Honors Algebra **Spring 2025**
HW 5: Fields **2/25/2025**

Abstract Algebra: An Integrated Approach by J.H. Silverman.
Page 151-155: 6.1, 6.7, 6.8, 6.12, 6.16, 6.21, 6.22, 6.26, 6.30, 6.31

Problem 1 (6.1)**.** Let $\psi : G \longrightarrow G'$ be a homomorphism of groups.

(a) Prove that the image $\psi(G) = \{\psi(g) : g \in G\}$ is a subgroup of G'.

Let's verify the subgroup criteria: Closure, Identity, and Inverses.

Let $a, b \in \psi(G)$. Then there exist $g_1, g_2 \in G$ such that $\psi(g_1) = a$ and $\psi(g_2) = b$. Since G is closed under multiplication, $g_1 g_2 \in G$, and thus

$$\psi(g_1 g_2) = \psi(g_1)\psi(g_2) = ab \in \psi(G).$$

Since G has an identity element e_G, applying ψ gives $\psi(e_G)$, which is the identity in G'. Thus, $\psi(G)$ contains the identity of G'.

Let $a \in \psi(G)$. Then $a = \psi(g)$ for some $g \in G$. Since G contains inverses, $g^{-1} \in G$, and applying ψ, we obtain $\psi(g^{-1}) = \psi(g)^{-1} = a^{-1} \in \psi(G)$.

Since all subgroup criteria are satisfied, $\psi(G)$ is a subgroup of G'.

(b) Suppose that G is a finite group. Prove that

$$\#G = \#\psi(G) \cdot \# \ker(\psi)$$

Consider the kernel of ψ, $\ker(\psi) = \{g \in G \mid \psi(g) = e'\}$, which is a normal subgroup of G. By the First Isomorphism Theorem, $G/\ker(\psi) \cong \psi(G)$, so $\#G/\ker(\psi) = \#\psi(G)$.

Since each coset of $\ker(\psi)$ has $\#\ker(\psi)$ elements, the number of cosets is $\#G/\#\ker(\psi)$, which equals $\#\psi(G)$. Rearranging gives the desired result:

$$\#G = \#\psi(G) \cdot \# \ker(\psi).$$

Problem 2 (6.17)**.** Let G be a group, let $K \subseteq H \subseteq G$ be subgroups, and assume that K is a normal subgroup of G.

(a) Prove that H/K is naturally a subgroup of G/K; more precisely, show that there is a natural injective homomorphism $H/K \hookrightarrow G/K$.

Define $\phi : H/K \to G/K$ by $\phi(hK) = hK$ for all $h \in H$. This function is well-defined, as coset multiplication in G/K respects multiplication in G. It is a homomorphism because for $h_1, h_2 \in H$, we have

$$\phi(h_1 K h_2 K) = (h_1 h_2)K = h_1 K h_2 K = \phi(h_1 K)\phi(h_2 K).$$

Injectivity follows because if $hK = K$, then $h \in K$, meaning the kernel of ϕ is trivial. Hence, H/K is isomorphic to its image in G/K and is thus a subgroup.

(b) Conversely, prove that every subgroup of G/K looks like H/K for some subgroup H satisfying $K \subseteq H \subseteq G$.

Let $S \leq G/K$. Define $H = \{g \in G \mid gK \in S\}$. Then H is a subgroup of G, since for $g_1, g_2 \in H$, we have $g_1K, g_2K \in S$, so $g_1g_2K \in S$, implying $g_1g_2 \in H$. Clearly, $K \subseteq H$. Moreover, S corresponds precisely to H/K, proving the claim.

(c) Prove that H is a normal subgroup of G if and only if H/K is a normal subgroup of G/K.

($\Rightarrow$) If H is normal in G, then for all $g \in G$, we have $gHg^{-1} = H$. Taking cosets modulo K, we get $gKH/Kg^{-1}K = H/K$, proving normality in G/K.

($\Leftarrow$) If H/K is normal in G/K, then for all $gK \in G/K$, we have $gKH/Kg^{-1}K = H/K$, meaning $gHg^{-1} \subseteq H$. Thus, H is normal in G.

(d) If H is a normal subgroup of G, prove that

$$\frac{G/K}{H/K} \equiv G/H.$$

(*Hint.* Prove that there is a well-defined surjective homomorphism $G/K \longrightarrow G/H$. What is its kernel?)

Define $\phi : G/K \to G/H$ by $\phi(gK) = gH$. This is well-defined since if $gK = g'K$, then $g^{-1}g' \in K \subseteq H$, implying $gH = g'H$.

This map is a homomorphism because for any $g_1, g_2 \in G$,

$$\phi(g_1Kg_2K) = \phi(g_1g_2K) = g_1g_2H = g_1Hg_2H = \phi(g_1K)\phi(g_2K).$$

The kernel of ϕ is H/K since $\phi(gK) = H$ if and only if $gH = H$, meaning $g \in H$. The First Isomorphism Theorem then gives

$$(G/K)/(H/K) \cong G/H.$$

Problem 3 (6.8)**.** Let G be a group, let $K \subseteq G$ be a normal subgroup of G, and let $H \subseteq H' \subseteq G$ be subgroups of G.

(a) Prove that $H \cap K$ is a normal subgroup of H and similarly that $H' \cap K$ is a normal subgroup of H'.

Since K is normal in G, for all $h \in H$ and $k \in H \cap K$, we have $hkh^{-1} \in K$. Moreover, since $hkh^{-1} \in H$ because $h, k, h^{-1} \in H$, it follows that $hkh^{-1} \in H \cap K$. Thus, $H \cap K$ is normal in H. The same argument applies to $H' \cap K$ in H'.

(b) Prove that $H/(H \cap K)$ is naturally a subgroup of $H'/(H' \cap K)$.

The inclusion $H \subseteq H'$ induces a natural homomorphism

$$H \to H'/(H' \cap K)$$

given by $h \mapsto h(H' \cap K)$. The kernel of this map is precisely $H \cap K$, so the First Isomorphism Theorem gives an injection

$$H/(H \cap K) \hookrightarrow H'/(H' \cap K).$$

Thus, $H/(H \cap K)$ is naturally a subgroup of $H'/(H' \cap K)$.

(c) Suppose further that H is a normal subgroup of H'. Prove that $H/(H \cap K)$ is a normal subgroup of $H'/(H' \cap K)$.

Since H is normal in H', conjugation by any element of H' sends H to itself. Given any $h' \in H'$ and coset $h(H \cap K) \in H/(H \cap K)$, we have

$$h'h(H \cap K)h'^{-1} = (h'hh'^{-1})(H \cap K).$$

Since $h'hh'^{-1} \in H$ (as H is normal in H'), it follows that $h(H \cap K)$ is mapped within $H/(H \cap K)$ under conjugation by elements of $H'/(H' \cap K)$. Thus, $H/(H \cap K)$ is normal in $H'/(H' \cap K)$.

Problem 4 (6.12). Let G be a group that acts on a set X. We say that the action is *doubly transitive* if it has the following property:

For all $x_1, x_2, y_1, y_2 \in X$ with $x_1 \neq x_2$ and $y_1 \neq y_2$, there exists an element $g \in G$ of the group satisfying $gx_1 = y_1$ and $gx_2 = y_2$.

(a) Let Z be the following set of ordered pairs:

$$Z = \{(z_1, z_2) \in X \times X : z_1 \neq z_2\}$$

Let G act on Z by the rule

$$g(z_1, z_2) = (gz_1, gz_2)$$

Prove that the action of G on X is doubly transitive if and only if the action of G on Z is transitive.

Suppose G acts doubly transitively on X. Then, given any two pairs $(x_1, x_2), (y_1, y_2) \in Z$, there exists $g \in G$ such that $gx_1 = y_1$ and $gx_2 = y_2$, showing transitivity on Z.

Conversely, if G acts transitively on Z, then for any distinct elements x_1, x_2 and y_1, y_2, there exists $g \in G$ such that $(gx_1, gx_2) = (y_1, y_2)$. This implies doubly transitive action on X.

(b) For each of the following groups and group actions, determine whether the action is transitive, and also whether the action is doubly transitive:

(1) The symmetric group S_n acting on the set $\{1, 2, \dots, n\}$.

The symmetric group S_n acts transitively and doubly transitively on $\{1, 2, \dots, n\}$ because it can send any pair (x_1, x_2) to any other pair (y_1, y_2) by permutation.

(2) The dihedral group $\mathcal{D}_n$ acting on the vertices of a regular n-gon.

The dihedral group $\mathcal{D}_n$ acts transitively on the vertices of the polygon, but it is not doubly transitive for $n > 3$, as reflections preserve orientation.

(3) A group G acts on itself via left multiplication; i.e., take X to be another copy of G, and let $g \in G$ send $x \in X$ to gx.

The left multiplication action is transitive but not doubly transitive, since left multiplication preserves group structure and does not allow arbitrary swaps of two elements.

Problem 5 (6.16)**.** Let p be a prime. We proved in Corollary 6.26 that a group with p^2 elements must be abelian. Let G be a group with p^3 elements.

(a) Mimic the proof of Corollary 6.26 to try to prove that G is abelian. Where does the proof go wrong?

The proof of Corollary 6.26 relies on the fact that a group of order p^2 has a nontrivial center and that the quotient by this center is cyclic, which forces the group to be abelian. When we attempt to extend this argument to a group of order p^3, we still get a nontrivial center $Z(G)$. If $|Z(G)| = p^2$, then $G/Z(G)$ has order p, which is cyclic, forcing G to be abelian. However, if $|Z(G)| = p$, then $G/Z(G)$ has order p^2, which is not necessarily cyclic. This is where the proof fails.

(b) Give two examples of non-abelian groups with 2^3 elements. (This shows that the proof in (a) can't work).

Two examples of non-abelian groups of order 2^3 are:

- The dihedral group D_4, which consists of the symmetries of a square.
- The quaternion group Q_8, which consists of elements $\{\pm 1, \pm i, \pm j, \pm k\}$ with multiplication rules defined by $i^2 = j^2 = k^2 = ijk = -1$.

Both of these groups have nontrivial centers of order 2 but remain non-abelian.

(c) What sort of information about G can you deduce from the proof in (a) that failed?

Even though the proof does not show that G is abelian, it does establish that $Z(G)$ is nontrivial and that $G/Z(G)$ has order p^2. Since we know that groups of order p^2 are abelian, this means that G is at most a central extension of an abelian group, making it close to being abelian in structure.

(d) **Challenge Problem**. Construct a non-abelian group of order p^3 for every prime p.

One general construction for a non-abelian group of order p^3 is given by the Heisenberg group over $\mathbb{Z}/p\mathbb{Z}$:

$$H_p = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \mid a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}.$$

This group has order p^3 and is non-abelian whenever $p > 1$ because matrix multiplication does not always commute.

Problem 6 (6.21)**.** Let p be prime, and let G be a group of order p^n. Prove that for every $0 \leq r \leq n$, there is a subgroup H of G of order p^r. (*Hint.* Give a proof by induction on n. Use Theorem 6.25, which says that G has a non-trivial center $Z(G)$, and apply the induction hypothesis to G/N, where N is an appropriately chosen subgroup of $Z(G)$).

We prove the result by induction on n.

Base case: When $n = 0$, the trivial group is the only group of order $p^0 = 1$, and it has a subgroup of order $p^0 = 1$.

Inductive step: Assume the statement holds for groups of order p^k for some $k \geq 0$. Let G be a group of order p^{k+1}. By Theorem 6.25, G has a non-trivial center $Z(G)$, which contains a subgroup N of order p. Consider the quotient group G/N, which has order p^k. By the induction hypothesis, for every $0 \leq r \leq k$, there exists a subgroup of G/N of order p^r. The preimage of this subgroup in G under the natural projection map is a subgroup of G of order p^{r+1}. Since N itself is of order p, it is also a valid subgroup. Thus, subgroups of all required orders exist in G.

Problem 7 (6.22)**.** This exercise asks you to give two different proofs of the following stronger version of the first part of Sylow's Theorem.

Theorem. Let G be a finite group, let p be a prime, and suppose that $\#G$ is divisible by p^r. Prove that G has a subgroup of order p^r. (Note that p^r is not required to be the largest power of p that divides G).

(a) Give a proof that directly mimics the proof of Theorem 6.29 by considering the set of all subsets of G that contain p^r elements. But note that if $n > r$, then $\binom{p^n m}{p^r}$ is divisible by p, so you'll need to make some changes in the proof.

Consider the set S of all subsets of G of size p^r. Let's analyze the number of ways to form such subsets.

Define an equivalence relation on S where two subsets are equivalent if they are conjugate under the action of G by left multiplication. The number of such subsets is given by the binomial coefficient $\binom{p^n m}{p^r}$. Since $p^n m$ is divisible by p^r, it follows that for sufficiently large n, this binomial coefficient is divisible by p.

Now, consider the subset stabilizers. By Sylow's counting arguments, the number of such subsets modulo p must be 1, ensuring the existence of a subgroup of order p^r. This construction follows a similar argument to the proof of Theorem 6.29 while modifying it to account for divisibility.

(b) Combine the version of Sylow's Theorem that we did prove with Exercise 6.21. (If you haven't already done Exercise 6.21, now would be a good time to do it!)

From Sylow's Theorem, we know that if p^n is the highest power of p dividing $\#G$, then there exists a Sylow p-subgroup of order p^n.

Exercise 6.21 establishes that if a group G has a normal subgroup of order p^k, then G contains a subgroup of order p^r for any $r \leq k$.

Applying this, we see that G must have a subgroup of order p^r, even if p^r is not the highest power of p dividing $\#G$. Thus, by combining Sylow's Theorem with the result from Exercise 6.21, we conclude the existence of a subgroup of order p^r.

Problem 8 (6.26)**.** This exercise describes a way to create new groups from known groups. Let G be a group. An isomorphism from G to itself is called an *automorphism* of G. The set of automorphisms is denoted

$$\mathrm{Aut}(G) = \{\text{group isomorphisms } G \longrightarrow G\}$$

We define a composition law on $\mathrm{Aut}(G)$ as follows: for $\alpha, \beta \in \mathrm{Aut}(G)$, we define $\alpha\beta$ to be the map from G to G give by $(\alpha\beta)(g) = \alpha(\beta(g))$.

(a) Prove that this composition law makes $\mathrm{Aut}(G)$ into a group.

Let's verify the group axioms for this:

Closure: If $\alpha, \beta \in \mathrm{Aut}(G)$, then $\alpha\beta$ is a composition of two isomorphisms, which is itself an isomorphism. Hence, $\alpha\beta \in \mathrm{Aut}(G)$.

Associativity: For $\alpha, \beta, \gamma \in \mathrm{Aut}(G)$, composition satisfies $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.

Identity element: The identity map $\mathrm{id}_G : G \to G$, given by $\mathrm{id}_G(g) = g$, is an automorphism and serves as the identity.

Inverses: If $\alpha \in \mathrm{Aut}(G)$, then α^{-1} exists and is also an automorphism, ensuring that each element has an inverse.

Thus, $\mathrm{Aut}(G)$ is a group.

(b) Let $a \in G$. Define a map ϕ_a from G to G by the formula

$$\phi_a : G \longrightarrow G, \quad \phi_a(g) = aga^{-1}$$

Prove that $\phi_a \in \mathrm{Aut}(G)$ and that the map (6.23 below)

$$G \longrightarrow \mathrm{Aut}(G), \quad a \longmapsto \phi_a$$

is a group homomorphism.

We check that $\phi_a(g) = aga^{-1}$ is an automorphism:

Homomorphism property: For any $g_1, g_2 \in G$,

$$\phi_a(g_1 g_2) = a g_1 g_2 a^{-1} = (a g_1 a^{-1})(a g_2 a^{-1}) = \phi_a(g_1)\phi_a(g_2).$$

Invertibility: The inverse of ϕ_a is $\phi_{a^{-1}}$, since $\phi_{a^{-1}}(\phi_a(g)) = a^{-1}(aga^{-1})a = g$.

The mapping $a \mapsto \phi_a$ respects group operation:

$$\phi_{ab}(g) = (ab)g(ab)^{-1} = a(bgb^{-1})a^{-1} = \phi_a(\phi_b(g)),$$

so it is a homomorphism.

(c) Prove that the kernel of homomorphism (6.23) is the center $Z(G)$ of G.

The kernel consists of elements $a \in G$ such that ϕ_a is the identity map, meaning $aga^{-1} = g$ for all $g \in G$. This holds precisely when a commutes with all elements of G, i.e., $a \in Z(G)$. Hence, $\ker(\phi) = Z(G)$.

(d) Elements of $\mathrm{Aut}(G)$ that are equal to ϕ_a for some $a \in G$ are called *inner automorphisms*, and all other elements of $\mathrm{Aut}(G)$ are called *outer automorphisms*. Prove that G is abelian if and only if its only inner automorphism is the identity map.

If G is abelian, then $aga^{-1} = g$ for all $a, g \in G$, implying that all ϕ_a are the identity map, making all inner automorphisms trivial. Conversely, if the only inner automorphism is the identity, then $aga^{-1} = g$, meaning G is abelian.

(e) More generally, if H is a normal subgroup of G, prove that there is a well-defined group homomorphism

$$G \longrightarrow \mathrm{Aut}(H), \quad a \mapsto \phi_a, \quad \text{where } \phi_a(h) = aha^{-1},$$

and that the kernel of this homomorphism is the centralizer of H in G.

The function $G \to \mathrm{Aut}(H)$ given by $a \mapsto \phi_a$ is well-defined because H is normal, ensuring that conjugation preserves H. The kernel consists of elements commuting with all of H, which defines the centralizer $C_G(H)$ of H in G.

Problem 9 (6.30). Let p and q be odd primes with $q < p$, and let G be a finite group with $\#G = p^n q$ for some $n \geq 1$. Let H_p be a p-Sylow subgroup, and let H_q be a q-Sylow subgroup.

(a) If $q \not\equiv 1 \pmod{p}$, prove that H_p is a normal subgroup of G.

By Sylow's theorems, the number of Sylow p-subgroups, denoted n_p, satisfies $n_p \equiv 1 \pmod{p}$ and divides q. Since q is a prime, the divisors of q are 1 and q. If $n_p = 1$, then H_p is unique and thus normal in G. Suppose for contradiction that $n_p = q$. Then $q \equiv 1 \pmod{p}$, contradicting the assumption that $q \not\equiv 1 \pmod{p}$. Thus, $n_p = 1$, and H_p is normal in G.

(b) If $n = 3$ and $q \equiv 2 \pmod{3}$, prove that H_q is a normal subgroup of G. (*Hint.* You may need to use the fact that -3 is not a square modulo q, which is a special case of quadratic reciprocity).

By Sylow's theorems, the number of Sylow q-subgroups, n_q, satisfies $n_q \equiv 1 \pmod{q}$ and divides p^3. Thus, n_q is either 1, p, p^2, or p^3. If $n_q = 1$, then H_q is normal. Suppose for contradiction that $n_q > 1$. Then $n_q \equiv 1 \pmod{q}$ implies that $p^k \equiv 1 \pmod{q}$ for some $k \in \{1, 2, 3\}$. Since $q \equiv 2 \pmod{3}$, the claim follows from the given hint that -3 is not a quadratic residue modulo q. This forces $n_q = 1$, implying that H_q is normal in G.

Problem 10 (6.31)**.** Let p and q be distinct primes, and let G be a group of order $p^2 q$. Let H_p be a p-Sylow subgroup, and let H_q be a q-Sylow subgroup. Prove that at least one of H_p and H_q is a normal subgroup of G.

By Sylow's theorems, n_p (the number of Sylow p-subgroups) satisfies $n_p \equiv 1 \pmod{p}$ and divides q, so $n_p \in \{1, q\}$. Similarly, n_q satisfies $n_q \equiv 1 \pmod{q}$ and divides p^2, so $n_q \in \{1, p, p^2\}$. If either $n_p = 1$ or $n_q = 1$, then the corresponding Sylow subgroup is normal. If $n_p = q$ and $n_q > 1$, then $n_q \equiv 1 \pmod{q}$ forces $p^k \equiv 1 \pmod{q}$, which contradicts the assumption that p and q are distinct primes. Hence, at least one of H_p or H_q must be normal in G.