January 2012

~~sábado, 12 de agosto de 2023~~ 10:54 a.m.

① (a) Define a p-Sylow subgroup of a finite group.

Pf: Let G be a fin. gp. s.t. $|G| = p^\alpha m$, p prime and $p \nmid m$.
We say that P is a p-Sylow subgp. of G s.t. $|P| = p^\alpha$.
In other words, a p-Sylow subgp. of a fin. gp. is a subgp. that has the highest power of p dividing $|G|$. □

(b) For each prime p, prove that any two p-Sylow subgroups of a finite group are conjugate. (That is, prove the second part of the Sylow theorems.)

Pf: Let G be a finite group, $|G| = p^k m$, p prime, $p \nmid m$, and let $P, Q \in Syl_p(G)$.
We want to show that $Q = gPg^{-1}$ for some $g \in G$.
Let Q (which is a p-gp.) act on G/P by left multiplication:
$q \cdot gP = qgP$.
Use fixed-point congruence: $|Set| \equiv |Fix_Q(Set)| \mod p$
$\Rightarrow |G/P| \equiv |Fix_Q(G/P)| \mod p$

$$|G/P| = \frac{|G|}{|P|} = \frac{p^k m}{p^k} = m \not\equiv 0 \mod p \text{ b/c } p \nmid m.$$

Since $|G/P| \not\equiv 0 \mod p$, $|Fix_Q(G/P)| \neq \emptyset$.
Thus, gP is fixed by a Q-action:

$$\begin{aligned} qgP = gP \quad & \forall q \in Q \\ \Leftrightarrow g^{-1}qgP = P \quad & \forall q \in Q \\ \Leftrightarrow g^{-1}qg \in P \quad & \forall q \in Q \\ \Leftrightarrow g^{-1}Qg < P. & \end{aligned}$$

Since Q is a p-Sylow subgp., $|g^{-1}Qg| = p^k = |P|$.
Thus, $g^{-1}Qg = P \Rightarrow Q = gPg^{-1}$. □

② Let the additive group $\mathbb{Z}$ act on the additive group $\mathbb{Z}[\frac{1}{3}] = \{\frac{a}{3^k} : a \in \mathbb{Z}, k \geq 0\}$ by $\varphi_n(r) = 3^n r$ for $n \in \mathbb{Z}$ and $r \in \mathbb{Z}[\frac{1}{3}]$.
Set $G = \mathbb{Z}[\frac{1}{3}] \rtimes_\varphi \mathbb{Z}$, a semi-direct product.

(a) Compute the product $(r,m)(s,n)$ and the inverse $(r,m)^{-1}$ in the group G.

Pf:

$$(r,m)(s,n) = (r + \varphi_m(s), m+n) = (r + 3^m s, m+n)$$

$$\begin{aligned}(r,m)^{-1} &= (\varphi_{-m}(r^{-1}), m^{-1}) = ((\varphi_{-m}(r))^{-1}, m^{-1}) \\ &= ((3^{-m} r)^{-1}, m^{-1}) \\ &= (-r \cdot 3^{-m}, -m)\end{aligned}$$

(can also do $(r + 3^m s, m+n) = (0,0)$ and solve for s, n in terms of r, m) □

(b) Show G is generated by $(1,0)$ and $(0,1)$.

Pf: First, we will work out what the powers of $(1,0)$ and $(0,1)$ are:
We will induct on the power: $(1,0)^1 = (1,0)$ and $(0,1)^1 = (0,1)$.

K=2: $(1,0)^2 = (1,0)(1,0) = (1 + \varphi_0(1), 0+0) = (1 + 3^0 \cdot 1, 0+0) = (1+1, 0) = (2,0)$
$(0,1)^2 = (0,1)(0,1) = (0 + \varphi_1(0), 1+1) = (0 + 3^1 \cdot 0, 1+1) = (0,2)$.

Ind. hyp.: assume this holds for $1 \leq k < n$, i.e., $(1,0)^k = (k,0)$, $(0,1)^k = (0,k)$

$$\begin{aligned}(1,0)^n &= (1,0)^{n-1}(1,0) = (n-1,0)(1,0) = (n-1+\varphi_0(1), 0+0) \\ &= (n-1+1, 0) = (n,0)\end{aligned}$$

$$\begin{aligned}(0,1)^n &= (0,1)^{n-1}(0,1) = (0,n-1)(0,1) = (0 + \varphi_{n-1}(0), n-1+1) \\ &= (0+0, n) = (0,n)\end{aligned}$$

Now we will show that conjugating $(r,0)$ by $(0,m)$ will give us non-integer first coordinates:

$$\begin{aligned}(0,m)(r,0)(0,m)^{-1} &= (0+\varphi_m(r), m+0)(0,-m) = (\varphi_m(r), m)(0,-m) \\ &= (\varphi_m(r) + \varphi_m(0), m+(-m)) = (\varphi_m(r), 0) \\ &= (3^m r, 0)\end{aligned}$$

and $(r,0) = r(1,0)$ and $(0,m) = m(0,1)$.
Therefore, we have show that G is generated by $(1,0)$ and $(0,1)$. □

③ Let R be a ring with identity, possibly noncommutative. Let I and J be two-sided ideals in R. Define IJ to be the set of finite sums $a_1b_1 + \dots + a_nb_n = \sum_{k=1}^{n} a_k b_k$ where $n \geq 1$, $a_k \in I$, and $b_k \in J$.

(a) Prove that IJ is a two-sided ideal in R and that $IJ \subset I \cap J$.

Pf: Let $a_1b_1 + \dots + a_nb_n \in IJ$, and let $r \in R$.
Then $r(a_1b_1 + \dots + a_nb_n) = ra_1b_1 + \dots + ra_nb_n = (ra_1)b_1 + \dots + (ra_n)b_n \in IJ$ b/c I is a two-sided ideal, which means that $ra_k \in I$ $\forall k$.

Then $(a_1b_1 + \dots + a_nb_n)r = a_1b_1r + \dots + a_nb_nr = a_1(b_1r) + \dots + a_n(b_nr) \in IJ$ b/c J is a two-sided ideal, which means that $b_kr \in J$ $\forall k$.

Therefore, we have shown that IJ is a two-sided ideal.
We know that $IJ \subset I$ b/c I is a two-sided ideal, so $I \cdot J \subset I$.
We know that $IJ \subset J$ b/c J is a two-sided ideal, so $I \cdot J \subset J$.
Therefore, $IJ \subset I \cap J$. □

(b) If R is commutative and $I + J = R$ then prove $IJ = I \cap J$, indicating where you use the commutativity in your proof.

Pf: From part (a), we have that $IJ \subset I \cap J$.
We want to show that $I \cap J \subset IJ$.
Since $I + J = R$, for $x \in I$, $y \in J$, we can write $x + y = 1$.
Let $z \in I \cap J$.
We want to show that $z \in IJ$.
If we can show that $z(x+y) \in IJ$, then we are done b/c $x+y = 1$.
We have $z(x+y) = zx + zy \in IJ$ because:
$z \in I \cap J \Rightarrow z \in I$ and $z \in J$, so $zy \in IJ$ $(z \in I, y \in J)$
$zx \in IJ$: since R is commutative $zx = xz \in IJ$ $(x \in I, z \in J)$.
Therefore, if R is commutative and $I + J = R$, then $IJ = I \cap J$. □

(c) Let $R = \begin{pmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & \mathbb{Z} \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a,b,c \in \mathbb{Z} \right\}$, which is a noncommutitive ring under addition and multiplication of matrices. Set
$I = \begin{pmatrix} 0 & \mathbb{Z} \\ 0 & \mathbb{Z} \end{pmatrix} = \left\{ \begin{pmatrix} 0 & y \\ 0 & z \end{pmatrix} : y,z \in \mathbb{Z} \right\}$ and $J = \begin{pmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & 0 \end{pmatrix} = \left\{ \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} : x,y \in \mathbb{Z} \right\}$.
Show I and J are two-sided ideals in R, $I + J = R$ and $IJ \neq I \cap J$. (This shows that part b becomes false in general if we drop its commutativity hypothesis.)

Pf: First we will show that I and J are two-sided ideals:

- Let $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in R$, $\begin{pmatrix} 0 & y \\ 0 & z \end{pmatrix} \in I$, and $\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \in J$. Then

$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} 0 & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} 0 & ay+bz \\ 0 & cz \end{pmatrix} \in I$ since $ay + bz \in \mathbb{Z}$ and $cz \in \mathbb{Z}$

$\begin{pmatrix} 0 & y \\ 0 & z \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & yc \\ 0 & zc \end{pmatrix} \in I$ since $yc \in \mathbb{Z}$ and $zc \in \mathbb{Z}$

This also shows that I is closed under mult.

For $\begin{pmatrix} 0 & y \\ 0 & z \end{pmatrix}, \begin{pmatrix} 0 & y' \\ 0 & z' \end{pmatrix} \in I$

$\begin{pmatrix} 0 & y \\ 0 & z \end{pmatrix} + \begin{pmatrix} 0 & y' \\ 0 & z' \end{pmatrix} = \begin{pmatrix} 0 & y+y' \\ 0 & z+z' \end{pmatrix} \in I$ since $y + y' \in \mathbb{Z}$ and $z + z' \in \mathbb{Z}$

So I is closed under addition.
Therefore, I is a two-sided ideal.

- $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ax & ay \\ 0 & 0 \end{pmatrix} \in J$ since $ax, ay \in \mathbb{Z}$

$\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} xa & xb+yc \\ 0 & 0 \end{pmatrix} \in J$ since $xa, xb+yc \in \mathbb{Z}$

} J is closed under multiplication

For $\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} x' & y' \\ 0 & 0 \end{pmatrix} \in J$

$\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} x' & y' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x+x' & y+y' \\ 0 & 0 \end{pmatrix} \in J$ since $x + x', y + y' \in \mathbb{Z}$

So J is closed under addition.
Therefore, J is a two-sided ideal.

- Let $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in R$. Then we can write

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix}}_{\in I} + \underbrace{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}}_{\in J}$$

Therefore, $I + J = R$.

- Let $\begin{pmatrix} 0 & y \\ 0 & z \end{pmatrix} \in I$ and $\begin{pmatrix} x' & y' \\ 0 & 0 \end{pmatrix} \in J$.

Then $\begin{pmatrix} 0 & y \\ 0 & z \end{pmatrix}\begin{pmatrix} x' & y' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

But $\begin{pmatrix} 0 & \alpha \\ 0 & 0 \end{pmatrix} \in I$ and $\in J$, so $\begin{pmatrix} 0 & \alpha \\ 0 & 0 \end{pmatrix} \in I \cap J$.
$(\alpha \in \mathbb{Z}, \alpha \neq 0)$

Therefore, $\begin{pmatrix} 0 & \alpha \\ 0 & 0 \end{pmatrix} \in I \cap J$, but $\begin{pmatrix} 0 & \alpha \\ 0 & 0 \end{pmatrix} \notin IJ \Rightarrow IJ \neq I \cap J$. □

④ (a) Show the only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1.

Pf: $\mathbb{Z}[\sqrt{-5}] = \{x + y\sqrt{-5} : x,y \in \mathbb{Z}\}$.
An elt. $x + y\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ is a unit iff $N(x + y\sqrt{-5}) = \pm 1$.
$N(x+y\sqrt{-5}) = (x + y\sqrt{-5})(x - y\sqrt{-5}) = x^2 + 5y^2 = \pm 1$
$x^2 + 5y^2 \geq 0$ $\forall x,y \in \mathbb{Z}$, so $x^2 + 5y^2 \neq -1$.
$x^2 + 5y^2 = 1$ iff $y = 0$ and $x = \pm 1$.
Therefore, the only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1. □

(b) Define what it means for an integral domain R to be a unique factorization domain (UFD) and use the equation $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ to show $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain.

Pf: A unique factn. domain (UFD) is an integral domain R s.t.
(1) every $a \neq 0$, unit in R has a factorization $a = p_1 p_2 \cdots p_k$ $(k \geq 1)$ where p_i are irreducible.
(2) if $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$ with p_i, q_j <u>all</u> irreducible, then
- $k = \ell$ (same number of factors) and
- after relabeling, $q_i = u_i p_i$, $u_i \in R^\times$.

Now we will show $\mathbb{Z}[\sqrt{-5}]$ is not a UFD using $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.
In an integral domain, prime $\Rightarrow$ irreducible.
Let $2 = \alpha\beta$, so $N(2) = 4 = N(\alpha)N(\beta) \Rightarrow$ WLOG $N(\alpha) = \pm 1, \pm 2$, or ± 4
If $N(\alpha) = \pm 1$, then α is a unit $\Rightarrow$ 2 is irred.
If $N(\alpha) = \pm 4$, then $N(\beta) = \pm 1 \Rightarrow \beta$ is a unit $\Rightarrow$ 2 is irred.
If $N(\alpha) = \pm 2$, then for $\alpha = x + y\sqrt{-5}$, $N(\alpha) = x^2 + 5y^2 = \pm 2 \mod 5$ gives us $x^2 \equiv 2 \mod 5$ or $x^2 \equiv 3 \mod 5$, which is impossible because squares mod 5 are $\equiv 0, 1, 4 \mod 5 \Rightarrow$ 2 is irred.
Since $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$,
$2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$, but $2 \nmid (1 + \sqrt{-5})$ and $2 \nmid (1 - \sqrt{-5})$
because $2(a + b\sqrt{-5}) = 2a + 2b\sqrt{-5} \neq 1 \pm \sqrt{-5}$ $\forall a, b \in \mathbb{Z}$.
Therefore, 2 is not prime.
2 is irred., but not prime.
Thus, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. □

⑥ Give examples as requested, with brief justification.

(a) A group action which has no fixed points.

Pf: Consider a group G acting on itself by left multiplication (or addition, if it's an additive group): $gx = x$
Consider this gp. action: $\varphi: S_3 \to S_3$ by $\varphi(\tau) = (12)\tau$, $\tau \in S_3$.

$$\left.\begin{aligned}(12)(1) &= (12) \\ (12)(12) &= (1) \\ (12)(13) &= (32) \\ (12)(23) &= (31) \\ (12)(123) &= (23) \\ (12)(132) &= (13)\end{aligned}\right\} \text{none of these are fixed points.}$$

Therefore, φ is a gp. action which has no fixed points. □

(b) The class equation for a non-abelian group that is not isomorphic to S_3. (Be sure to specify what the group is.)

Pf: Let S_4 be the group that is non-abelian and not isomorphic to S_3.
The class eqn. is $|S_4| = |Z(S_4)| + \sum_{i=1}^{r} [S_4 : C_{S_4}(\tau_i)]$
$|S_4| = 4! = 24$
$|Z(S_4)| = 0$ b/c S_4 is non-abelian
$\sum_{i=1}^{r} [S_4 : C_{S_4}(\tau_i)] = 1 + 6 + 8 + 3 + 6 = 24$:
The conjugacy classes of S_4 are:
- $\{(1)\}$
- $\{(12), (13), (14), (23), (24), (34)\}$
- $\{(123), (132), (124), (142), (134), (143), (234), (243)\}$
- $\{(12)(34), (13)(24), (14)(23)\}$
- $\{(1234), (1243), (1324), (1342), (1423), (1432)\}$

The class eqn. of S_4 gives us $|S_4| = 0 + 1 + 6 + 8 + 3 + 6 = 24$. □

(d) A unique factorization domain (UFD) which is not a principal ideal domain (PID).

Pf: $\mathbb{Z}[x]$ is a UFD that is not a PID.
It is not a PID b/c $(2, x)$ is not a principal ideal.
The gcd of $(2, x) = 1$, but $1 \notin (2, x)$ because every poly. in the ideal has even constant terms. □