January 2018

~~viernes, 30 de diciembre de 2022~~ 3:49 p.m.

① Prove every group of order $2p$, where p is an odd prime, is either cyclic or is isomorphic to the dihedral group.

Pf: Let G be a group s.t. $|G| = 2p$, p odd prime.

Then by the first Sylow thm., G has a 2-Sylow subgp and a p-Sylow subgp.
By the third Sylow thm, we have that
$n_2 \equiv 1 \bmod 2$ and $n_2 \mid p \Rightarrow n_2 = 1$ or p
$n_p \equiv 1 \bmod p$ and $n_p \mid 2 \Rightarrow n_p = 1$.
Therefore, the p-Sylow subgp. is normal in G.
Let H be the p-Sylow subgp. and let K be the 2-Sylow subgp.
So $|H| = p$ and $H \cong \mathbb{Z}/p\mathbb{Z}$ and $|K| = 2$ and $K \cong \mathbb{Z}/2\mathbb{Z}$.
Since $H, K \leq G$ and $H \trianglelefteq G$, we have that $HK \leq G$.
Since $|HK| = \dfrac{|H||K|}{|H \cap K|} = \dfrac{p \cdot 2}{1} = 2p$, we have that $G = HK$.
($H \cap K \subset H$ and $H \cap K \subset K$, so $|H \cap K| \mid |H| = p$ and $|H \cap K| \mid |K| = 2$ by Lagrange's thm, so $|H \cap K| = 1$ since $(2, p) = 1$.)
Since $H \trianglelefteq G$, $HK = G$, and $H \cap K = 1$, by the recognition thm we have that G is realized by $H \rtimes_\varphi K$ by $\varphi: K \to \operatorname{Aut}(H)$.
We know that $|\varphi(1)| \mid 2$, so $|\varphi(1)| = 1$ or 2.
If $|\varphi(1)| = 1$, then φ is the trivial homomorphism and we have a direct product $H \times K \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which is cyclic.
Now suppose $|\varphi(1)| = 2$.
Observe that $\varphi: K \to \operatorname{Aut}(H)$ is the same as
$\varphi: \mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, where $|(\mathbb{Z}/p\mathbb{Z})^\times| = p-1$ which is even since p is an odd prime, so $2 \mid (p-1)$.
Let $\varphi(1) = x$. Then $x^2 = 1$ since $|\varphi(1)| = 2$.
$\Rightarrow x^2 \equiv 1 \bmod p$ has at most 2 solns: either $x = 1$ or $x = -1$.
$x = 1$ cannot happen b/c then $\varphi(1) = 1$.
$x = -1 \equiv p-1 \bmod p$, so $x = -1$ is the only elt. of order 2.
So $\varphi(1) = -1 \bmod p$.
The dihedral group D_p is a group of order $2p$ and it is not cyclic (D_p is nonabelian). Therefore, $D_p \cong \mathbb{Z}/p\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$.
Thus, every group of order $2p$, where p is an odd prime, is either cyclic or is isomorphic to the dihedral group. □

② (a) If G is a group with an abelian normal subgroup N of index 2 and $a \in G - N$, prove a subgroup H of N is normal in G if $aHa^{-1} = H$.

Pf: Since $[G:N] = 2$, N only has two cosets in G, namely N and gN for $g \in G$.
Since $a \in G - N$, $a \notin N \Rightarrow a \in gN$.
Let $a = a'n \in gN$ ($a' \in G$, $n \in N$).
Then $aHa^{-1} = H \Rightarrow (a'n)H(a'n)^{-1} = H$
$a'nHn^{-1}a'^{-1} = H$
$a'Ha'^{-1} = H$
Since $H \leq N$ and N is abelian, we have that $H \trianglelefteq N$, so $nHn^{-1} = H$
Since $a' \in G$, we have shown that H is normal in G ($a'Ha'^{-1} = H$)
(If $a \in G$, $a \in N$, then $aHa^{-1} = aa^{-1}H = H$ since N is abelian and $H < G$.) □

(b) Let $G = (\mathbb{Z}/3\mathbb{Z})^2 \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$, where $\varphi: \mathbb{Z}/2 \to \operatorname{Aut}((\mathbb{Z}/3\mathbb{Z})^2)$ is the action of $\mathbb{Z}/2\mathbb{Z}$ on $(\mathbb{Z}/3\mathbb{Z})^2$ that sends the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$ to the automorphism $(x,y) \mapsto (y,x)$ of $(\mathbb{Z}/3\mathbb{Z})^2$. Use part (a) to show $H = \langle (1,2) \rangle \times \{0\} = \{(1,2),(2,1),(0,0)\} \times \{0\}$ is a normal subgp. of G.

Pf: $|G| = 9 \cdot 2 = 18$
Let $N = (\mathbb{Z}/3\mathbb{Z})^2 \times \{0\}$. Then $|N| = 9$, so N is an abelian normal subgp. of index 2, and H is a subgp. of N.
Let $a \in G$, $a \notin N$, so $a = ((0,0),1) \in G - N$.
$a \cdot a = ((0,0),1)((0,0),1) = ((0,0) + \varphi_1(0,0), 1+1) = ((0,0),0)$, so $a^{-1} = ((0,0),1)$.
Observe that for $((1,2),0) \in H$
$((0,0),1)((1,2),0)((0,0),1)^{-1} = ((0,0) + \varphi_1(1,2), 1+0)((0,0),1)$
$= ((2,1),1)((0,0),1)$
$= ((2,1) + \varphi_1(0,0), 1+1)$
$= ((2,1),0) \in H$
Likewise, $((0,0),1)((2,1),0)((0,0),1)^{-1} = ((1,2),0) \in H$ and
$((0,0),1)((0,0),0)((0,0),1)^{-1} = ((0,0),1)((0,0),1) = ((0,0),0) \in H$.
Therefore, by part (a), since $aHa^{-1} = H$, we have that the subgp. H of N is a normal subgp. of G. □

(c) With G and H as in part (b), determine whether G/H is abelian.

Pf: $|G| = 18$ and $|H| = 3$, so $|G/H| = \dfrac{|G|}{|H|} = \dfrac{18}{3} = 6$.
Every subgp. of order 6 is isomorphic to S_3 or $\mathbb{Z}/6\mathbb{Z}$.
Consider the element $((1,1),1) \in G/H$.
$\overline{((1,1),1)}\,\overline{((1,1),1)} = \overline{((1,1) + \varphi_1(1,1), 1+1)} = \overline{((2,2),0)} \notin H$
$\overline{((2,2),0)}\,\overline{((1,1),1)} = \overline{((2,2) + \varphi_0(1,1), 0+1)} = \overline{((0,0),1)} \notin H$.
Therefore, $|((1,1),1)| > 3$, so G/H cannot be isom. to S_3.
Thus, $G/H \cong \mathbb{Z}/6\mathbb{Z}$, which is abelian.
Therefore, we conclude that G/H is abelian. □

③ (a) Prove the direct product ring $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ (component wise operations) and the quotient ring $\mathbb{Z}[x]/(x^2)$ are not isomorphic.

Pf: There are no nonzero nilpotent elements in $\mathbb{Z}^2$ since $\nexists\, a \in \mathbb{Z}$ s.t. $a^n = 0$ for any $n \in \mathbb{Z}^+$.
In $\mathbb{Z}[x]/(x^2)$, the nonzero element x is nilpotent since $x^2 = 0$.
Since $\mathbb{Z}[x]/(x^2)$ has a nonzero nilpotent element and $\mathbb{Z}^2$ does not, the two rings are not isomorphic, $\mathbb{Z}^2 \ncong \mathbb{Z}[x]/(x^2)$. □

(b) Prove $\mathbb{Z}^2 \cong \mathbb{Z}[x]/(x^2 - x)$ as rings.

Pf: Observe that $x^2 - x = x(x-1)$, and $(x) + (x-1) = 1$.
Therefore, by the CRT, we have that
$\mathbb{Z}[x]/(x^2-x) \cong \mathbb{Z}[x]/(x) \times \mathbb{Z}[x]/(x-1) \cong \mathbb{Z} \times \mathbb{Z} \cong \mathbb{Z}^2$
Note that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ and $\mathbb{Z}[x]/(x-1) \cong \mathbb{Z}$ by evaluation @ $x = 0$ and @ $x = 1$, respectively.
Therefore, $\mathbb{Z}[x]/(x^2-x) \cong \mathbb{Z} \times \mathbb{Z} \cong \mathbb{Z}^2$. □

(c) For integers $c \geq 2$, prove $\mathbb{Z}^2 \ncong \mathbb{Z}[x]/(x^2 - cx)$ as rings. (Hint: for a ring A, consider A/pA for a suitable prime number p.)

Pf: Observe that $x^2 - cx = x(x-c)$, so $\mathbb{Z}[x]/(x^2-cx) \cong \mathbb{Z}[x]/(x)(x-c)$.
Suppose that $(x) + (x-c) = 1$. Then $\exists\, g(x), h(x) \in \mathbb{Z}[x]$ s.t.
$xg(x) + (x-c)h(x) = 1 \Rightarrow$ evaluation @ $x = c$ gives us $cg(c) = 1$, $c \geq 2$. ↯ ($g(c) = 1/c$)
This is not possible, so x and $x-c$ are not relatively prime. (b/c we are in $\mathbb{Z}$)
In $\mathbb{Z} \times \mathbb{Z}$, $(0,1)(1,0) = (0,0)$ is the additive identity, and $(0,1) + (1,0) = (1,1)$ is the multiplicative identity.
Assume $\varphi: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}[x]/(x^2 - cx)$.
Let $\overline{f(x)} = \varphi(1,0)$ and $\overline{g(x)} = \varphi(0,1)$.
Then $\varphi(1,0)\varphi(0,1) = \varphi(0,0) = \bar{0} \Rightarrow \overline{f(x)}\,\overline{g(x)} = \bar{0}$.
$\Rightarrow f(x)g(x) \in (x^2 - xc) = x(x-c) \Rightarrow f(x)g(x) = h(x)x(x-c)$.
$f(x) = xf_1(x)$ and $g(x) = (x-c)g_1(x)$
Then $\varphi(1,0) + \varphi(0,1) = \varphi(1,1) = \bar{1} \Rightarrow \overline{f(x)} + \overline{g(x)} = \bar{1}$
$\Rightarrow f(x) + g(x) = 1 + x(x-c)j(x)$
$\Rightarrow xf_1(x) + (x-c)g_1(x) = 1 + x(x-c)j(x)$
evaluation @ $x = c$: $cf_1(c) + 0 = 1 + 0 \Rightarrow cf_1(c) = 1 \Rightarrow c = \pm 1$ ↯ since $c \geq 2$.
Therefore, $\mathbb{Z}^2 \ncong \mathbb{Z}[x]/(x^2 - cx)$ as rings for $c \geq 2$. □

④ Let $G = \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

(a) What is the order of the element $(10,3,2)$ in G?

Pf: The order of $(10,3,2)$ in G is $\operatorname{lcm}(|10|, |3|, |2|)$.
The order of 10 in $\mathbb{Z}/24\mathbb{Z}$ is 12 since $10 \cdot 12 = 120 \equiv 0 \bmod 24$.
The order of 3 in $\mathbb{Z}/6\mathbb{Z}$ is 2 since $3 \cdot 2 = 6 \equiv 0 \bmod 6$.
The order of 2 in $\mathbb{Z}/3\mathbb{Z}$ is 3 since $2 \cdot 3 = 6 \equiv 0 \bmod 3$.
Therefore, $\operatorname{lcm}(|10|, |3|, |2|) = \operatorname{lcm}(12, 2, 3) = 12$.
Thus, the order of $(10,3,2)$ in G is 12. □

(b) Consider the quotient group $H = G/\langle (10,3,2) \rangle$. Determine a direct product of cyclic groups that is isomorphic to H.

Pf: $|G| = 24 \cdot 6 \cdot 3$ and $|\langle (10,3,2) \rangle| = 12$.
$|H| = |G| / |\langle (10,3,2) \rangle| = 24 \cdot 6 \cdot 3 / 12 = 36$.
$36 = 2^2 \cdot 3^2$
By the fundamental theorem of finitely generated abelian groups, we have that these are the distinct groups of order 36:
- $\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (only gp. w/ elt. of order 18)
- $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ (only gp. w/ elt. of order 12)
- $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ (only gp. w/ elt. of order 6)
- $\mathbb{Z}/36\mathbb{Z}$ (only gp. w/ elt. of order 36)

Consider $(x,y,z) \in G$. The order of (x,y,z) must be a factor of 24 ($\operatorname{lcm}(24,6,3) = 24$).
This means that there are no elts. of order 18 or 36.
Consider $f: G \to H$. Every element of H must have order dividing 24
(if x has order n, then $x^n = 1$, so $f(x)^n = 1 \Rightarrow$ the order of $f(x)$ divides n.)
Consider the element $(1,0,0) \in H$.
We want to find the least $n \in \mathbb{Z}^+$ s.t. $(n,0,0) \in K = \langle (10,3,2) \rangle$.
Let $(10m, 3m, 2m) = (n,0,0)$.
Then $6 \mid m$. Let $m = 6$, then $(60,18,12) \equiv (12,0,0)$
Therefore, $|(1,0,0)| = 12$ in $\langle (10,3,2) \rangle$, so there is an element of order 12.
Thus, $H \cong \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. □

⑤ Let R be a commutative ring w/ identity. Prove that R has a unique maximal ideal if and only if for all x and y in R satisfying $x + y = 1$, x or y is a unit in R.

Pf:
- Assume that R has a unique maximal ideal M.
Then we know that $R - M$ must contain all of the units, or in other words, M contains every non-unit of R.
If x and y are both nonunits, then $x + y$ must also be a nonunit b/c x, y nonunit $\Rightarrow x, y \in M$ and since M is an ideal $x + y \in M \Rightarrow x + y$ is a nonunit. So $x + y \neq 1$.
(contrapositive of: if $x + y = 1$, then x or y is a unit.)
- Assume that for all x and y in R satisfying $x + y = 1$, x or y is a unit.
If we can show that $R - R^\times$ is an ideal, then we are done b/c all proper ideals are contained in $R - R^\times$, so no other ideal can be maximal.
If x, y are nonunits, i.e., if $x, y \in R - R^\times$, then $x + y$ is a nonunit so $x + y \in R - R^\times$.
Therefore, $R - R^\times$ is closed under addition.
If r is any ring element ($r \in R$) and x is a nonunit ($x \in R - R^\times$), then rx is a nonunit ($rx \in R - R^\times$) because if rx has an inverse u, then $urx = 1$, so $ur = x^{-1}$, but x is a nonunit $\Rightarrow rx$ is a nonunit.
Therefore, $R - R^\times$ is an ideal.
Thus, we conclude that $R - R^\times$ is the unique maximal ideal of R. □

⑥ Give examples as requested, with justification.

(a) An integral domain that is not a PID.

Pf: Consider $\mathbb{Z}[x]$.
The ring $\mathbb{Z}[x]$ is an integral domain since $\mathbb{Z}$ is.
$\mathbb{Z}[x]$ is not a PID since the ideal $(2, x)$ is not principal.
Suppose $(2, x)$ was principal. Then $\exists\, g(x), h(x) \in \mathbb{Z}[x]$ s.t.
$2g(x) + xh(x) = 1$. Plug in $x = 0 \Rightarrow 2 \cdot g(0) + 0 \cdot h(0) = 1$
$2 \cdot g(0) = 1 \Rightarrow$ cannot happen in $\mathbb{Z}$
Therefore, $(2, x)$ is not a principal ideal, so $\mathbb{Z}[x]$ is not a PID.
Thus, $\mathbb{Z}[x]$ is an integral domain that is not a PID. □

(b) Find a permutation $\pi \in S_6$ such that $\pi(12)(456)\pi^{-1} = (36)(154)$.

Pf: $\pi(12)(456)\pi^{-1} = \pi(12)\pi^{-1}\pi(456)\pi^{-1}$
$= (\pi(1)\ \pi(2))(\pi(4)\ \pi(5)\ \pi(6))$
$= (3\ 6)(1\ 5\ 4)$
so $\pi(1) = 3$, $\pi(2) = 6$, $\pi(4) = 1$, $\pi(5) = 5$, $\pi(6) = 4$
$2 \mapsto 6 \mapsto 4 \mapsto 1 \mapsto 3$, $5 \mapsto 5$
Let $\pi = (2\,6\,4\,1\,3)$.
<u>Check:</u> $\pi(12)(456)\pi^{-1} = (36)(154)$
$(2\,6\,4\,1\,3)(12)(456)(2\,3\,1\,4\,6) = (36)(154)$ ✓
Therefore, $\pi = (2\,6\,4\,1\,3) \in S_6$ is such a permutation. □

(c) An element of an integral domain that is irreducible, but not prime.

Pf: Consider the element 2 of the integral domain $\mathbb{Z}[\sqrt{-5}]$.
Suppose $2 = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$.
Then $N(2) = 4 = N(\alpha)N(\beta) \Rightarrow N(\alpha) = \pm 1, \pm 2, \pm 4$.
If $N(\alpha) = \pm 1$, then α is a unit $\Rightarrow$ 2 is irred.
If $N(\alpha) = \pm 4$, then $N(\beta) = \pm 1$, so β is a unit $\Rightarrow$ 2 is irred.
If $N(\alpha) = \pm 2$, then for $\alpha = a + b\sqrt{-5}$, $N(\alpha) = a^2 + 5b^2 = \pm 2$.
By reducing mod 5, we get $x^2 \equiv 2 \bmod 5$, $x^2 \equiv 3 \bmod 5$. ↯
This is impossible b/c the squares mod 5 are $\equiv 0, 1, 4$.
So there is no $\alpha \in \mathbb{Z}[\sqrt{-5}]$ w/ $N(\alpha) = \pm 2$.
Therefore, 2 is irred.
Observe that $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, so $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$, but $2 \nmid (1 + \sqrt{-5})$ and $2 \nmid (1 - \sqrt{-5})$.
($1 + \sqrt{-5} = 2(x + y\sqrt{-5}) = 2x + 2y\sqrt{-5} \Rightarrow 2x = 1$ and $2y = 1$, $x = 1/2 \notin \mathbb{Z}$, $y = 1/2 \notin \mathbb{Z}$)
Therefore, 2 is not prime.
Thus, 2 is an elt. of $\mathbb{Z}[\sqrt{-5}]$ that is irreducible, but not prime. □

(d) A polynomial $f(x)$ in $(\mathbb{Z}/2\mathbb{Z})[x]$ such that the quotient ring $(\mathbb{Z}/2\mathbb{Z})[x]/(f(x))$ is a field of order 8.

Pf: We want $(\mathbb{Z}/2\mathbb{Z})[x]/(f(x)) = \{ax^2 + bx + c : a, b, c \in \mathbb{Z}/2\mathbb{Z}\}$ b/c this has order 8.
Observe that $(\mathbb{Z}/2\mathbb{Z})[x]/(f(x)) \cong \mathbb{Z}[x]/(2, f(x))$.
We want to find $f(x)$ s.t. it is a degree 3 polynomial that is irred. in $\mathbb{Z}/2\mathbb{Z}$, so that $(2, f(x))$ is a maximal ideal in $\mathbb{Z}[x]$.
Consider $f(x) = x^3 + x + 1$: $0^3 + 0 + 1 \equiv 1\ (2)$
$1^3 + 1 + 1 \equiv 1\ (2)$
Therefore, $f(x)$ is irred. mod 2.
Thus, $(\mathbb{Z}/2\mathbb{Z})[x]/(x^3 + x + 1)$ is a field and has order 8 b/c all of the polys. are of the form $ax^2 + bx + c$ ($a, b, c \in \mathbb{Z}/2\mathbb{Z}$), so $2 \cdot 2 \cdot 2 = 8$.
Therefore, we conclude that $f(x) = x^3 + x + 1$ in $(\mathbb{Z}/2\mathbb{Z})[x]$ is s.t. $(\mathbb{Z}/2\mathbb{Z})[x]/(f(x))$ is a field of order 8. □