MATH 1530 Problem Set 6

Tanish Makadia

(Collaborated with Esmé and Kazuya)

March 2023

Problem 1. Let G be a finite Abelian group and let n be a positive integer that is relatively prime to $|G|$. Prove that the mapping $a \mapsto a^n$ is an automorphism of G.

Proof. Define $\alpha : G \to G$ such that $a \mapsto a^n$. Let $g, h \in G$.

1. **Injective:** Suppose $g^n = h^n$.

$$\begin{aligned} g^n = h^n &\implies e = g^n h^{-n} \\ &\implies e = (gh^{-1})^n \\ &\implies |gh^{-1}| \mid n \end{aligned}$$

   Additionally, $gh^{-1} \in G$. By *Lagrange's Theorem*, we have $|gh^{-1}| \mid |G|$. Since $|gh^{-1}|$ divides both n and $|G|$, and $\gcd(n, |G|) = 1$, we have that $|gh^{-1}| = 1$. Therefore, $gh^{-1} = e \implies g = eh \implies g = h$.

2. **Surjective:** Consider g^n. We have that $g \mapsto g^n$.

3. **Preserves Group Operation:** $\alpha(gh) = (gh)^n = g^n h^n = \alpha(g) \cdot \alpha(h)$.

□

Problem 2. Let G be a group of order pqr, where p, q, r are distinct primes. If H is a subgroup of G of order pq and K is a subgroup of G of order qr, prove that $|H \cap K| = q$.

Proof. We have already proven that $H \cap K$ is a subgroup of G. This implies that $H \cap K$ is also a subgroup of H and K. By *Lagrange's Theorem*, we have that

$$|H \cap K| \mid |H|, |K| \implies |H \cap K| \mid pq, qr$$

Therefore, $|H \cap K|$ is either 1 or q. Assume for contradiction that $|H \cap K| = 1$. By lemma 1, we have that

$$|HK| = \frac{pq \cdot qr}{1} = pq^2r$$

which is a contradiction since HK is a subset of G, which implies that $|HK| \leq |G|$. Therefore, we have shown that $|H \cap K| = q$ as desired. □

Lemma 1. *Let H and K be subgroups of a finite group G. Then,*

$$|HK| = \frac{|H||K|}{|H \cap K|} \text{ where } HK = \{hk \mid h \in H,\ k \in K\}$$

Proof. We can separate HK into a union of left cosets of K in G:

$$HK = \bigcup_{h \in H} hK$$

By the properties of cosets, we have that $hK = h'K$ or $hK \cap h'K = \emptyset$ for all $h, h' \in H$. We must now determine how many of these cosets are distinct.

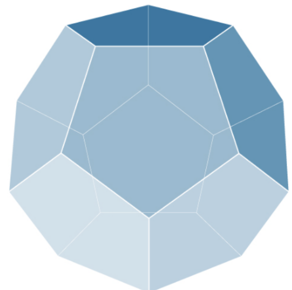
Suppose $hK = h'K$ for some $h, h' \in H$. Since $hK = h'K \Leftrightarrow h^{-1}h' \in K$, we have that $h^{-1}h' = k$ for some $k \in K$. This implies that $k \in H \implies k \in H \cap K$. Additionally, $h' = hk$. Thus, there are $|H \cap K|$ ways to create the same coset for each $h' \in H$ (by *Cayley's Theorem*, we know that each $k \in H \cap K$ has exactly one corresponding $h \in H$ such that $hk = h'$). Therefore, the number of distinct cosets hK where $h \in H$ is $|H|/|H \cap K|$.

Since $|hK| = |h'K|$ for all $h, h' \in H$, the number of elements in each coset is $|hK| = |K|$. Therefore, the cardinality of HK equals the number of distinct cosets times the number of distinct elements in each coset, giving us

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

□

Problem 3. Calculate the order of the group of rotations of a regular dodecahedron:



Proof. Let G be the rotation group of the dodecahedron. Assign each of the 12 faces of the dodecahedron a unique number $1-12$. Since every rotation must take each face to exactly one other face, G is a group of permutations on the set $\{1,\dots,12\}$.

Consider a single face, $\mathsf{f} \in \{1,\dots,12\}$, of the dodecahedron. By the *orbit-stabilizer theorem*, we have that

$$|\mathsf{G}| = |\mathsf{orb}_\mathsf{G}(\mathsf{f})| \cdot |\mathsf{stab}_\mathsf{G}(\mathsf{f})|$$

1. $|\mathbf{orb_G}(\mathbf{f})|$: Picking an axis of rotation through the centers of any two parallel faces allows us to bring f to any other face $\mathsf{f}' \in \{1,\dots,12\}$. Therefore, $\mathsf{orb}_\mathsf{G}(\mathsf{f}) = \{1,\dots,12\}$ which implies that $|\mathsf{orb}_\mathsf{G}(\mathsf{f})| = 12$.

2. $|\mathbf{stab_G}(\mathbf{f})|$: Let $\overline{\mathsf{f}} \in \{1,\dots,12\}$ be the face parallel to f. Picking an axis of rotation through the centers of f and $\overline{\mathsf{f}}$ allows us to rotate the dodecahedron in 5 distinct ways while fixing the position of f. This implies that $|\mathsf{stab}_\mathsf{G}(\mathsf{f})| = 5$.

Together, we have $|\mathsf{G}| = 12 \cdot 5 = 60$. $\square$

Problem 4. Determine the number of cyclic subgroups of order 15 in $\mathbb{Z}_{90} \oplus \mathbb{Z}_{36}$.

Proof. A cyclic subgroup of order 15 has $\phi(15) = 8$ distinct elements of order 15. We will now determine the number of distinct elements of order 15 in $\mathbb{Z}_{90} \oplus \mathbb{Z}_{36}$.

Let $(g_1, g_2) \in \mathbb{Z}_{90} \oplus \mathbb{Z}_{36}$ such that $|(g_1, g_2)| = 15$. By *(Gallian, Theorem 8.1)*, we have that $\operatorname{lcm}(|g_1|, |g_2|) = 15$. For each of the resulting cases, we can use the *Euler phi function* since $\mathbb{Z}_{90}$ and $\mathbb{Z}_{36}$ are both cyclic.

1. **($|g_1| = 5$, $|g_2| = 3$):**
   - $\phi(5) = 4 \implies 4$ distinct elements of order 5 in $\mathbb{Z}_{90}$.
   - $\phi(3) = 2 \implies 2$ distinct elements of order 3 in $\mathbb{Z}_{36}$.

   Therefore, we have $4 \cdot 2 = 8$ ways to make (g_1, g_2) from this case.
2. **($|g_1| = 15$, $|g_2| = 1$):**
   - $\phi(15) = 8 \implies 8$ distinct elements of order 15 in $\mathbb{Z}_{90}$.
   - $\phi(1) = 1 \implies 1$ distinct element of order 1 in $\mathbb{Z}_{36}$.

   So there are $8 \cdot 1 = 8$ ways to make (g_1, g_2) from this case.
3. **($|g_1| = 15$, $|g_2| = 3$):** From above, we have 8 distinct elements of order 15 in $\mathbb{Z}_{90}$, and 2 distinct elements of order 3 in $\mathbb{Z}_{36}$. Hence, there are $8 \cdot 2 = 16$ ways to make (g_1, g_2) from this case.

In total, there are $8 + 8 + 16 = 32$ distinct elements of order 15 in $\mathbb{Z}_{90} \oplus \mathbb{Z}_{36}$. Since each cyclic subgroup of order 15 is disjoint and has 8 distinct elements of order 15 which can generate it, the number of cyclic subgroups of order 15 in $\mathbb{Z}_{90} \oplus \mathbb{Z}_{36}$ is $32/8 = 4$. $\square$

Problem 5. Let p and q be odd primes and let m and n be positive integers. Prove that $U(p^m) \oplus U(q^n)$ is not cyclic. [hint: read the book to find a useful result we didn't cover in class]

Proof. By *(Gallian, pg. 160)*, we have that $U(p^m) \approx \mathbb{Z}_{p^m - p^{m-1}}$ and $U(q^n) \approx \mathbb{Z}_{q^n - q^{n-1}}$. Because $\mathbb{Z}_{p^m - p^{m-1}}$ and $\mathbb{Z}_{q^n - q^{n-1}}$ are both cyclic, we have that $U(p^m)$ and $U(q^n)$ are cyclic as well. Therefore, by *(Gallian, Theorem 8.2)*, we must show that $|U(p^m)|$ and $|U(q^n)|$ are not relatively prime.

By lemma 3, we have that $|U(p^m)| = p^m - p^{m-1}$ and $|U(q^n)| = q^n - q^{n-1}$. Since the product of odds is odd, p^m, p^{m-1}, q^n, and q^{n-1} must all be odd. Since the difference of odds is even, we have that $2 \mid p^m - p^{m-1}, q^n - q^{n-1} \implies \gcd(p^m - p^{m-1}, q^n - q^{n-1}) \neq 1$. Therefore, $|U(p^m)|$ and $|U(q^n)|$ are not relatively prime, which means $|U(p^m)| \oplus |U(q^n)|$ is not cyclic. $\square$

Lemma 2. *Let* p *be an odd prime. Then* $\mathsf{U}(\mathsf{p}^n) \approx \mathbb{Z}_{\mathsf{p}^n - \mathsf{p}^{n-1}}$.

Proof. By lemma 3, we have that $|\mathsf{U}(\mathsf{p}^n)| = \mathsf{p}^n - \mathsf{p}^{n-1}$. We can arrange the elements of $\mathsf{U}(\mathsf{p}^n)$ in ascending order so that $\mathsf{U}(\mathsf{p}^n) = \{u_1, \ldots, u_{\mathsf{p}^n - \mathsf{p}^{n-1}}\}$ where $j < k \implies u_j < u_k$. Similarly, we can arrange the elements of $\mathbb{Z}_{\mathsf{p}^n - \mathsf{p}^{n-1}}$ in ascending order so that $\mathbb{Z}_{\mathsf{p}^n - \mathsf{p}^{n-1}} = \{z_1, \ldots, z_{\mathsf{p}^n - \mathsf{p}^{n-1}}\}$ where $j < k \implies z_j < z_k$.

Define a mapping $\phi : \mathsf{U}(\mathsf{p}^n) \to \mathbb{Z}_{\mathsf{p}^n - \mathsf{p}^{n-1}}$ such that $u_i \mapsto z_i$. We will now show that ϕ is an isomorphism. Let $z_m, z_n \in \mathbb{Z}_{\mathsf{p}^n - \mathsf{p}^{n-1}}$.

1. **Injective:** to be proved ...
2. **Surjective:** to be proved ...
3. **Preserves Group Operation:** $\phi(u_m \cdot u_n) = \phi((u_m u_n)) = \ldots$ to be proved

□

Lemma 3. *Let* p *be an odd prime. Then* $\phi(\mathsf{p}^n) = \mathsf{p}^n - \mathsf{p}^{n-1}$.

Proof. We will show $|\mathsf{U}(\mathsf{p}^n)| = \mathsf{p}^n - \mathsf{p}^{n-1}$. Of course, there are p^n integers up to p^n. Therefore, $|\mathsf{U}(\mathsf{p}^n)| = \mathsf{p}^n - m$ where m is the number of integers in the set $\{1, \ldots, \mathsf{p}^n\}$ that are not relatively prime with p^n. Evidently, the prime factorization of p^n only contains the prime p. This implies that p divides every integer that is not relatively prime with p^n. The number of such integers in the set $\{1, \ldots, \mathsf{p}^n\}$ is p^n/p. Therefore,

$$|\mathsf{U}(\mathsf{p}^n)| = \mathsf{p}^n - m = \mathsf{p}^n - \frac{\mathsf{p}^n}{\mathsf{p}} = \mathsf{p}^n - \mathsf{p}^{n-1}$$

□