# MIDTERM 2

COLTON GRAINGER (MATH 6130 ALGEBRA)

## 1. Due 2018-11-16 at 9:00am

**1.1. Subgroups of a symmetric group.** Find explicit generators for subgroups of the symmetric group $S_7$ that are isomorphic to each of the groups (a) $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (b) $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and (c) $D_8$. Show also that $S_7$ has no subgroup isomorphic to $\mathbf{Z}/8\mathbf{Z}$ or $Q_8$.

*Demonstration.* By inspection:

- $C_2 \times C_4 \cong \langle (1\,2), (3\,4\,5\,6) \rangle$
- $C_2 \times C_2 \times C_2 \cong \langle (1\,2), (3\,4), (5\,6) \rangle$
- $D_8 \cong \langle (1\,2\,3\,4), (1\,2)(3\,4) \rangle$

The integer partitions of $7$ correspond bijectively to the disjoint cycle types (i.e., conjugacy classes) of the $7!$ elements of $S_7$. The order of an element of a given cycle type is the least common multiple of the disjoint cycle lengths. We list the integer partitions of $7$ explicitly

| integer partition | least common multiple |
|---|---|
| $7$ | $7$ |
| $6, 1$ | $6$ |
| $5, 1, 1$ | $5$ |
| $5, 2$ | $10$ |
| $4, 1, 1, 1$ | $4$ |
| $4, 2, 1$ | $4$ |
| $4, 3$ | $12$ |
| $3, 1, 1, 1, 1$ | $3$ |
| $3, 2, 1, 1$ | $6$ |
| $3, 2, 2$ | $6$ |
| $3, 3, 1$ | $3$ |
| $2, 1, 1, 1, 1, 1, 1$ | $2$ |
| $2, 2, 1, 1, 1$ | $2$ |
| $2, 2, 2, 1$ | $2$ |
| $1, 1, 1, 1, 1, 1, 1$ | $1$ |

- Because $S_7$ has no element $x$ of order $8$, there cannot exist $H \leqslant S_7$ such that $H \cong C_8$.
- $Q_8$ has $3$ normal subgroups of order $4$ each pairwise incomparable under the relation "is a subgroup of", i.e.. "$\leqslant$". Since normal subgroups are unions of conjugacy classes, a subgroup $H$ of $S_7$ could only have $2$ normal subgroups of order $4$ incomparable under the relation $\leqslant$. Should an isomorphism from $H \leqslant S_7$ to $Q_8$ exist, the lattice isomorphism theorem would produce a contradiction, as the relation $\leqslant$ is preserved under isomorphism (as well as the order of subgroups and their embedded normality). □

*Date:* 2018-11-15.
*Compiled:* 2018-11-16.

1.2. **Transitive group actions.** *Given.* Suppose $G$ acts transitively on sets $X$ and $Y$, where $1 < |X| < |Y| = p$ and $p$ is prime.

*To prove.* G is not simple.

*Proof.* For contradiction, suppose $G$ is a simple group. Since $G$ acts transitively on $X$, where $|X| > 1$, there's a *nontrivial* permutation representation $\pi \colon G \to S_X \cong S_n$. Now $\ker \pi \triangleleft G$ is a *proper* normal subgroup of the simple group $G$, so we must have $\ker \pi = \{1\}$. Since $\pi$ is injective, we identify $G$ with its image as a permutation group:

$$G \leqslant S_n.$$

Let $y \in Y$. By orbit-stabilizer,

$$|G| = |G(y)| \cdot |\mathrm{Stab}_G(y)|.$$

$G$ acts transitively on $Y$, so $G(y) = Y$. Thus

$$|G| \text{ is divisible by } |Y|.$$

Whence the contradiction: $|Y| = p$ is a prime strictly greater than $n$, yet

$$G \leqslant S_n \quad \text{implies, by Lagrange,} \quad p \mid n! \quad \text{and this is absurd.}$$

So $G$ cannot be simple. □

1.3. **A homomorphism into a solvable group.** *Given.* Let $G$ be a finite group with a normal subgroup $N \triangleleft G$, and suppose $\theta \colon G \to H$ is a group homomorphism into a solvable group $H$. Suppose the commutator subgroup of $G/N$ is itself.

*To prove.* $\theta(G) = \theta(N)$.

*Proof.* $\theta$ induces $\varphi \colon G/N \to \theta(g)\theta(N)$ such that

$$gN \mapsto \theta(g)\theta(N).$$

Observe:

- $\varphi$ is well defined. Let $g, h \in G$. Say $gN = hN$. Then $h^{-1}g \in N$. Under the homomorphism $\theta$, we see
$$\theta(h^{-1}g) \in \theta(N),$$
so $\theta(g) \in \theta(h)\theta(N)$. Thus
$$\theta(g)\theta(N) = \theta(h)\theta(N).$$
- $\varphi$ is a homomorphism. For each $gN, hN \in G/N$, we have
$$\varphi(ghN) = \theta(gh)\theta(N) = \theta(g)\theta(N) \cdot \theta(h)\theta(N) = \varphi(gN)\varphi(hN).$$
- $\varphi$ is surjective immediately from its definition.

Now $\theta(G) \leqslant H$ implies $\theta(G)$ is solvable (it's a subgroup of a solvable group). There's a natural epimorphism from $\theta(G)$ to $\theta(G)/\theta(N)$. So

$$\theta(G)/\theta(N) \quad \text{is solvable (it's homomorphic image of a solvable group).}$$

Under the hypothesis that $[G/N, G/N] = G/N$, we have

$$\theta(G)/\theta(N) = \varphi(G/N) = \varphi([G/N, G/N]) = [\varphi(G/N), \varphi(G/N)] = [\theta(G)/\theta(N), \theta(G)/\theta(N)].$$

Since $\theta(G)/\theta(N)$ is solvable, its derived series must stabilize at $\{1\}$. So $\theta(G)/\theta(N) = \{1\}$. Thus $\theta(G) = \theta(N)$. $\square$

1.4. **A semi-direct product.** *Given.* Let $G = H \ltimes U$ be a finite group for groups $H$ and $U$. Let $p$ be prime.

*To prove.*

(a) If $\mathrm{Syl}_p(G) \cap \mathrm{Syl}_p(U) \neq \varnothing$, then $\mathrm{Syl}_p(G) = \mathrm{Syl}_p(U)$.

(b) If $\mathrm{Syl}_p(G) \cap \mathrm{Syl}_p(U) \neq \varnothing$ and $\gcd(|H|, |U|) = 1$, then:

$H$ acts transitively on $\mathrm{Syl}_p(G)$ if and only if $Q \lhd U$ for some $Q \in \mathrm{Syl}_p(G)$.

*Proof.*

(a) Say $P \in \mathrm{Syl}_p(G) \cap \mathrm{Syl}_p(U)$. Now $G$ acts transitively on its Sylow $p$-subgroups by conjugation, so

$$\mathrm{Syl}_p(G) = \{gPg^{-1} : g \in G\}.$$

To argue $\mathrm{Syl}_p(G) \subset \mathrm{Syl}_p(U)$. As $U \lhd G$, we know for all $g \in G$ that $gPg^{-1} \cap U \in \mathrm{Syl}_p(U)$. Being conjugates in $U$, and considering finite order,

$$\left|gPg^{-1}\right| = |P| = \left|gPg^{-1}\right|.$$

It follows that $gPg^{-1} \cap U = gPg^{-1}$, hence $\mathrm{Syl}_p(G) \subset \mathrm{Syl}_p(U)$. The other inclusion is obvious by recognizing that if $|P| = p^k$, then each $P_i \in \mathrm{Syl}_p(G)$ also has order $p^k$, and is thus in $\mathrm{Syl}_p(G)$.

(b) ($\Leftarrow$) If $Q \lhd U$, then $1 = n_p(U) = n_p(G)$. We see $H$ acts transitively (trivially) on the singleton set $\mathrm{Syl}_p(G)$. ($\Rightarrow$) Say that $H$ acts transitively on $\mathrm{Syl}_p(G)$. It's true as well that $U$ acts transitively on $\mathrm{Syl}_p(U)$ (which is identically $\mathrm{Syl}_p(U)$).

Let $Q \in \mathrm{Syl}_p(G)$. We compute the cardinal number of the orbit of $Q$ under the action of $H$ and $U$ respectively:

$$n_p(G) = \frac{|H|}{|N_H(Q)|} \quad \text{and} \quad n_p(G) = \frac{|U|}{|N_U(Q)|}.$$

So the cardinal number of the orbit of $Q$ (which is the number of Sylow $p$-subgroups of both $U$ and $G$) divides both $|H|$ and $|U|$. Since $\gcd(|H|, |U|) = 1$, it must be that $Q$ is the only Sylow $p$-subgroup in $U$ (and, also, the only one in $G$). We conclude $Q \lhd U$. □

1.5. **No simple group of order** $120$. *Given.* Suppose $G$ is a group of order $120$.

*To prove.* $G$ cannot be simple.

*Proof.* Suppose for contradiction $G$ is simple. As $|G| = 2^3 \cdot 3 \cdot 5$, by Sylow we have:

- The minimal permissible index of a proper subgroup of $G$ is $5$,
  - that is, $5 = \min\{k \in \mathbf{N} : |G| \mid k!\}$;
- The number of Sylow $p$-groups must be
  - $n_5 = 6$,
  - $n_3 \in \{10, 40\}$,
  - $n_2 \in \{5, 15\}$.

We consider $n_5 = 6$ to obtain a contradiction. Let $H_5 \in \mathrm{Syl}_5(G)$. Then $G$ acts transitively by conjugation on $G/N_G(H_5)$. I assert

$$G \leqslant S_6$$

by identifying $G$ with its image in $S_6$ afforded by the (necessarily injective) permutation representation $G \to S_6$. As $G$ has no subgroup of index $2$, $G \leqslant A_6$. Since $|A_6| = 6!/2$, it's the case that Sylow $5$-subgroups of $G$ coincide with Sylow $5$-subgroups of $A_6$. It follows that

$$N_{A_6}(H_5) \geqslant N_{A_6}(H_5) \cap G = N_G(H_5)\,.$$

Now, the number of Sylow $5$-subgroups of $S_6$ is given by the number of $5$-cycles divided by the number of $p$-cycles in a Sylow $p$-subgroup. In particular,

$$|N_{A_6}(H_5)| = \frac{1}{2}|N_{S_6}(H_5)| = 10.$$

Yet also $n_5(G) = 6$ is the index of the normalizer of $H_5$ in $G$, hence

$$|N_G(H_5)| = 20.$$

But $N_G(H_5)$ of order $20$ cannot be contained in a group of order $10$—the desired contradiction.

We conclude $n_5$ cannot be $6$ for a simple group $G$ of order $120$. So no such simple group $G$ exists. $\square$

1.6. **Comaximal Ideals.** *Given.* Let $R = I + J$ be a commutative ring with identity where $I$ and $J$ are two ideals.

*To prove.*

(a) $IJ = I \cap J$.

(b) There are instances where $I + J \neq R$ and $IJ \neq I \cap J$.

*Proof.*

(a) To verify $IJ$ is an ideal contained in $I \cup J$.

- $IJ$ is nonempty and closed under addition, following immediately from $IJ$'s definition.
- $IJ$ is closed under multiplication, for let $\sum_1^n x_i y_i \in IJ$ and $r \in R$.
  - Then $r \sum_1^n x_i y_i \sum_1^n \underbrace{(rx_i)}_{\in I} y_i \in IJ$.
- So $IJ$ is an ideal.
- As $I, J$ are ideals, we have $\sum_1^n \underbrace{x_i y_i}_{\in I \cup J} \in I \cup J$.
- Thus $IJ \subset I \cup J$.

To verify that $I \cap J = IJ$, we require the hypotheses that $R$ is a commutative unital ring with comaximal ideals $I$ and $J$.

- Let $z \in I \cap J$.
- As $I + J = R$, we may find $e_I \in I$ and $e_J \in J$ such that $e_I + e_J = 1$.
- Since $I + J$ contains $IJ$, $z \in I + J$.
- Then $z = z \cdot 1 = ze_I + e_J z \in IJ$.
- So $I \cap J \subset IJ$.

(b) Consider $R = \mathbf{Z}$ and $I = J = n\mathbf{Z}$ for $n \in \mathbf{Z}_{\geqslant 2}$. Since $\gcd(n, n) = n$, we have $n\mathbf{Z} + n\mathbf{Z} = n\mathbf{Z} \neq \mathbf{Z}$. Furthermore $IJ = n^2\mathbf{Z}$, yet $I \cap J = n\mathbf{Z}$. □