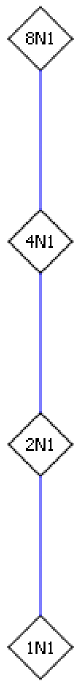
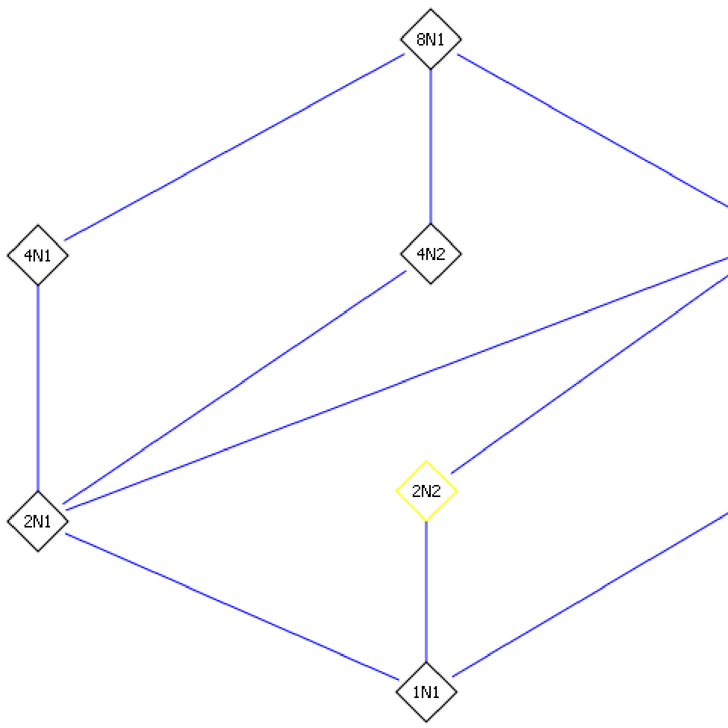


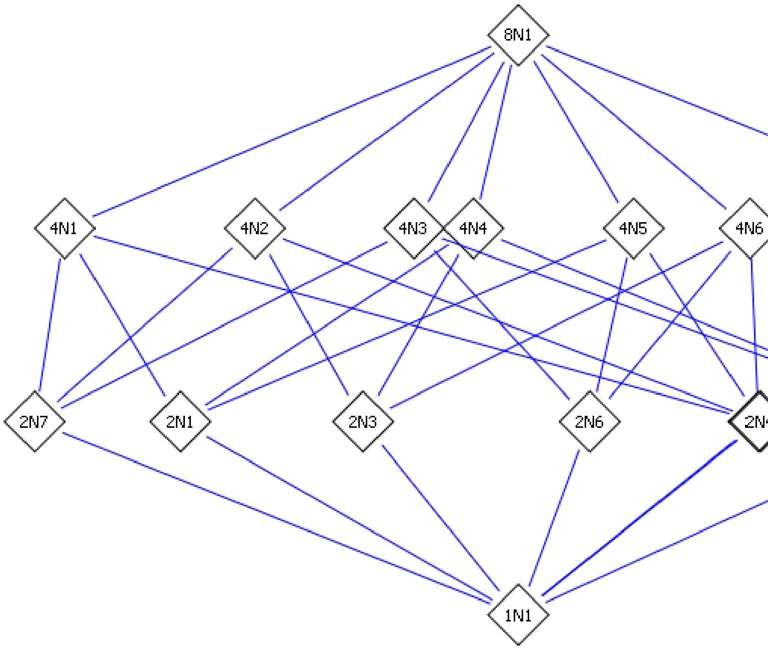
Figure 3: img



- $Z_8 \cong Z_{15}^{\times} \cong Z_{16}^{\times}$ (cyclic)
- $Z_2 \times Z_4$

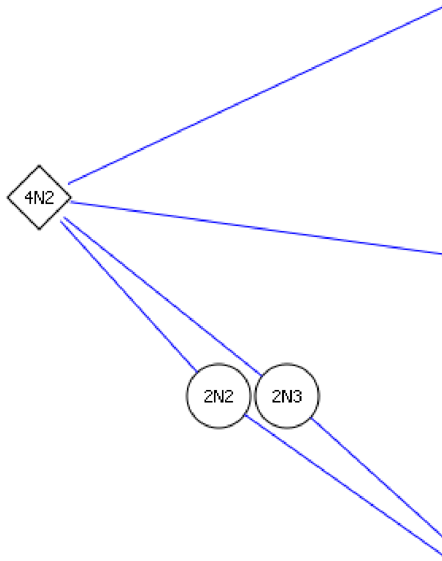


  * Abelian, one element of order 4
- $Z_2 \times Z_2 \times Z_2$



  * Abelian, every element has order 2

- $D_8 \cong \left\langle r, s \,\middle|\, r^4 = s^2 = e, srs^{-1} = r^{-1} \right\rangle$

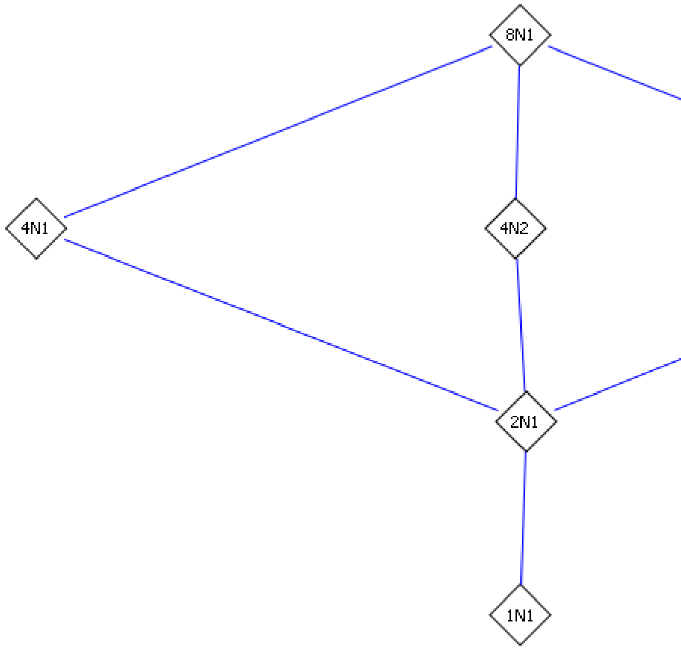


  $\cong \{(), (1234), (13)(24), (1432), (13)(24), (14)(23), (12)(34)\} \leq S_4$

- $Q_8 \cong \left\langle i, j, k \,\middle|\, i^2 = j^2 = k^2 = ijk \right\rangle$

  $\cong \left\langle a, b, c \,\middle|\, a^4 = b^4 = e, a^2 = b^2, ba = a^3 b \right\rangle$

    * Every element has order 4



    * All subgroups are normal, but not abelian

- 9 *(Two groups)*
  - Z_9
  - $Z_3 \times Z_3$
- 10 *(Two groups)*
  - $Z_{10} \cong Z_{11}^{\times}$
  - D_{10}
- 11 (One group)
  - Z_{11}
- 12 **(Five groups)**
  - $Z_{12} \cong Z_{13}^{\times}$
- 13 (One group)
  - Z_{13}
- 14 *(Two groups)*
  - Z_{14}
- 15 (One group)
  - Z_{15}
- 16 ***(Fourteen groups!)***