January 2020

martes, 20 de diciembre de 2022 5:50 p.m.

① Let p be a prime number.

(a) Show every group of order p^n where $n \geq 1$ has nontrivial center.

Pf: Let G be a finite group s.t. $|G| = p^n$, p prime, $n \geq 1$.
Let G act on itself by conjugation.
Then by fixed point congruence, we have
$|G| \equiv |Fix_G(G)| \mod p \Rightarrow |G| \equiv |Z(G)| \mod p$.
Observe that $|G| = p^n \equiv 0 \mod p \Rightarrow |Z(G)| \equiv 0 \mod p$
$\Rightarrow p \mid |Z(G)|$
Since $|Z(G)| \geq 1$ and $p \mid |Z(G)|$, we get that $|Z(G)| \geq p$.
Therefore, G has a nontrivial center ($Z(G) \neq \{1\}$). □

(b) Use part (a) to show every group whose order is p^2 is abelian.

Pf: Let G be a finite group s.t. $|G| = p^2$.
Since G is a p-group, by part (a), we have that $Z(G)$ is nontrivial.
Therefore, $|Z(G)| = p$ or $|Z(G)| = p^2$.
If $|Z(G)| = p^2$, then since $Z(G) \leq G$, we have $Z(G) = G$.
Thus, G is abelian.
If $|Z(G)| = p$, then $\left|G/Z(G)\right| = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p$
$\Rightarrow G/Z(G) \cong \mathbb{Z}/p\mathbb{Z}$, so $G/Z(G)$ is cyclic.
Therefore, G is abelian. □

* $G/Z(G)$ cyclic $\Rightarrow$ G is abelian.

---

② For $a \in \mathbb{Z}$ and $u = (u_1, u_2, u_3) \in \mathbb{R}^3$, define $a * u = (u_1, au_1 + u_2, a^2u_1 + 2au_2 + u_3)$.

(a) Prove the above formula defines an action of the additive group $(\mathbb{Z}, +)$ on $\mathbb{R}^3$.

Pf: We WTS that for $0 \in \mathbb{Z}$ and $u \in \mathbb{R}^3$, $0 * u = u$, and that for $a, b \in \mathbb{Z}$ and $u \in \mathbb{R}^3$, $a*(b*u) = (a+b)*u$.

- First, let $0 \in \mathbb{Z}$ and $u = (u_1, u_2, u_3) \in \mathbb{R}^3$: (0 is the additive identity)
$0*(u_1,u_2,u_3) = (u_1, 0 \cdot u_1 + u_2, 0^2 \cdot u_1 + 2 \cdot 0 \cdot u_2 + u_3) = (u_1, u_2, u_3)$ ✓
- Now let $a, b \in \mathbb{Z}$ and $u = (u_1,u_2,u_3) \in \mathbb{R}^3$:
$a*(b*(u_1,u_2,u_3)) = a*(u_1, bu_1+u_2, b^2u_1 + 2bu_2 + u_3)$
$= (u_1, au_1 + bu_1 + u_2, a^2u_1 + 2a(bu_1+u_2) + b^2u_1 + 2bu_2 + u_3)$
$= (u_1, (a+b)u_1 + u_2, a^2u_1 + 2abu_1 + 2au_2 + b^2u_1 + 2bu_2 + u_3)$
$= (u_1, (a+b)u_1 + u_2, (a+b)^2u_1 + 2(a+b)u_2 + u_3)$

$(a+b)*(u_1,u_2,u_3) = (u_1, (a+b)u_1 + u_2, (a+b)^2u_1 + 2(a+b)u_2 + u_3)$
$\Rightarrow a*(b*u) = (a+b)*u$ ✓
Therefore, the above formula defines an action of the additive group $(\mathbb{Z},+)$ on $\mathbb{R}^3$. □

(b) Show a vector $u = (u_1,u_2,u_3)$ in $\mathbb{R}^3$ has a finite $\mathbb{Z}$-orbit for this action if and only if $u_1 = u_2 = 0$.

Pf: If $u_1 = u_2 = 0$, then $u = (0,0,u_3)$.
Let $a \in \mathbb{Z}$. Then $a*u = a*(0,0,u_3) = (0,0,u_3)$, so u has a finite $\mathbb{Z}$-orbit for this action.
Assume that $u = (u_1,u_2,u_3)$ in $\mathbb{R}^3$ has a finite $\mathbb{Z}$-orbit for this action.
Then there exists a nonzero $a \in \mathbb{Z}$ s.t. $a*u = u$.
$a*u = (u_1, au_1+u_2, a^2u_1 + 2au_2 + u_3) = (u_1,u_2,u_3)$
$\Rightarrow au_1 + u_2 = u_2 \Rightarrow u_1 = 0$ ($au_1 = 0$, since $a \neq 0 \Rightarrow u_1 = 0$)
$\Rightarrow a^2u_1 + 2au_2 + u_3 = u_3 \Rightarrow u_1 = 0, u_2 = 0$
(we know $u_1 = 0$, so $2au_2 + u_3 = u_3 \Rightarrow 2au_2 = 0$
$\Rightarrow u_2 = 0$ since $a \neq 0$)
Therefore, u has to equal $(0,0,u_3)$, i.e., $u_1 = u_2 = 0$. □

---

③ The goal of this problem is to classify all groups of order 35 up to isomorphism.

(a) Determine all abelian groups of order 35 up to isomorphism.

Pf: $35 = 5 \cdot 7$
By the fundamental thm. for finitely generated abelian groups, the only abelian group of order 35 is $\mathbb{Z}/35\mathbb{Z}$, which is isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ since $(5,7) = 1$. □

(b) Show that every group of order 35 is abelian.

Pf: Let G be a finite group w/ $|G| = 35 = 5 \cdot 7$.
By the first Sylow theorem, there exists a 5-Sylow subgp. P w/ $|P| = 5$ and a 7-Sylow subgp. Q w/ $|Q| = 7$.
By the third Sylow theorem, we have
$n_5 \equiv 1 \mod 5$ and $n_5 \mid 7 \Rightarrow n_5 = 1$
$n_7 \equiv 1 \mod 7$ and $n_7 \mid 5 \Rightarrow n_7 = 1$
} P and Q are the unique 5-Sylow and 7-Sylow subgroups, respectively
$\Rightarrow P \triangleleft G, Q \triangleleft G$
Since $P \triangleleft G$ (and $Q \triangleleft G$), it follows that PQ is a subgroup of G.
Observe that $|P \cap Q| = 1$: $P \cap Q \subset P$ and $P \cap Q \subset Q$, so by Lagrange's thm, $|P \cap Q| \mid |P|$ and $|P \cap Q| \mid |Q|$, but $(|P|, |Q|) = (5,7) = 1$, so $|P \cap Q| = 1$.
Therefore, $|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{5 \cdot 7}{1} = 35 = |G| \Rightarrow PQ = G$.
Note that $|P| = 5$, so P is abelian (cyclic b/c 5 is prime) and $|Q| = 7$, so Q is abelian (cyclic b/c 7 is prime).
We want to show that the elements of P and Q commute:
Let $x \in P, y \in Q$. Then
$xyx^{-1}y^{-1} = xyx^{-1}y^{-1} \in P \cap Q = \{1\} \Rightarrow xyx^{-1}y^{-1} = 1 \Rightarrow xy = yx$.
($x \in P$; $yx^{-1}y^{-1} \in P$ since $P \triangleleft G$; $xyx^{-1} \in Q$ since $Q \triangleleft G$; $y^{-1} \in Q$)
Therefore, the elements of P and Q commute with each other.
Thus, we conclude that G is abelian. □

---

④ Let I be the ideal $(7, 1+\sqrt{-13})$ in $\mathbb{Z}[\sqrt{-13}]$.

(a) Show the ring homomorphism $\mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}[\sqrt{-13}]/I$ given by $a \mod 7\mathbb{Z} \mapsto a \mod I$ is an isomorphism.

Pf: Let $\varphi: \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}[\sqrt{-13}]/(7, 1+\sqrt{-13})$ given by
$a \mod 7\mathbb{Z} \mapsto a \mod I = (7, 1+\sqrt{-13})$
We are given that φ is a ring homomorphism, so it remains to show that φ is bijective.
Injective: $\ker(\varphi) = \{a \in \mathbb{Z}/7\mathbb{Z} : \varphi(a) = 0\}$
$= \{a \in \mathbb{Z}/7\mathbb{Z} : a \mod 7 \mapsto 0 \mod I\} \Rightarrow a \equiv 0 \mod 7$
Therefore, $\ker(\varphi)$ is trivial.
Surjective: Let $a + b\sqrt{-13} \in \mathbb{Z}[\sqrt{-13}]/I$, then for all $a, b \in \mathbb{Z}$
$a + b\sqrt{-13} \equiv a + b(-1) \mod (1+\sqrt{-13})$
$\equiv a - b \mod (1+\sqrt{-13})$
and then we are left with $a - b \mod 7$ in $\mathbb{Z}[\sqrt{-13}]/I$, where $a, b \in \mathbb{Z}$.
There exists $a - b \in \mathbb{Z}/7\mathbb{Z}$ s.t. $a - b \mod 7 \mapsto a - b \mod I$
Therefore, φ is surjective.
Thus, φ is a bij. hom., so $\mathbb{Z}/7\mathbb{Z} \cong \mathbb{Z}[\sqrt{-13}]/I$ □

(b) Show I is not principal.

Pf: Suppose that $(7, 1+\sqrt{-13}) = (\alpha)$ for some $\alpha \in \mathbb{Z}[\sqrt{-13}]$.
Then $7 \in (\alpha)$, so $7 = \alpha\beta$ for some $\beta \in \mathbb{Z}[\sqrt{-13}]$.
By taking norms, we get:
$N(7) = 49 = N(\alpha)N(\beta) \Rightarrow N(\alpha) = \pm 7$
(if $N(\alpha) = \pm 1$, then $(\alpha) = \mathbb{Z}[\sqrt{-13}]$)
We also have $1+\sqrt{-13} \in (\alpha)$, so $1+\sqrt{-13} = \alpha\gamma$ for some $\gamma \in \mathbb{Z}[\sqrt{-13}]$.
By taking norms, we get:
$N(1+\sqrt{-13}) = (1+\sqrt{-13})(1-\sqrt{-13}) = 14 = N(\alpha)N(\gamma)$
Let $\alpha = a + b\sqrt{-13}$. Then $N(\alpha) = a^2 + 13b^2$.
If $N(\alpha) = \pm 7$, then $a^2 + 13b^2 = \pm 7$ has a solution in $\mathbb{Z}$.
$a^2 + 13b^2 \neq -7$ since $a^2 + 13b^2 \geq 0$
$a^2 + 13b^2 \neq 7$ for any $a, b \in \mathbb{Z}$
} Therefore, there is no elt. in $\mathbb{Z}[\sqrt{-13}]$ with norm ± 7.
Therefore, $(7, 1+\sqrt{-13}) \neq (\alpha)$
Thus, the ideal I is not principal. □

---

⑤ Let p be a prime number.

(a) Prove $\mathbb{Z}[x]/p\mathbb{Z}[x] \cong (\mathbb{Z}/p\mathbb{Z})[x]$ as rings.

Pf: Let $\varphi: \mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$ by $f(x) \mapsto f(x) \mod p$ be the redn. map, so φ is a homomorphism and it is onto.
Then $\ker(\varphi) = \{f(x) \in \mathbb{Z}[x] : \varphi(f(x)) = 0 \mod p\} = p\mathbb{Z}[x]$ since $\varphi(f(x)) = 0$ only if $f(x)$ reduces to $0 \mod p$, which only happens if $f(x)$ has p-multiple coefficients, i.e., $f(x) \in p\mathbb{Z}[x]$.
Therefore, by the first isom. thm., we get that $\mathbb{Z}[x]/p\mathbb{Z}[x] \cong (\mathbb{Z}/p\mathbb{Z})[x]$. □

(b) Prove that a maximal ideal in $\mathbb{Z}[x]$ that contains p must have the form $(p, f(x))$ where $f(x)$ is monic in $\mathbb{Z}[x]$ and $f(x) \mod p$ is irreducible in $(\mathbb{Z}/p\mathbb{Z})[x]$.

Pf: By part (a), we have that $\mathbb{Z}[x]/p\mathbb{Z}[x] \cong (\mathbb{Z}/p\mathbb{Z})[x]$.
In order for an ideal M containing p to be maximal, we need to have $\mathbb{Z}[x]/M$ is a field.
Note that $\mathbb{Z}/p\mathbb{Z}$ is a field, but $(\mathbb{Z}/p\mathbb{Z})[x]$ is not, so we want to mod out by a polynomial s.t. $(\mathbb{Z}/p\mathbb{Z})[x]/(f(x)) \cong \mathbb{Z}/p\mathbb{Z}$, $f(x) \in \mathbb{Z}[x]$.
Since the ideal M contains p, the surjective homomorphism $\mathbb{Z}[x] \to \mathbb{Z}[x]/M$ kills p and thus induces a surjective ring homomorphism: $\varphi: (\mathbb{Z}/p\mathbb{Z})[x] \to \mathbb{Z}[x]/M$
The $\ker(\varphi) = \{\pi(x) \in (\mathbb{Z}/p\mathbb{Z})[x] : \varphi(\pi(x)) = 0 \text{ in } \mathbb{Z}[x]/M\}$ has to be maximal in $(\mathbb{Z}/p\mathbb{Z})[x]$, so it is $(\pi(x))$ for some monic irreducible $\pi(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$.
Let $f(x)$ be a monic lifting of $\pi(x)$ to $\mathbb{Z}[x]$:
$f(x)$ is monic and $\pi(x) = \overline{f(x)}$ in $(\mathbb{Z}/p\mathbb{Z})[x]$.
That $\varphi(\pi(x)) = 0$ in $\mathbb{Z}[x]/M$ implies that $f(x) \equiv 0 \mod M$, so the monic irreducible $f(x)$ must also be in the maximal ideal, i.e., $f(x) \in M$ in $\mathbb{Z}[x]$. Therefore, $M = (p, f(x))$.
Thus, a maximal ideal in $\mathbb{Z}[x]$ that contains p must have the form $(p, f(x))$ where $f(x)$ is monic in $\mathbb{Z}[x]$ and $f(x) \mod p$ is irred. in $(\mathbb{Z}/p\mathbb{Z})[x]$. □

---

⑥ Give examples as requested, with justification.

(a) A nonabelian group of order 21.

Pf: Consider the semidirect product $G = \mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$ with
$\varphi: \mathbb{Z}/3\mathbb{Z} \to Aut(\mathbb{Z}/7\mathbb{Z}) \cong (\mathbb{Z}/7\mathbb{Z})^\times$. ($|Aut(\mathbb{Z}/7\mathbb{Z})| = |(\mathbb{Z}/7\mathbb{Z})^\times| = 6$)
$|\varphi(1)| \mid 3$, so $\varphi(1) = 1$ or 3
If $\varphi(1) = 1$, then we get the trivial hom.
Since $3 \mid |Aut(\mathbb{Z}/7\mathbb{Z})|$ $(3 \mid 6)$, we have the nontrivial hom. given by $|\varphi(1)| = 3$.
(this means ∃ a nontrivial hom. φ)
Therefore, $\mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$ is a nonabelian group of order 21. □

(b) An expression of (12345) as a product of transpositions.

Pf: Consider $(12)(23)(34)(45)$.
Then $(12)(23)(34)(45) = (12345)$.
Thus, $(12)(23)(34)(45)$ is an expression of (12345) as a product of transpositions. □

(c) Gaussian integers γ and ρ s.t. $7 + 2i = (2+3i)\gamma + \rho$ and $N(\rho) < N(2+3i)$.

Pf: $\frac{7+2i}{2+3i} \cdot \frac{(2-3i)}{(2-3i)} = \frac{14 - 21i + 4i + 6}{4+9} = \frac{20 - 17i}{13} = \frac{20}{13} - \frac{17i}{13}$.
Let $\gamma = 1 - i$. Then $\rho = 7 + 2i - (2+3i)(1-i)$
$= 7 + 2i - (2 - 2i + 3i + 3)$
$= 7 + 2i - (5 + i)$
$= 2 + i$.
$N(\rho) = N(2+i) = (2+i)(2-i) = 5$
$N(2+3i) = (2+3i)(2-3i) = 13$
} $N(\rho) = 5 < 13 = N(2+3i)$ ✓
Check: $7 + 2i = (2+3i)(1-i) + (2+i)$ ✓
Therefore, $\gamma = 1 - i$ and $\rho = 2 + i$. □

(d) A homomorphism of commutative rings $f: R \to S$ and an ideal I in R such that $f(I)$ is not an ideal in S.

Pf: Let $R = \mathbb{Z}$ and $S = \mathbb{Q}$, so $f: \mathbb{Z} \to \mathbb{Q}$ is the inclusion map.
Then $\mathbb{Z}$ is an ideal in $\mathbb{Z}$
Observe that $f(\mathbb{Z})$ is not an ideal of $\mathbb{Q}$ b/c the only ideals of $\mathbb{Q}$ are (0) and $\mathbb{Q}$. □