Theorem Reference

Chen Xu

December 14, 2020

Lecture Notes

Theorem 1. A monomorphism is injective, and an epimorphism is surjective.

Definition 2. $\hookrightarrow$ is injective, $\twoheadrightarrow$ is surjective.

Definition 3. There are several interesting matrix groups:
1. $M_n(\mathbb{R})$ is the group of all $n \times n$ matrices under addition.
2. $\mathrm{GL}_n(\mathbb{R})$ is the group of all invertible $n \times n$ matrices.
3. $\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) | \det A = 1\}$
4. $O_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) | AA^T = I\}$
5. $\mathrm{SO}_n(\mathbb{R}) = \{A \in \mathrm{SL}_n(\mathbb{R}) | AA^T = I\}$

Definition 4. An exact sequence $G_i \xrightarrow{f_i} G_{i+1} \xrightarrow{f_{i+1}}$ is exact iff $(\forall i) \ker f_{i+1} = \operatorname{Im} f_i$

Definition 5. A short exact sequence is one of the form

$$1 \to G_1 \xrightarrow{f} G_2 \xrightarrow{g} G_3 \to 1$$

In other words:
1. f is a monomorphism
2. g is an epimorphism
3. $\operatorname{Im} f = \ker g$

Sometimes referenced as "s.e.s."

Theorem 6. If $H \lhd G$, then

$$1 \to H \to G \to G/H \to 1$$

is a short exact sequence, and all short exact sequences of this form for some H, G.

Theorem 7. *Cayley's Theorem*: Every group G is isomorphic to $S(G)$, or the symmetric group acting on elements of G.

Theorem 8. First Isomorphism Theorem. If $f : G \to G'$ is a group homomorphism, then there exists a canonical isomorphism from $G/\ker f \xrightarrow{\sim} G'$.

Theorem 9. Second Isomorphism Theorem. If $H \lhd G$, and $K < G$, then:
1. $H \cap K \lhd K$
2. $H \cap K < H$
3. $H \lhd HK$
4. $K/(H \cap K) \cong HK/H$

Theorem 10. Third Isomorphism Theorem. For any $H \lhd G$
1. There exists a one to one mapping between subgroups of G containing H and subgroups of G/H. This mapping preserves normality and subgroup relations.
2. $K \lhd H \lhd G \implies (H/K) \lhd (G/K)$
3. $(G/K)\Big/(H/K) \cong G/H$

Group Actions

Definition 11. An action is *faithful* if $G \to S(X)$ is a monomorphism.

Definition 12. An action is *transitive* if $\forall x, y \in X$, $\exists g \in Gy = gx$.

Definition 13. The orbit of x is

$$Gx = \{gx | g \in G\}$$

Definition 14. The *isotropy group* or *stabilizer* of $x \in X$ is

$$\mathrm{Stab}_G(x) = \{g \in G | gx = x\}$$

Definition 15. The *centralizer* of $x \in X$, is simply the isotropy group under the conjugation action

$$G_x = C_G(x) = \{g | gxg^{-1} = x\}$$

Theorem 16. $G/G_x \xrightarrow{\sim} Gx$, where it's only a bijection of sets and not a homomorphism

Theorem 17. The *orbit stabilizer* theorem says that for any group action

$$[G : \mathrm{Stab}_G(g)] = \mathrm{Orb}_G(g)$$

Theorem 18. Class formula

$$|X| = \sum_{x_i \text{ orbit representatives}} [G : G_{x_i}]$$

Definition 19. The *normalizer* of H is the stabilizer of the conjugation action on subgroups of G

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

Definition 20. The *center* of G is

$$Z(G) = \{h \in G | \forall g \in G, gh = hg\}$$

or the intersection of all centers of G ($\bigcap_{g \in G} C_G(g)$)

Definition 21. A p-group is a group of size p^k for some k.

Definition 22. A Sylow subgroup $H < G$ is a subgroup where $|H| = p^n$ and $(|H|, |G/H|) = 1$. In other words, it is the p-subgroup of "max order".

Theorem 23. *Sylow I*: If $p \mid |G|$, then there exists a p-Sylow subgroup in G.

Theorem 24. *Sylow II*

1. Any 2 Sylow subgroups are conjugate
2. Any p-subgroup is also a subgroup of a p-Sylow subgroup

Theorem 25. *Sylow III*: If N_p is the number of p-Sylow subgroups, then

1. $N_p \equiv 1 \pmod p$
2. $N_p \mid |G|$
3. $N_p = 1 \iff$ Sylow subgroup is normal

Definition 26. A short exact sequence (5)

$$1 \to H \to G \xrightarrow{p} K \to 1$$

is *split* if there exists some $i : K \to G$ such that $p \circ i = \mathrm{id}_K$.

Theorem 27. A short exact sequence given subgroups $H, K \triangleleft G$

$$1 \to H \to G \to K \to 1$$

splits if and only if $G \cong H \times K$.

Theorem 28. $G \equiv A \times B$ if and only if

1. $A, B \lhd G$
2. $A \cap B = \{e\}$
3. $AB = G$

Definition 29. For some implied group action $\varphi : H \to \mathrm{Aut}_{\mathrm{gr}}(N)$, we sometimes use the notation ${}^{h}n$ to denote $\varphi(h)(n)$

Definition 30. The *semidirect product* given groups N, H and a group action $\varphi : H \times N \to N$ is defined as the product except with the group operation as

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1\varphi(h_1, n_2), h_1h_2)$$

and is denoted $N \rtimes_\varphi H$. Oftentimes the $_\varphi$ is dropped because it is implied (or is conjugation).

The inverse of (n, h) is $(\varphi(h^{-1}, n^{-1}), h^{-1})$

Theorem 31. If $G = N \rtimes_\varphi H$. Then $N \lhd G$, $H < G$, and $N \lhd H$. Additionally, conjugation by elements in H corresponds to the group action φ.

Theorem 32. If $N, H < G$. Then the following are equivalent:

1. $G \cong N \rtimes H$ considering the action when H acts on N via conjugation.
2. $N \lhd G$, $N \cap H = \{e\}$, $NH = G$
3. $\exists \pi : G \to H$ such that
$$H \xrightarrow{i_H} G \xrightarrow{\pi} H$$
and $\pi \circ i_H = \mathrm{id}$ and $N = \ker \pi$.
4. There exists a split short exact sequence
$$1 \to N \to G \xrightarrow{\pi} H \to 1$$

Definition 33. A *filtration* of a group G is a tower of subgroups

$$\cdots < G_2 < G_1 < G_0 = G$$

There are a couple different kinds of filtrations:

1. *Finite*: If $G_n = \{e\}$ for some n
2. *Normal*: If $G_i \lhd G_{i-1}$
3. *Abelian*: If normal and G_{i-1}/G_i is abelian

Definition 34. The *commutator* of two elements $x, y \in G$ is

$$[x, y] = xyx^{-1}y^{-1}$$

For two subgroups $G_1, G_2 < G$, the commutator subgroup is

$$[G_1, G_2] \coloneqq \big\langle [x, y] : x \in G_1, y \in G_2 \big\rangle$$

(Note that the set of commutators is not a subgroup in general)

Lemma 35. If $H, K \lhd G$, then $[H, K] \lhd G$.

Definition 36. $[G, G]$ is the *commutator subgroup*, or *derived subgroup* of G.

Theorem 37. $G/[G, G]$ is abelian.

Definition 38. Let $G^{(0)} = G$, and $G^{(1)} = [G, G]$. Define $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$. Then the *derived series* is the filtration

$$\cdots < G^{(2)} < G^{(1)} < G^{(0)} = G$$

Note this is an abelian filtration, and $G^{(i)} \lhd G$.

Lemma 39. If G is a finite group with abelian filtration, then G has a normal filtration with cyclic quotients.

Theorem 40.
1. $G/[G,G]$ is abelian
2. $$[G,G] = \bigcap_{G/N \text{ is abelian}} N$$
3. The following universal property holds:

$$\begin{tikzcd} G \arrow[rr, two heads, "f"] \arrow[dr, "\pi"'] & & A \\ & G\big/[G,G] \arrow[ur, dashed, "\exists!\widetilde{f}"'] & \end{tikzcd}$$

where A is an abelian group, and $f = \widetilde{f} \circ \pi$

Definition 41.
1. $G_{\text{ab}} = G/[G,G]$, and is known as the *abelization* of G.
2. G is *perfect* if $G = [G,G]$

Theorem 42. The following are equivalent
1. There exists a finite normal series in G with abelian quotients.
2. There exists a finite normal series in G with abelian quotients and $G_i \lhd G$, for each element G_i in the series.
3. The derived series terminates at e.

Definition 43. G is *solvable* if any of the equivalent conditions in theorem 42 are satisfied.

Definition 44. $H < G$ is *central* if $H < Z(G)$

Lemma 45. $H < K < G$. Then $H \lhd G$ and $K/H < Z(G/H)$ if and only if $[G,K] < H$.

Definition 46. A filtration $\cdots < G_i < G_{i-1} \cdots < G$ is *central* if it satisfies one of the following equivalent conditions:
1. $G_i \lhd G, G_i/G_{i+1} < Z(G/G_{i+1})$
2. $[G_i, G] < G_{i+1}$.

Definition 47. The *descending central series* for G is

$$\cdots < \Gamma_2 < \Gamma_1 < G$$

where $\Gamma_1 = [G,G]$ and $\Gamma_i = [\Gamma_{i-1}, G]$

Definition 48. The *ascending central series* for G is

$$e = Z_0 < Z_1 < \cdots < G$$

where $Z_1 = Z(G)$, and Z_i is the group such that $Z_i \lhd G$ and $Z_i/Z_{i-1} = Z(G/Z_{i-1})$.

Theorem 49. The following are equivalent
1. There exists a finite central series for G
2. The descending central series terminates at e
3. The ascending central series terminates at G

Definition 50. G is *nilpotent* if it satisfies one of the conditions of theorem 49

Theorem 51. If $G_1, \ldots, G_n$ is nilpotent, then so is $G_1 \times \cdots \times G_n$.

Theorem 52. If G is nilpotent, and $H \lneqq G$, then $H \lneqq N_G(H)$.

Theorem 53. If P is a Sylow subgroup of G, then $N_G(N_G(P)) = N_G(P)$

Theorem 54. If G is a p-group, then G is nilpotent.

Theorem 55. If G is nilpotent, then $G \cong P_1 \times P_2 \times \cdots \times P_n$ where $P_1, \ldots, P_n$ are the Sylow subgroups of G

Definition 56. G is *simple* if it does not have proper nontrivial normal subgroups.

Definition 57. A normal series

$$e = G_0 < G_1 < \cdots < G_n = G$$

is a *composition series* (or *Jordan Holder series*) if G_i/G_{i-1} is simple.

Remark 58. Solvable groups have composition series

Definition 59. Let $\cdots < G_i < G_{i+1} < \cdots < G$ is a normal series.

A *refinement* is then any normal series which contains $\ldots, G_i, G_{i+1}, \ldots$ in the same order, but with an additional subgroup different than all the G_i.

Definition 60. Two normal series are *equivalent* if there is a one to one correspondence between intermediate nontrivial factors such that the corresponding factors are isomorphic.

Theorem 61. *Jordan Holder*: Any two composition series are equivalent.

Lemma 62. *Zassenhaus*: If $H_1 \triangleleft H < G$ and $K_1 \triangleleft K < G$, then:

1. $H_1(H \cap K) \triangleright H_1(H \cap K_1)$
2. $K_1(H \cap K) \triangleright K_1(H_1 \cap K)$
3. $\frac{H_1(H \cap K)}{H_1(H \cap K_1)} \cong \frac{K_1(H \cap K)}{K_1(H_1 \cap K)}$

Theorem 63. *Schreier*: For a group G, any two normal series have equivalent refinements.

Free Groups

Definition 64. Given an alphabet X, a *word* is a sequence of elements from $X \amalg X^{-1}$.

Definition 65. Two words u, v are equivalent ($u \sim v$) if we can get v from u by adding or removing elements of the form xx^{-1}.

Definition 66. The *free group* on X is the set of words $F(X)$, where the group operation is concatenation.

Definition 67. If W is a set of words on X, then we consider the free group $\langle X|W\rangle$ as the group of words on X where two words u, v are equivalent if there is a way to get from v to u by adding or removing elements of W or elements xx^{-1}.

Remark 68. $\langle X|W\rangle$ is a group with respect to concatenation.

Remark 69. $F(X) = \langle X|\varnothing\rangle$

Remark 70. All elements in $F(X)$ have a *reduced form*, which is of the form

$$x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$$

Theorem 71. Let $X = \{x_i\}_{i \in I}$ and W is a set of words on X. Let G be a group generated by $\{g_i\}_{i \in I}$ such that for all $w = x_{i_1} x_{i_2} \ldots x_{i_n} \in W$ that $g_{i_1} g_{i_2} \ldots g_{i_n} = e$. Then there exists a unique surjective group homomorphism from $\langle X|W\rangle$ to G, being $x_i \mapsto g_i$.

Theorem 72. Let X be a set and G be a group, and $\varphi : X \to G$ be a map of sets. Then there exists a unique group homomorphism $\widetilde{\varphi} : F(X) \to G$ such that

$$\begin{tikzcd}
X \arrow[r, "\varphi"] \arrow[d, "x \mapsto x"'] & G \\
F(X) \arrow[ur, "\widetilde{\varphi}"'] &
\end{tikzcd}$$

commutes

Theorem 73. For any G, there exists a free group $F(X)$ such that $F(X) \twoheadrightarrow G$.

Definition 74. For two groups $G_1 = \langle X_1 | W_1 \rangle$ and $G_2 = \langle X_2 | W_2 \rangle$, the *free product* is defined to be

$$G_1 * G_2 = \langle X_1 \amalg X_2 | W_1 \cup W_2 \rangle$$

Definition 75. For groups $A = \langle X_A | W_A \rangle$ and $B = \langle X_B | W_B \rangle$, $H = \langle X_h | W_H \rangle$, the *amalgamated free product* $A *_H B$ is defined to be

$$\langle X_A \amalg X_B | W_A \cup W_B \cup \{\varphi(x) = \psi(x)\}_{x \in X_H} \rangle$$

Remark 76. If $N \subset A * B$ is the minimal normal subgroup containing all words $\varphi(x)\psi(x^{-1})$ for $x \in X_H$, then $\frac{A*B}{N} \cong A *_H B$

Theorem 77. For all commutative diagrams

$$\begin{tikzcd}
H \arrow[r, "\varphi"'] \arrow[d, "\psi"] & A \arrow[d] \arrow[ddr, bend left] & \\
B \arrow[r] \arrow[drr, bend right] & A *_H B \arrow[dr, dashed, "\exists! f"'] & \\
 & & G
\end{tikzcd}$$

there exists a unique f such that the diagram commutes.

Remark 78. The free product is a final object in the category of groups.

Theorem 79. $A *_H B$ is unique up to unique isomorphism.

Rings and Fields

Definition 80. A *ring* R satisfies the following properties

1. $(R, +)$ is an abelian group
2. Multiplication is associative
3. The operations work with distributivity and are both associative.

A ring is said to have a *unit* if it has an element 1 such that $1 \cdot a = a \cdot 1$ for all $a \in R$.

A ring is said to be *commutative* if $ab = ba$ for all $a, b \in R$.

Remark 81.

1. All rings in this class are assumed to have units
2. All rings in this class have that $1 \neq 0$.

Definition 82. F is a *field* if:

1. F is a commutative ring
2. All nonzero elements are invertible

Definition 83. A *division ring* is a non commutative field (just has invertible elements).

Example 84. If F is a field, then $F[x]$ is the polynomial ring with variable x.

$F[x_1, \ldots, x_m]$ is the polynomial ring on m variables.

$F(x)$ is the field of fractions:

$$F(x) := \left\{ \frac{f(x)}{g(x)} \middle| f, g \in F[x], g \neq 0 \right\}$$

Definition 85. For a field F:

$$\bigcap_{K \subset R} K = F_0$$

where K is a subfield. F_0 is termed the *prime subfield*.

The *characteristic* of the field is defined as follows:

1. If $F_0 \cong \mathbb{Q}$, then the characteristic is 0
2. If $F_0 \cong \mathbb{F}_p$ for some prime p, then the characteristic of F is p.

Definition 86. For rings R, S, $f : R \to S$ is a *ring homomorphism* if

1. $f(a+b) = f(a) + f(b)$
2. $f(ab) = f(a)bf(b)$
3. $f(0) = 0$
4. $f(1) = 1$ if 1 exists

Definition 87. $I \subset R$ is a *left ideal* if

1. I is an abelian subgroup with respect to addition
2. For all $a \in R$, and $b \in I$, $ab \in I$.

In a commutative ring, left ideals are right ideals.

Theorem 88. If $f : R \to S$ is a ring homomorphism, then $\ker f$ is an ideal in R.

Definition 89. Let $I \subset R$ be an ideal. I is generated by $(a_i)_{i \in X}$ if for all $a \in I$, there exists coefficients in $b_i \in R$ such that

$$a = b_1 a_{i_1} + b_2 a_{i_2} + \cdots + b_n a_{i_n}$$

I is *finitely generated* if it can be generated by a finite set.

I is a *principal ideal* if it can be generated by one element.

We write $I = (a_1, \ldots, a_n)$ when I can be generated by $\{a_1, \ldots, a_n\}$.

Definition 90. We call $a \in R$ a *zero divisor* if $\exists b \in R$ such that $\neq 0$ and $ab = 0$.

Definition 91. R is an *integral domain* if there are no zero divisors except for $a = 0$ (and is commutative).

Definition 92. R is a *PID* or *principal ideal domain* if R is an integral domain such that all ideals are principal.

Definition 93. If $I \subseteq R$ and we have the relation $a \sim_I b \iff a - b \in I$, then $R/I := R/\sim_I$.

Theorem 94. (Isomorphism Theorem): Let $f : R \to S$ be a ring homomorphism. Then f induces an isomorphism $R/\ker f \xrightarrow{\sim} \operatorname{Im} f$.

Theorem 95. (Correspondence Theorem): Let $I \subset R$ be an ideal. Then there is a 1-1 correspondence between ideals in R and ideals in R/I.

Definition 96. $P \subsetneq R$ is a *prime ideal* if $\forall a, b \in R$ such that $ab \in P$, then $a \in P$ or $b \in P$.

Definition 97. $M \subsetneq R$ is *maximal* if $\nexists I \subsetneq R$ such that $M \subsetneq I \subsetneq R$.

Theorem 98. Given an integral domain R, R is a field if and only if R has 2 ideals, R and (0).

Theorem 99. $P \subset R$ is prime if and only if R/P is an integral domain.

Theorem 100. $M \subset R$ is maximal if and only if R/M is a field.

Corollary 101. Maximal ideals are prime

Corollary 102. (0) is prime if and only if R is an integral domain.

Theorem 103. Every proper ideal can be embedded into a maximal ideal

Definition 104. $s \in R$ is a *unit* if it's invertible.

Definition 105. $r \in R$ when r not a unit is *irreducible* if whenever $r = bc$, either b or c is a unit.

Now assuming R is an integral domain:

Theorem 106. If $a \in R$, then (a) being prime implies a is irreducible.

Theorem 107. If R is a PID, then for $a \in R$, a being irreducible implies (a) is prime.

Definition 108. Let R be an integral domain. We say R is a *UFD* or *unique factorization domain* if for all $a \in R$, there exists a unique product

$$a = up_1p_2 \dots p_n$$

such that u is a unit, and the p_i are irreducible.

Uniqueness means for any other factorization $vq_1q_2 \dots q_m$, that

1. $n = m$
2. After reordering the q_i, we have that $p_i = u_iq_i$ for some unit u_i.

Theorem 109. A Euclidean domain is a PID. A PID is a UFD.

Homework Problems

HW 1

Theorem 110. If G is a set with two binary operations $*$ and $\circ$, with an element e such that

1. e is the identity for both operations
2. $(a \circ b) * (c \circ d) = (a * c) \circ (b * d)$

Then the operations coincide, and are associative and commutative

Theorem 111.

1. If a has order n, then $a^m = e \implies n | m$
2. Subgroups of cyclic groups are cyclic
3. Homomorphisms out of cyclic groups are cyclic
4. All subgroups of $\mathbb{Z}$ have form $m\mathbb{Z}$.
5. All subgroups of $\mathbb{Z}/m\mathbb{Z}$ are isomorphic to $\mathbb{Z}/d\mathbb{Z}$ where $d|m$? ~~$(d, m) = 1$~~.
6. All finitely generated nontrivial subgroups of $\mathbb{Q}$ are isomorphic to $\mathbb{Z}$.

HW 2

Theorem 112. If $(m, p) = 1$, p prime, and a an positive integer, then $\binom{p^a m}{p^a}$ is not divisible by p.

Theorem 113. $N_G(H)$ is the maximal subgroup of G in which H is normal

Theorem 114. If $H < G$ is index 2, then H is normal.

Theorem 115. If $H \triangleleft G$ and $(|H|, [G : H]) = 1$, then H is the only subgroup of order $|H|$.

Theorem 116. The orbits of $\mathrm{GL}_n(\mathbb{C})$ are matrices with different Jordan normal forms.

Theorem 117. All groups of order p^2 are abelian.

HW 3

Theorem 118. If G is a p-group and H is a nontrivial normal subgroup, then $H \cap Z(G) \neq \{e\}$

Theorem 119. $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$

Theorem 120. All groups of order pq are of the form

1. $C_p \times C_q$
2. $C_p \rtimes C_q$ if $p|(q-1)$

HW 6

Theorem 121. Let $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{-I, I\}$. Then $\mathrm{PSL}_2(\mathbb{Z}) \cong \mathbb{Z}_2 * \mathbb{Z}_3$.

Additionally, $\mathrm{SL}_2(\mathbb{Z}) \cong \mathbb{Z}_4 *_{\mathbb{Z}_2} \mathbb{Z}_6$.

Theorem 122. If B_n is the group of upper triangular matrices over a field F, then B_n is not nilpotent.

Theorem 123. If G is a group generated by 2 elements, where every element in G has order dividing 3, then $|G| \leq 27$. One example is $G = U_3(\mathbb{F}_3)$.

Definition 124. Let G be a p-group. The subgroup

$$\Phi(G) = \bigcap_{[G:H]=p} H$$

is the *Frattini subgroup* of G.

Theorem 125.

1. $\Phi(G) \lhd G$
2. $\Phi(G)$ is the minimal subgroup such that
$$G/\Phi(G) \cong \mathbb{Z}/p \times \mathbb{Z}/p \times \cdots \times \mathbb{Z}/p$$
3. $\Phi(G) = G^p[G,G]$
4. Let G' be another p-group and $f : G' \to G$ be a group homomorphism. f is surjective if and only if
$$\overline{f} : G/\Phi(G) \to G'/\Phi(G')$$
is surjective.
5. $\{x_1, \dots, x_n\}$ is a system of generators for G if and only if $\{\overline{x_1}, \dots, \overline{x_n}\}$.

HW 7

Theorem 126. (*Chinese Remainder Theorem*): If $A_1, \dots, A_n$ are ideals in R such that $A_i + A_j = R$ for $i \neq j$, then there exists $x \in R$ such that $x \equiv 1 \pmod{A}_1$ and $x \equiv 0 \pmod{A}_i$ for $i > 1$.

Or, $R/(\bigcap A_i) \cong R/A_1 \times \dots R/A_n$.

Definition 127. Let R be an integral domain. A *Euclidean function* on R is a function $\lambda A \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that any $a, b \in R, b \neq 0$ there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\lambda(r) < \lambda(b)$. R is a *Euclidean domain* if it has a Euclidean function associated with it.

Theorem 128.

1. $\mathbb{Z}[i]$ is a UFD.
2. The units of $\mathbb{Z}[i]$ are $1, -1, i, -i$.
3. The irreducible elements of $\mathbb{Z}[i]$ are $1 + i, 1 - i$, primes p, or $a + bi, a - bi$ when $a^2 + b^2$ is a prime.

Theorem 129. If F is a field, then letting $\deg : F[x] \to \mathbb{N}$, we have that using deg as the Euclidean function, $F[x]$ is a Euclidean domain.

Midterm

Theorem 130. (1) Let $p < q < r$ be primes. Prove that a group of order pqr cannot be simple.
(2) Let $p \geq 5$ be a prime. For which p does there exist a simple group of order $12p$? (For each p either establish a simple group, or prove it does not exist. You can sight facts about alternating groups A_n).

Theorem 131. Let G be a solvable group, and $N \lhd G$ be a normal subgroup. Prove that G has normal series with abelian factors $\{e\} = G_n \lhd G_{n-1} \lhd \dots \lhd G_0 = G$ which contains N (that is, $G_i = N$ for some i).

Theorem 132. Let G be a p-group. Show that if $G/[G,G]$ is cyclic, then G is also cyclic.

Theorem 133. Let $B_n(p)$ be the (finite) group of $n \times n$ upper triangular invertible matrices with integer entries considered mod p. Show that

1. $B_n(p)$ is solvable.
2. $B_n(p)$ is not nilpotent.

SUMMARY OF TOPICS AND A FEW PRACTICE PROBLEMS, MATH 504, FALL 2020

General principle: the expectation is that you are well versed in everything covered in lectures and homework. In particular, know at least one solution to all and any homework problems, **including** all presentation problems. Know how to prove all theorems stated or proven in class. The list below is not claimed to be comprehensive but I tried to mention most of the topics we covered. If you notice an omission, let me know!

(1) Basic concepts:
   (a) Groups, subgroups, homomorphisms, cosets and double cosets, normal subgroups, factor groups
   (b) Group actions, stabilizers, centralizers, normalizers
   (c) Presentations by generators and relations
   (d) Exact sequences, split exact sequences for groups
   (e) p-groups, Sylow subgroups
   (f) Direct and semi-direct products
   (g) Center, commutator subgroup
   (h) Filtrations, derived series, central series, composition series
   (i) Solvable and nilpotent groups (several equivalent descriptions)
   (j) Free groups, free products, amalgamated free products
   (k) Ideals, maximal and prime ideals
   (l) units, zero divisors, irreducible elements
   (m) Factoriality, PID, UFD, Euclidean domains

(2) Fundamental examples:
   (a) Symmetric groups (everything about them you learned from the worksheet),
   (b) dihedral groups (various presentations)
   (c) cyclic and abelian groups
   (d) groups of small order
   (e) matrix groups.
   (f) free groups
   (g) Polynomial rings as examples of many things

(3) Theorems:
   (a) Cayley
   (b) Lagrange
   (c) Three isomorphism theorems
   (d) Class formula
   (e) Jordan canonical form
   (f) Sylow theorems (two proofs for the first theorem)
   (g) Jordan-Holder theorem; Zassenhaus lemma; Schreier's theorem
   (h) Universal property of groups given by generators and relations
   (i) Frattini subgroup and Burnside theorem
   (j) Characterization of prime and maximal ideals in terms of quotients

(k) Euclidean $\Rightarrow$ PID $\Rightarrow$ UFD

1. A few practice problems

Disclaimer: this is not a comprehensive list. Once you are confident you've gone over all homework problems, you could try your hand at these, and then continue with an almost unlimited supply in Dummit and Foote.

Problem 1. Classify all finite groups of orders 1 through 10.

Problem 2. Classify all groups of order 2015.

Problem 3. Show that the dihedral group D_m of symmetries of regular m-gon is isomorphic to a subgoup of

(1) S_m,
(2) $\mathrm{GL}_2(\mathbb{C})$.

Note: We now know at least 4 different presentations of D_m: as a semi-direct product of cyclic groups, by generators and relations, a permutation representation, and a matrix representation.

Problem 4. Let $B_n < \mathrm{GL}_n(\mathbb{R})$ be the subgroup of upper-triangular matrices, $T_n < B_n$ be the subgroup of diagonal matrices, and $U_n < B_n$ be the subgroup of upper-triangular matrices with 1's on the main diagonal. Assume $n \geq 2$. Show that
(a) U_n is nilpotent. What is the minimal length of its central series?
(b) B_n is solvable but not nilpotent.
(c) B_n is isomorphic to a semi-direct product of T_n and U_n.

Note: U_n is called the unipotent subgroup, B_n - the Borel subgroup, and T_n is the torus (of $\mathrm{GL}_n(\mathbb{R})$). The statements are valid for any field of coefficients F, at least if characteristic is not 2, and so should be your proofs.

Problem 5 (Prelim 2006, #7). There are five nonisomorphic groups of order 8. For each of those groups G, find the smallest positive integer n such that there is an injective homomorphism $\phi\colon G \to S_n$.

Problem 6 (Prelim 2009, #1).

(1) Classify groups of order $2009 = 7^2 \times 41$.
(2) Suppose that G is a group of order 2009. How many intermediate groups are there—that is, how many groups H are there with $1 \subset H \subset G$, where both inclusions are proper? (There may be several cases to consider.)

Problem 7 Using what we learned since the midterm, find a new (short) proof of problem 4 from the midterm.

Problem 8 Give two different proofs of the first Sylow theorem.

Problem 9 (Prelim 2005, #5). Let R and S be commutative rings with 1, and $f\colon R \to S$ a ring homomorphism.

"C1-rings"

(1) Show that if I is a prime ideal of S, then
$$f^{-1}(I) = \{r \in R : f(r) \in I\}$$
is a prime ideal of R.

(2) Let N be the set of nilpotent elements of R:
$$N = \{r \in R : r^m = 0 \text{ for some } m \geq 1\}.$$
N is called the *nilradical* of R. Prove that it is an ideal which is contained in every prime ideal.

(3) Part (a) lets us define a function
$$f_*\colon \{\text{prime ideals of } S\} \to \{\text{prime ideals of } R\}$$
$$I \mapsto f^{-1}(I)$$
Let N be the nilradical of R. Show that if $S = R/N$ and $f\colon R \to R/N$ is the quotient map, then f_* is a bijection.

For more practice on commutative rings, review all the problems from the last homework.

(1) first, if f^{-1}(an ideal) is an ideal:

subring:

- $0 \in f^{-1}(I)$ b/c $0 \in f^{-1}(0)$.
- $a, b \in f^{-1}(I) \Rightarrow f(a) = s_1,\ f(b) = s_2,\ s_1, s_2 \in I$.

$$\begin{cases} f(a-b) = s_1 - s_2 \in I \Rightarrow a-b \in f^{-1}(I) \\ f(ab) = s_1 s_2 \in I \Rightarrow ab \in f^{-1}(I). \end{cases}$$

ideal:

- let $a \in f^{-1}(I)$. Then $f(ra) = f(r)f(a) \in I$ b/c $f(a) \in I$, I ideal $\Rightarrow ra \in f^{-1}(I)$.

Now if I is prime. Suppose $ab \in f^{-1}(I)$. then $f(ab) = f(a)f(b) \in I \Rightarrow f(a)$ or $f(b) \in I$
$\Rightarrow a$ or $b \in f^{-1}(I)$.

(2). $N = \{r \in R : r^m = 0$ for some $m \geq 1\}$, the nilradical of R.
Suppose $P \subseteq R$ is prime ideal. First, N is ideal, b/c $0 \in N$, if $a \in N \Leftrightarrow a^m = 0 \Rightarrow (-a)^2 = a^2 \Rightarrow (-a)^{2m} = 0$
$(a+b)^{m+n} = 0$, and $(ab)^{mn} = 0$.
$(ra)^m = r^m a^m = 0$.

Now let $a \in N$. Then $a^m = 0$. But $0 \in P$, so $a \cdot a^{m-1} \in P \Rightarrow$
$a \in P$ or $a^{m-1} \in P$. Easy to see u can just keep reducing exponent to ultimately get $a \in P$. $a \in N$ arbitrary, P arbitrary prime ideal
$\boxed{\text{QED}}$.

(3) f_* : {prime ideals of R/N} → {prime ideals of R}
$I \mapsto f^{-1}(I)$. where $f(r) = r+N$.

show inverse of f_* is g_* defined as $P \mapsto f(P)$, P prime ideal in R.

$f_*(g_*(P)) = f_*(\{f(p) : p \in P\}) = f_*(\{p+N : p \in P\}) = f^{-1}(\{p+N : p \in P\}) = \{r \in R : r+N = p+N \text{ for some } p \in P\}$
$= \{r \in R : r \in P+N\} = P+N = P$
b/c $N \subseteq P$.
(part (b))

$g_*(f_*(I)) = g_*(\{r \in R : f(r) \in I\}) = g_*(\{r \in R : r+N \in I\})$
$= \{r+N : r \in R,\ r+N \in I\} = I$.

G is p-group.
WTS: if $G/[G,G]$ is cyclic, then G is cyclic.. Suffices to show G is abelian.

Problem 7. (look at the Frattini Subgroup Section below)

Recall (Thm 40 in Chen's doc) the following facts regarding $[G:G]$:

- $G/[G:G]$ is abelian

- $[G:G] = \bigcap_{G/N \text{ abelian}} N$

- Universal property of abelianization:

$$\begin{tikzcd}
G \arrow[r, two heads, "f"] \arrow[d, "\pi"'] & A \\
G/[G:G] \arrow[ur, dashed, "\hat{f}"'] &
\end{tikzcd}$$

where A is an abelian group

and $f = \check{f} \circ \pi$

Proof 1: In Frattini section we showed $[G,G] \leq \Phi(G)$

Lemma $a | bc$, $(a,b) = 1$. $\Rightarrow$ $a | c$.

(proof by prime factorization or Bezout Identity)

Lemma $(a,b)=1$, $(a,c)=1$, then $(a,bc)=1$.

If not, then $\exists$ some prime $p | a$; $p | bc$.
But $p|bc \Rightarrow p|b$ or $p|c$, contradiction.

Problem 6:

Classify all groups of order $2009 = 7^2 41$

Sylow I gives existence of Sylow 7 group (order 49) and Sylow 41 group.

$n_7 = \#$ of " $\quad n_{41} = \#$ of "

Sylow III gives $n_7 \equiv 1 \bmod 7$, $n_7 | 7^2 41 \Rightarrow n_7 | 41 \Rightarrow n_7 = 1, 41$ but not 41 b/c $41 \not\equiv 1 \bmod 7$.

$\Rightarrow (n_7, 7) = 1$

$\Rightarrow n_7 = 1 \Rightarrow$ H, the Sylow 7 group is normal

$n_{41} \equiv 1 \bmod 41$, $n_{41} | 7^2 41 \Rightarrow n_{41} | 49$

$\Rightarrow (n_{41}, 41) = 1$

$\Rightarrow n_{41} = 1$ or 42, but not 42 b/c $42 \nmid 49$.

$\Rightarrow n_{41} = 1 \Leftrightarrow$ N, the Sylow 41 group is normal in G.

Clearly $H \cap N = \{e\}$, b/c non-trivial elements of N have order 41, and for H it's 7 or 49.

Using that $|HK| = \dfrac{|H||K|}{|H \cap K|}$ (proof: HK has $|H||K|$ symbols, and $h_1 k_1 = h_2 k_2 \Leftrightarrow \exists t \in H \cap K$ s.t. $h_2 = h_1 t$, $k_2 = t^{-1} k_1$ so each element in HK is represented by exactly $|H \cap K|$ products.)

(proof 2: $H \times K$ acts on HK by $(h,k)x = hxk^{-1}$.
Stabilizer of $1 \in HK$ is all (h,k) s.t. $hk^{-1} = 1 \Leftrightarrow h = k$, i.e all (t,t) s.t. $t \in H \cap K$. So $\text{Stab}(1) \cong H \cap K$.
Orbit of 1 is all of HK. so orbit-stabilizer-thm gives $\underset{|H||K|}{|H \times K|} = |HK|\,|H \cap K|$
$|G| = |\text{orb}|\,|\text{stab}|$)

we get that HK has order 2009 and hence must be G.

Thus, by identification thm for direct products (see also generalization of that thm in Frattini Subgroup section below)

$G \cong H \times N$.

We know that b/c $|N| = 41$ is prime, $N \cong \mathbb{Z}_{41}$. But we do not know this about H, which has order 7^2.

Recall (see Thm 117 in Chen's doc) that all groups of order p^2 are abelian.

- if H contains 1 element of order 49, say a, then $H = \langle a \rangle \cong \mathbb{Z}_{49}$.
- only other possibility is that H has all elements order 7. Let a be nontrivial, and consider $\langle a \rangle$ which has order 7. Then b/c H is abelian, $\langle a \rangle \trianglelefteq H$. Take some b nontrivial in $H \setminus \langle a \rangle$; similarly $\langle b \rangle \trianglelefteq H$. Clearly $\langle b \rangle \cap \langle a \rangle = \{e\}$ (by construction of b), and like above we have that

$$|\langle a \rangle \langle b \rangle| = \frac{|\langle a \rangle|\,|\langle b \rangle|}{|\langle a \rangle \cap \langle b \rangle|} = 7^2 \Rightarrow \langle a \rangle \langle b \rangle = H$$

so again by identification thm for direct products $H \cong \mathbb{Z}_7 \times \mathbb{Z}_7$.

OR could use fundamental thm of finitely generated abelian groups on pg 158 of Dummit & Foote.

Thus, two groups of order 2009: $\mathbb{Z}_{49} \times \mathbb{Z}_{41} \cong \mathbb{Z}_{2009}$

$\mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{41} \cong \mathbb{Z}_{287} \times \mathbb{Z}_7$

---

b. How many intermediate groups? Possibilities for $|H|$: 7, 41, 49, 287

Case A: $G \cong \mathbb{Z}_{49} \times \mathbb{Z}_{41} \cong \mathbb{Z}_{2009}$. See HW1, Chen's doc Thm 111: all subgroups of $\mathbb{Z}_{2009}$ are isomorphic to $\mathbb{Z}/d\mathbb{Z}$ for all $d | n$ (and in fact all $\mathbb{Z}/d\mathbb{Z}$ are attained). So $\mathbb{Z}_7, \mathbb{Z}_{41}, \mathbb{Z}_{49}, \mathbb{Z}_{287}$ all attained once, and no others.

Case B. $G \cong \mathbb{Z}_{287} \times \mathbb{Z}_7$.

(only) subgrp order 7 in $\mathbb{Z}_{287}$ $\{41, \ldots, 287\}$ $\quad$ (41,0) (41,1), (41,2) ... (41,6) each generate distinct order 7 subgroup. $\quad$ 7

any other # in first coordinate will just lie in one of the $\langle (41,n) \rangle$.

order 41 $\{7, \_\_\_\_, 287\}$. $\quad$ (7,0) ← order 41 $\quad$ (7,1) ____ (7,6) each generate distinct order 41 subgroup. $\quad$ 1 + 1

b/c $(7,41)=1$, all the same group of order 287

order 287 $\{1 \_\_\_\_ 287\}$. $\quad$ (1,0) (1,1) ____ (1,6) ____ 287 subgroup. $\quad$ 7

Finally there is (0,1), generating order 7 subgroup. $\quad$ 1

and then $\langle (41,0)(0,1) \rangle$ is order 49. $\quad$ + 1

18 intermediate groups

NOTE! left proof only works b/c 7 | 287.
In above, if we think of $\mathbb{Z}_{49} \times \mathbb{Z}_{41}$,

in $\mathbb{Z}_{49}$

order 7 $\{7 \_\_\_\_ 49\}$ $\quad$ $\boxed{(7,1)\ (7,2) \cdots (7,41)}$

order 49 $\{1 \_\_\_\_ 49\}$

all generate the same group b/c $(7,41) = 1$!

More rigorous proof:

$G \cong \mathbb{Z}_{287} \times \mathbb{Z}_7$. We know there is unique Sylow 7, 41 groups, so 1 each of orders 49, 41. 2

How many subgroups of order 7? These are cyclic, so $\frac{\text{\# of order 7 elements}}{6}$.

$(x,y)^7 = 1 \Rightarrow 7x = 0$ and $7y = 0$.

↑ ↑

7 options $\{41, \dots 287\}$ × 7 options

- 1 option (both can't be 0, that's identity element) = 48

↑ by counting # order 7 elements, we are counting each order 7 subgroup 6 times.

$\Downarrow$ $\frac{48}{6} = 8$.

How many subgroups of order 287? Let H be such a group.

By Cauchy's thm, H has elements of order 41 and 7, say a, b. Then $\langle a \rangle \cap \langle b \rangle = \{e\}$,

$|\langle a \rangle||\langle b \rangle| = 41 \cdot 7 = 287 \Rightarrow H = \langle a \rangle \times \langle b \rangle$.

↑ ↑

1 possibility 8 possibilities, so 8 total possibilities.

$$\boxed{8+8+2 = 18}$$

if overlap, $(xy)(yz) = (xzy)$ $\neq$!
but $(yz)(xy) = (yza)$
these don't commute, but a,b,c do.

so must have ≥ 6 elements

Problem 5.

Case 1: $\overset{a}{\mathbb{Z}_2} \times \overset{b}{\mathbb{Z}_2} \times \overset{c}{\mathbb{Z}_2}$. elements need to have order 2, so transpositions. can't overlap, so send generators $a \mapsto (1,2)$, $b \mapsto (3,4)$, $c \mapsto (5,6)$. 6 suffices

Case 2: $\overset{a}{\mathbb{Z}_4} \times \overset{b}{\mathbb{Z}_2}$. send a to length 4 cycle, b to transposition. No overlap, so again ≥ 6. $a \mapsto (1234)$ $b \mapsto (56)$. 6 suffices

Case 3: $\mathbb{Z}_8$. need ≥ 8 elements. (12345678) suffices, so 8 suffices

cuz if $n<8$, S_n has no elements of order 8

Case 4: D_4. If $n<4$, then $|S_n| < 8$, so no. S_4 works (see Problem 3 of final review).

Alternate proof that S_4, S_5 don't work in Cases 1,2,3. D_4 is Sylow 2 subgroup of S_4, S_5, and all Sylow 2-subgroups are conjugate hence isomorphic, so the abelian groups of Cases 1,2,3 can not be isomorphic to a size 8 subgroup of S_4, S_5 (since all size 8 subgroups of S_4, S_5 are Sylow 2-subgroups.

Case 5: $Q_8 = \langle \bar{e}, i, j, k \mid \bar{e}^2 = e, i^2 = j^2 = k^2 = ijk = \bar{e} \rangle$ Cayley's thm gives embedding $Q_8 \hookrightarrow S_8$.

$= \langle x, y \mid x^4 = 1, x^2 = y^2, xy = yx^{-1} \rangle$

Suppose Q_8 isomorphic to subgroup of S_n, $n \leq 7$, i.e. some injection $f: Q \hookrightarrow S_n$. Then we have action $\phi: Q \times S_n \to S_n$
$\phi(g,a) = f(g) \cdot a$

Let A be group w/ order ≤ 7. Consider action of Q_8 on A.
Let $a \in A$. Then,

$$|Q/\text{Stab}(a)| = |\text{Orb}(a)| \leq |A| \leq 7 \Rightarrow \text{Stab}(a) \geq 2.$$

So $\forall a \in A$, $\text{Stab}(a)$ is nontrivial subgroup of Q. But all nontrivial subgroups of Q include $\{\pm 1\}$, so we know $\forall a \in A$ $\text{Stab}(a) \supseteq \{\pm 1\}$. So then $\phi(\pm 1, a) = f(\pm 1) \cdot a = a \Rightarrow f(\pm 1) = e$. So contradict: f is not injective.

More general lemma:

Frattini Subgroup

and a theorem about direct products $H_1 \times \cdots \times H_k \cong G \Leftrightarrow$

- $H_i \trianglelefteq G$
- $G = H_1 \cdots H_k = \{h_1 \cdots h_k : h_i \in H_i\}$
- $\hat{H}_i := H_1 \cdots H_{i-1} \cdot H_{i+1} \cdots H_k$, and $\forall i \in [k]$, $H_i \cap \hat{H}_i = \{e\}$.

let G be a p-group. Define the Frattini subgroup to be

$$\Phi(G) = \bigcap_{[G:H]=p} H .$$

(a) $\Phi(G) \trianglelefteq G$.

Proof 1: let σ be arbitrary in $\mathrm{Aut}(G)$.

σH maps to H', where H' has same # elements as H.

$\Rightarrow [G:H'] = p$.

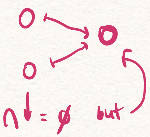
In fact σ induces bijection from all subgroups of index p to itself. (inverse is σ^{-1})

$$\sigma(\Phi(G)) = \sigma\Big(\bigcap_{[G:H]=p} H\Big) = \bigcap_{[G:H]=p} \sigma(H) = \bigcap_{[G:H]=p} H = \Phi(G)$$

can do this b/c injectivity

can do this b/c surjectivity

w/o injectivity, maybe



$\cap \downarrow = \emptyset$ but is not nonempty

Subgroups w/ this property are called "characteristic" (subgroup is fixed under all automorphisms). And characteristic $\Rightarrow$ normal (b/c conjugation).

Proof 2: lemma: for any group G, if p is smallest prime dividing $|G|$, subgroups H s.t. $[G:H]=p$ are normal.

Proof: G acts on set of left cosets $\{xH : x \in G\}$ by left multiplication $g(xH) = (gx)H$. (where there are p cosets), inducing homomorphism from $G \to S_p$. Let K be the kernel $= \{k \in G : kxH = H \ \forall x \in G\}$ so in particular taking $x = 1_G$, we see that K must be in H; i.e. $K \leq H$. Thus by 1st isomorphism thm, $G/K \cong$ some subgroup of S_p, so $|G/K|$ must divide $p!$. But $|G/K|$ also divides $|G|$, and p is smallest prime dividing $|G|$, so $|G/K|$ must $= p$. So we have that

$$p = |G/K| = [G:K] = [G:H][H:K] = p\,[H:K] \Rightarrow [H:K] = 1 \Rightarrow K = H.$$

But K is kernel $\Rightarrow$ normal, so H is normal too.

So in our problem, G is p group, so p is smallest prime $\mid |G|$, so all H s.t. $[G:H]=p$ are normal. Intersection of normal subgroups is normal subgroup, so $\Phi(G)$ is in fact normal.

(b). $\Phi(G)$ is minimal subgrp s.t. $G/\Phi(G) \cong \mathbb{Z}/p\mathbb{Z} \times$ ———— $\times \mathbb{Z}/p\mathbb{Z}$. (abelian!)

From lemma above, all H s.t. $[G:H]=p$ are normal in G. Thus, $|G/H| = p$, and so G/H must be the cyclic group $\mathbb{Z}/p\mathbb{Z}$ (abelian!). I.e. we have $\forall$ such H; $\forall x,y \in G$,

$(xy)H = (yx)H$, implying that $(y^{-1}x^{-1}yx)H = H$, so $[G,G] \leq H$

(for all such H), so $[G:G] \leq \Phi(G)$. (Side note: G/N abelian iff $[G:G] \leq N$)

B/c $G/H \cong \mathbb{Z}/p\mathbb{Z}$, $\forall x \in G$, $(xH)^p = x^pH = H \Rightarrow x^p \in H$. True for all such $H \Rightarrow x^p \in \Phi(G)$ $\forall x \in G$.

Choose some $x_1 \in G$ s.t. $x_1\Phi(G)$ nontrivial, and let $X_1 = \langle x_1\Phi(G)\rangle$. Pick $x_2 \in G \setminus X_1$ and so on until we get $X_1 \cdots X_k$ (process terminates b/c G finite). Clearly $X_i \cap X_j = \{e\}$, $\bigcup_{i=1}^{k} X_i = G/\Phi(G)$.

WTS $X_1 \cdots X_k = G/\Phi(G)$.

- $\subseteq$ b/c $(x_1^{a_1} \cdots x_k^{a_k})\Phi(G) \in G/\Phi(G)$ obviously.
- $\supseteq$ b/c $\bigcup_{i=1}^{k} X_i = G/\Phi(G) \Rightarrow \forall x \in G, \exists i \in [k]$ s.t. $x\Phi(G) \in X_i \subseteq X_1 \cdots X_k$.

Then $G/\Phi(G) \cong X_1 \times \cdots \times X_k$.

Lemma: (Thm 28 in Chen's doc). $G \cong A \times B$ iff

or use

- $A, B \trianglelefteq G$
- $A \cap B = \{e\}$
- $AB = G$.

Proof:

INTERNAL DIRECT PRODUCT

MATH 457

Here is the definition of internal direct product from the text:

Definition 1. Let $H_i \lhd G$ for $i \in \{1, \dots, n\}$. [Note that we *require* that H_i is normal!] Then G is the *internal direct product of the H_i's* if for any $g \in G$, $\exists! h_i \in H_i$ such that $g = h_1 \cdot h_2 \cdots h_n$.

Here is the properties I gave to decide if a group is isomorphic to the (external) direct product of a finite number of its subgroups:

Definition 2. Let $H_i \leq G$ for $i \in \{1, \dots, n\}$. Then the sets H_i *satisfy the* IDP *properties* if:

(1) $H_i \lhd G$, for all i;
(2) $G = H_1 \cdots H_n \overset{\text{def}}{=} \{h_1 \cdots h_n \ : \ h_i \in H_i\}$;
(3) if $\hat{H}_i \overset{\text{def}}{=} H_1 \cdots H_{i-1} \cdot H_{i+1} \cdots H_n$, then $H_i \cap \hat{H}_i = \{1\}$. [Note that if $n = 2$, then $\hat{H}_1 = H_2$ and $\hat{H}_2 = H_1$.]

We will prove that the definitions are equivalent, i.e., G is the internal direct product of the H_i's if and only if the H_i's satisfy the IDP properties. [This is Theorem 5 below.]

We need the following lemma.

Lemma 3. *If $H_i \leq G$ for $i \in \{1, \dots, n\}$ satisfy* IDP *properties, then $h_i h_j = h_j h_i$ for all $h_i \in H_i$ and $h_j \in H_j$ with $i \neq j$.*

Proof. Since $h_i^{-1} \in H_i \lhd G$, we have that $h_j h_i^{-1} h_j^{-1} \in H_i$. So, $h_i(h_j h_i^{-1} h_j^{-1}) \in H_i$.

Similarly, since $h_j \in H_j \lhd G$, we have that $h_i h_j h_i^{-1} \in H_j$. So, $(h_i h_j h_i^{-1}) h_j^{-1} \in H_j$.

Thus, we have that $h_i h_j h_i^{-1} h_j^{-1} \in H_i \cap H_j$. But since $i \neq j$, we have that $H_j \subseteq \hat{H}_i$, and so $H_i \cap H_j \subseteq H_i \cap \hat{H}_i$. Moreover, by property (3), we have that $H_i \cap \hat{H}_i = \{1\}$. Hence, $h_i h_j h_i^{-1} h_j^{-1} \in H_i \cap H_j \subseteq H_i \cap \hat{H}_i = \{1\}$, which implies that $h_i h_j h_i^{-1} h_j^{-1} = 1$, i.e., $h_i h_j = h_j h_i$. □

We then have:

Theorem 4. *Let $H_1, \dots, H_n \leq G$. Then, $\phi : H_1 \times \cdots \times H_n \to G$ defined by $\phi(h_1, \dots, h_n) = h_1 \cdots h_n$ is an isomorphism if and only if the H_i's satisfy the IDP properties.*

Proof. [$\Rightarrow$:] Assume that ϕ [as in the statement] is an isomorphism. Let $\tilde{G} \overset{\text{def}}{=} H_1 \times \cdots \times H_n$ and $\tilde{H}_i \overset{\text{def}}{=} \{1\} \times \cdots \{1\} \times H_i \times \{1\} \times \cdots \times \{1\} \leq \tilde{G}$ [with H_i in the i-th coordinate]. Then, clearly $\phi(\tilde{H}_i) = H_i$. Since $\tilde{H}_i \lhd \tilde{G}$ [easy exercise!], we have that $H_i \lhd G$, as ϕ is an isomorphism [by assumption]. [This was a problem in the exam.] Thus, IDP property (1) is proved.

Since ϕ is an isomorphism [and hence onto] and $\phi(\tilde{G}) = H_1 \cdots H_n$ [by definition of ϕ and the product of groups], we have that $G = H_1 \cdots H_n$, proving property (2).

Now, let $\hat{\tilde{H}}_i \overset{\text{def}}{=} H_1 \times \cdots \times H_{i-1} \times \{1\} \times H_{i+1} \times \cdots \times H_n$. Then, clearly $\phi(\hat{\tilde{H}}_i) = \hat{H}_i$ [with $\hat{H}_i$ as in Definition 2] and $\tilde{H}_i \cap \hat{\tilde{H}}_i = \{(1, \dots, 1)\}$. Thus,

$$\begin{aligned}
\{1\} &= \phi(\{(1, \dots, 1)\}) \\
&= \phi(\tilde{H}_i \cap \hat{\tilde{H}}_i) && \text{[as noted above]} \\
&= \phi(\tilde{H}_i) \cap \phi(\hat{\tilde{H}}_i) && \text{[as } \phi \text{ is a } \textbf{bijection} \text{ – this is a Math 300 exercise]} \\
&= H_i \cap \hat{H}_i && \text{[as noted above]}
\end{aligned}$$

Hence, property (3) is also satisfied.

[$\Leftarrow$:] Assume now that the H_i's satisfy the IDP property. Then, ϕ is a homomorphism by Lemma 3. It is onto by property (2) [as $\phi(H_1 \times \cdots \times H_n) = H_1 \cdots H_n$ by definition of ϕ].

Now we show that ϕ is injective. Suppose that $\phi(h_1, \dots, h_n) = 1$. This means that $h_1 \cdots h_n = 1$, or $h_1^{-1} = h_2 \cdots h_n$. Since the left hand side is in H_1 and the right hand side is in $\hat{H}_1$, property (3) tells us that $h_1 = 1$ and $h_2 \cdots h_n = 1$. Then, $h_2^{-1} = h_3 \cdots h_n$ and now the left hand side is in H_2 and the right hand side is in $\hat{H}_2$. As before, we obtain $h_2 = 1$ and $h_3 \cdots h_n = 1$. Inductively, we obtain that $h_i = 1$ for all i. Hence, $\ker \phi = \{(1, \dots, 1)\}$ and ϕ is injective. □

Now, we can prove that equivalency of the Definitions 1 and 2:

Theorem 5. *Let $H_i \lhd G$ for $i \in \{1, \ldots, n\}$. [Note that we are already assuming that the H_i's are normal, since it is in the conditions of* both *definitions!] We have that G is the internal direct product of the H_i if and only if the H_i's satisfy the IDP properties.*

Proof. [⇒:] Assume that G is the internal direct product of the H_i's. Clearly properties (1) and (2) of IDP are satisfied.

Now, let $h_i \in H_i \cap \hat{H}_i$. Then, since $h_i \in \hat{H}_i$, we have, by definition, that

$$1 \cdots 1 \cdot h_i \cdot 1 \cdots 1 = h_i = x_1 \cdots x_{i-1} \cdot 1 \cdot x_{i+1} \cdots x_n,$$

where $x_j \in H_j$. By the unique representation hypothesis, we have that $h_i = 1$. Thus $H_i \cap \hat{H}_i = \{1\}$, i.e., property (3) is also satisfied.

[⇐:] Assume now that the H_i's satisfy the IDP properties. [By (1), we would then get that the H_i's are normal, but we are already assuming it here.] Then, by (2), every element $g \in G$ can be written as $g = h_1 \cdots h_n$ with $h_i \in H_i$. [We need to show uniqueness.]

Now assume that

$$h_1 \cdots h_n = x_1 \cdots x_n, \qquad \text{with } h_i, x_i \in H_i.$$

Thus, with ϕ as in the statement of Theorem 4 [which we can use since are assuming IDP properties], we have that

$$\phi(h_1, \ldots, h_n) = \phi(x_1, \ldots, x_n).$$

Since ϕ is an isomorphism [and hence one-to-one], we have that $h_i = x_i$ for all i, and hence the representation is unique. □

This gives us:

Corollary 6. *G is the internal direct product of the subgroups H_i's for $i \in \{1, \ldots, n\}$ [and hence $H_i \lhd G$* by assumption!*] if and only if $\phi : H_1 \times \cdots \times H_n \to G$ defined by $\phi(h_1, \ldots, h_n) = h_1 \cdots h_n$ is an isomorphism.*

Proof. By Theorem 4, we know that that H_i's satisfying IDP is equivalent to ϕ [as in the statement] being an isomorphism. Since the former is equivalent to G being the internal direct product of the subgroups H_i's [by Theorem 5], the result follows. □

MATH 504 PRESENTATION PROBLEM

A. WAUGH

Lemma 1. Let G be a finite group. If p is the smallest prime dividing $|G|$ and $[G : H] = p$, then H is a normal subgroup of G.

Problem 1 (Frattini Subgroup)**.** Let G be a p-group and

$$\Phi(G) = \bigcap_{[G:H]=p} H,$$

denote the **Frattini subgroup** of G. Then $\Phi(G)$ is normal is G and is the smallest subgroup such that

$$G/\Phi(G) \cong \mathbb{Z}/p \times \mathbb{Z}/p \times \cdots \times \mathbb{Z}/p.$$

Such a product group is called an **elementary abelian p-group**.

Proof. First, $\Phi(G)$ is a subgroup of G since the intersection of subgroups is a subgroup. To see $\Phi(G)$ is normal, we show that it is a characteristic subgroup[1] of G. Suppose $H \leq G$ is such that $[G : H] = p$ and let $\sigma \in \text{Aut}(G)$ be arbitrary. Then $|\sigma(H)| = |H|$ and $\sigma(H) \leq G$ implies $[G : \sigma(H)] = p$. Moreover, every such subgroup H of index p is the image of a subgroup $H' \leq G$ of index p by taking $H' = \sigma^{-1}(H)$. So

$$\sigma(\Phi(G)) = \sigma(\bigcap H) = \bigcap \sigma(H) = \Phi(G),$$

where the intersections are being taken over all subgroups of index p in G. Hence $\Phi(G)$ is characteristic in G and therefore normal in G.

For the statement that $G/\Phi(G)$ is elementary abelian, notice if $H \leq G$ has index p, then H is normal in G (by Lemma 1). Consequently, $G/H \cong \mathbb{Z}/p$ is abelian for each subgroup H of index p. In particular, $[G : G] < \Phi(G)$. Next, because $|G/H| = p$, if $x \in G$, then $(xH)^p = H$. So $x^p \in \Phi(G)$ for all $x \in G$.

Now, let $\{x_i\Phi(G)\} \subset G/\Phi(G)$ be such that $\langle x_i\Phi(G)\rangle \cap \langle x_j\Phi(G)\rangle = \{e\}$ for all $i \neq j$. This is possible first choosing a non-identity element $x_1\Phi(G)$ of $G/\Phi(G)$, letting $X_1 = \langle x_1\Phi(G)$, and choosing our next element from $G \setminus X_1$. Continuing this process inductively, the above argument implies every element we choose will will generate a cyclic group of order p which, by construction, will not intersect any of the already chosen subgroups. As $G/\Phi(G)$ is a finite p-group, this process will eventually terminate when $\bigcup X_i = G/\Phi(G)$. Finally, the X_i intersect only at the identity, each X_i is normal in the abelian group $G/\Phi(G)$ and $\prod_{i=1}^{k} X_i = G/\Phi(G)$ by a clear cardinality argument. So

$$G/\Phi(G) \cong X_1 \times X_2 \times \cdots \times X_k \cong \mathbb{Z}/p \times \mathbb{Z}/p \times \cdots \times \mathbb{Z}/p.$$

Date: December 3, 2020.

[1] A subgroup H of G is said to be **characteristic** if for every $\sigma \in \text{Aut}(G)$, $\sigma(H) \leq H$. In particular, because conjugation by $g \in G$ is an automorphism of G, every characteristic subgroup is normal.

To see $\Phi(G)$ is the smallest subgroup for which $G/\Phi(G)$ is elementary abelian, suppose K were a normal subgroup of G such that G/K is elementary abelian. Then G/K is generated by cosets $\{z_iK\}_{i=1}^m$ (each of order p) such that

$$G/K \cong \langle z_1K\rangle \times \cdots \times \langle z_mK\rangle.$$

This group has maximal subgroups K_i/K generated by $\{z_jK : j \neq i\}$ in the above product. Consequently, $\bigcap K_i/K = 1$ which, by the third isomorphism theorem, implies $\bigcap K_i = K$. Now, because $K \leq K_i \leq G$,

$$p = [G : K] = [G : K_i][K_i : K] = [G : K_i]p^{n-1},$$

implies $[G : K_i] = p$. Thus

$$\Phi(G) = \bigcap_{[G:H]=p} H \leq \bigcap_i K_i = K.$$

□

Nongenerators

Amalgamated product $\boxed{\text{definition}}$

$A = \langle X_A \mid W_A \rangle$

$B = \langle X_B \mid W_B \rangle$

$H = \langle X_H \mid W_H \rangle$.

$$A *_H B = \langle X_A \cup X_B \mid W_A \cup W_B \cup \{\varphi(x) = \psi(x)\}_{x \in X_H} \rangle$$

$\varphi : H \to A$

$\psi : H \to B$ injective homomorphisms.

Bashir says most common case is $H \leq A, B$ and φ, ψ are inclusion maps.

$\mathbb{Z}_4 *_{\mathbb{Z}_2} \mathbb{Z}_6$. $\langle A, B \mid A^4 = 1, B^6 = 1, \varphi(x) = \psi(x) \rangle$

$\langle x \mid x^2 = 1 \rangle$

what are φ and ψ? we know φ, ψ must map identity to identity, so we only need to worry about x. To make it injective homomorphism, it must be that $\varphi(x) = A^2$ $\psi(x) = B^3$.

(unique choice).

so we have $\mathbb{Z}_4 *_{\mathbb{Z}_2} \mathbb{Z}_6 \simeq \langle A, B \mid A^4 = B^6 = 1, A^2 = B^3 \rangle \overset{G}{=}$.

WTS it's iso to $SL_2(\mathbb{Z})$

$\Phi : G \to SL_2(\mathbb{Z})$ by evaluating the word.

$$AB^2AB = O$$

Φ is surjective (from part 1 of (a))

we just need to prove injectivity.

$A^2 A^m = A^{2+m} = A^{m+2} = A^m A^2$

$A^2 B^n = B^3 B^n$ ———— $= B^n A^2$

That means, for any word w, $A^2 w = w A^2$.

$N = \{Id, A^2\}$. is central (hence normal) in G.

$G/N = \{wN : w \in G\} \simeq \langle A, B \mid A^2 = B^3 = 1 \rangle \underset{\text{part (a)}}{\simeq} PSL_2(\mathbb{Z})$.

if W contains $A^{2,3}$ or $B^{3,4,5}$, then we can just swap them to merge with N.

Now consider $\phi : G/N \to PSL_2(\mathbb{Z}) \simeq SL_2(\mathbb{Z})/\{Id,-Id\}$.

$$\phi(wN) = \Phi(w)\{Id,-Id\}.$$

well-defined:

if $W_1N = W_2N$, then $W_1 = W_2 n$ for some $n \in N$. but $\Phi(n)$ = either Id, $-Id$

so $\phi(W_1N) = \Phi(W_1)\{Id,-Id\} = \Phi(W_2)\underbrace{\Phi(n)\{Id,-Id\}}_{} = \Phi(W_2)\{Id,-Id\} = \phi(W_2N)$

ϕ is in fact isomorphism (from part (a))

Finally, to prove Φ is injective. Let w_0 be arbitrary in $\ker\Phi$. $\Phi(w_0) = Id$.

$$\phi(w_0N) = \{Id,-Id\} = 1_{PSL_2(\mathbb{Z})}.$$

i.e. $w_0N \in \ker\phi$. But $\ker\phi$ is trivial, so $w_0N = N \Rightarrow w_0 \in N$.

either $w_0 = Id$, A^2.

But $\Phi(Id) = Id \Leftarrow$ only possible case.

~~$\Phi(A^2) = -Id$.~~

So $w_0 = Id$. So $\ker\Phi$ is trivial. QED