January 2017 3:33 p.m.

① Let G be a finite group and p a prime number.

(a) Define a p-Sylow subgroup of G and state the Sylow Theorems for G.

Let $|G| = p^n m$ s.t. $p \nmid m$. A p-Sylow subgp. of G is a subgp. of G with order the highest power of p that divides $|G|$. ($|P| = p^n$)

① Let $Syl_p(G)$ be the set of p-Sylow subgps. of G. $Syl_p(G) \neq \emptyset$.

② Let $P, Q \in Syl_p(G)$. Then $Q = gPg^{-1}$ for some $g \in G$.

③ Let n_p = # of p-Sylow subgps. $= |Syl_p(G)|$. Then $n_p \equiv 1 \mod p$ and $n_p \mid m$.

(b) If H is a p-Sylow subgroup of G and N is a normal subgroup of G, prove $H \cap N$ is a p-Sylow subgroup of N. (Hint: Consider the order of $H \cap N$ relative to that of H and N.)

Pf: Let $|G| = p^n m$, $p \nmid m$, $|H| = p^n$ ($H < G$, $N \trianglelefteq G$)

Since $N \trianglelefteq G$, we have that HN is a subgp of G.

$|HN| = \frac{|H||N|}{|H \cap N|} = \frac{p^n \cdot |N|}{|H \cap N|}$

Since $H < HN < G$, we can write $|HN| = p^n m'$, $p \nmid m'$, $m' \mid m$.

$p^n m' = \frac{p^n \cdot |N|}{|H \cap N|} \Rightarrow m' = \frac{|N|}{|H \cap N|}$

Let $|N| = p^b \ell$ and $|H \cap N| = p^{b-n} k$, so $m' = \frac{p^b \ell}{p^{b-n} k} = p^n \frac{\ell}{k} \Rightarrow n = 0$ b/c $p \nmid m'$

So $|H \cap N| = p^b$, which is the highest power of p in $|N|$.

There fore, $H \cap N$ is a p-Sylow subgp. of N. □

② (a) Let p be a prime. Prove the group $GL_2(\mathbb{Z}/p\mathbb{Z})$ has order $(p^2-1)(p^2-p)$.

Pf: $GL_2(\mathbb{Z}/p\mathbb{Z}) = \{A \in M_2(\mathbb{Z}/p\mathbb{Z}) : \det(A) \neq 0\}$

Let an arbitrary matrix $M \in GL_2(\mathbb{Z}/p\mathbb{Z})$ be $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

We know $\det(M) = ad - bc \neq 0$.

For the first column there are p^2-1 options b/c we can have any pair $\binom{a}{c}$ except $a=c=0$ b/c then $\det(M)=0$.

For the second column there are p^2-p options b/c we can have any pair $\binom{b}{d}$ except for the scalar multiple of $\binom{a}{c}$ and since we are in $\mathbb{Z}/p\mathbb{Z}$ there are p scalars.

Therefore, the gp. $GL_2(\mathbb{Z}/p\mathbb{Z})$ has order $(p^2-1)(p^2-p)$. □

(b) Construct a non-trivial semidirect product $(\mathbb{Z}/3\mathbb{Z})^2 \rtimes_\varphi (\mathbb{Z}/3\mathbb{Z})$. That is, construct a semidirect product where $\varphi: \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}((\mathbb{Z}/3\mathbb{Z})^2)$ is not trivial and explicitly describe the group law in the semidirect product. (Hint: $\mathrm{Aut}((\mathbb{Z}/3\mathbb{Z})^2) \cong GL_2(\mathbb{Z}/3\mathbb{Z})$.)

Pf: Let $\varphi: \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}((\mathbb{Z}/3\mathbb{Z})^2) \cong GL_2(\mathbb{Z}/3\mathbb{Z})$

Observe that $|GL_2(\mathbb{Z}/3\mathbb{Z})| = (3^2-1)(3^2-3) = 8 \cdot 6 = 48$ by part (a).

We know that $|\varphi(1)| \mid 3$, so $|\varphi(1)| = 1$ or 3.

If $|\varphi(1)| = 1$, then φ is the trivial homomorphism.

So let $\varphi(1)$ be some element of order 3: $\varphi(1)^3 = Id$, $\varphi(1) \neq Id$.

By Cauchy's theorem, there is an element of order 3 since $3 \mid 48$.

Observe that $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ is an element of order 3.

Let $\varphi(n) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^n$.

This is well-defined b/c the matrix has order 3.

The gp. law of this semi-direct prod. is:

let $((a,b),c), ((x,y),z) \in (\mathbb{Z}/3\mathbb{Z})^2 \rtimes_\varphi (\mathbb{Z}/3\mathbb{Z})$

$((a,b),c)((x,y),z) = ((a,b) + \varphi_c(x,y), c+z) = \left(\binom{a}{b} + \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^c \binom{x}{y}, c+z\right)$.

(c) Show the only semidirect product $(\mathbb{Z}/7\mathbb{Z})^2 \rtimes_\varphi (\mathbb{Z}/5\mathbb{Z})$ is the trivial one.

Pf: Let $\varphi: \mathbb{Z}/5\mathbb{Z} \to \mathrm{Aut}((\mathbb{Z}/7\mathbb{Z})^2) \cong GL_2(\mathbb{Z}/7\mathbb{Z})$

Observe that $|GL_2(\mathbb{Z}/7\mathbb{Z})| = (7^2-1)(7^2-7) = 48 \cdot 42$

we have that $|\varphi(1)| \mid 5$, so $|\varphi(1)| = 1$ or 5.

$|\varphi(1)| \neq 5$ b/c $5 \nmid 48 \cdot 42$, so there is no element of order 5, by Lagrange's theorem.

Therefore, $|\varphi(1)| = 1$, so φ is the trivial homomorphism. □

③ Let $i = \sqrt{-1}$ in $\mathbb{C}$.

(a) Show that $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$ are isomorphic as additive groups.

Pf: Let $\varphi: \mathbb{Z}[i] \to \mathbb{Z}[\sqrt{-2}]$ by $a+bi \mapsto a+b\sqrt{-2}$.

φ is a homomorphism: let $a+bi, c+di \in \mathbb{Z}[i]$, then

$\varphi((a+bi)+(c+di)) = \varphi(a+c+(b+d)i) = a+c+(b+d)\sqrt{-2} = a+b\sqrt{-2}+c+d\sqrt{-2}$
$= \varphi(a+bi) + \varphi(c+di)$.

φ is clearly surjective since $a+bi \mapsto a+b\sqrt{-2}$ and

φ is injective since if $a+bi \neq c+di$, then $\varphi(a+bi) = a+b\sqrt{-2} \neq c+d\sqrt{-2} = \varphi(c+di)$.

Therefore, φ is an isomorphism. Thus, $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$ are isom. as add. gps. □

(b) Show that $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$ are not isomorphic as rings.

Pf: Assume $\varphi: \mathbb{Z}[\sqrt{-2}] \to \mathbb{Z}[i]$ was a ring isomorphism, then $(\sqrt{-2})^2 = -2$

$\Rightarrow \varphi(\sqrt{-2})^2 = \varphi(-2) = \varphi(-1) + \varphi(-1) = -2$

Let $\varphi(\sqrt{-2}) = x+yi$. Then $(x+yi)^2 = x^2 - y^2 + 2xyi$.

$\varphi(\sqrt{-2})^2 = (x+yi)^2 = -2 \Rightarrow x^2 - y^2 + 2xyi = -2$

$\Rightarrow x^2 - y^2 = -2$ and $2xyi = 0$

If $x = 0$, then $-y^2 = -2$ no soln. in $\mathbb{Z}$.

If $y = 0$, then $x^2 = -2$ no soln. in $\mathbb{Z}$.

Thus, $\mathbb{Z}[i]$ has no soln. to $\alpha^2 = -2$.

Therefore, $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$ are not isom. as rings. □

④ (a) For an integral domain A, define an irreducible element of A, a prime element of A, and what it means to say A is a unique factorization domain (UFD).

- An element $a \in A$ is irreducible if $a \neq 0$, $a \neq$ unit and when $a = uv$, u is a unit (v is a unit multiple).
- An element $p \in A$ is prime if $p \neq 0$, $p \neq$ unit and when $p \mid xy$ either $p \mid x$ or $p \mid y$ ($x, y \in A$).
- A is a UFD if (1) every $a \in A$, $a \neq 0$, $a \neq$ unit has a factorization $a = p_1 p_2 \cdots p_k$ ($k \geq 1$) where p_i are irred.
  (2) if $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$ with p_i, q_j all irred., then
  ↳ $k = \ell$ (same # of factors) and
  ↳ after relabeling $q_i = u_i p_i$, $u_i \in A^\times$.

(b) Prove that in a UFD every irreducible element is prime.

Pf: Let R be a UFD and let $p \in R$ be an irred. elt. and assume $p \mid ab$ for some $a, b \in R$. WTS $p \mid a$ or $p \mid b$.

Since $p \mid ab$, $\exists\, c \in R$ s.t. $pc = ab$

Writing a and b as a product of irred., we see from $pc = ab$ and from the uniqueness of the decomposition into irreducibles of ab that the elt. p must be associate to one of the irreducibles occuring in either the factorization of a or b.

WLOG assume p is associate to one of the irred. in the factn. of a, i.e., a can be written as $a = (up)p_2 p_3 \cdots p_n$ for a unit u and some (possibly empty set of) irreducibles $p_2, \ldots, p_n$.

But then $p \mid a$, since $a = pd$ where $d = up_2 \cdots p_n$. □

⑤ Let R be an integral domain. An element $s \in R$ that is not zero and not a unit is called "special" if, in the quotient ring $R/(s)$, each coset is represented by 0 or a unit from R: for each $a \in R$ we have $a \equiv 0 \mod (s)$ or $a \equiv u \mod (s)$ where $u \in R^\times$.

(a) If $s \in R$ is special, prove that the principal ideal (s) in R is maximal.

Pf: Suppose $s \in R$ is special. To show that (s) in R is maximal, we will show that $R/(s)$ is a field.

Let $x + (s)$ be a nonzero elt. in $R/(s)$ (if it were 0, then it has no mult. inverse).

Since (s) is special we know either $x + (s) = 0 + (s)$ or $x + (s)$ can be represented by a unit.

Since $x + (s)$ is nonzero, we can write $x + (s) = u + (s)$, where u is a unit in R.

Since u is a unit in R, u^{-1} exists.

We claim $[x + (s)]^{-1} = u^{-1} + (s)$.

Observe $[x+(s)][u^{-1}+(s)] = [u+(s)][u^{-1}+(s)] = uu^{-1} + (s) = 1 + (s)$

Thus, every nonzero elt. in $R/(s)$ is a unit, i.e., $R/(s)$ is a field.

Therefore, (s) is maximal. □

(b) In $\mathbb{Z}[i]$ prove $1+i$ is special and 3 is not special.

Pf: Let's assume $a+bi+(1+i) \notin 0+(1+i)$.

Then apply the division algorithm to $a+bi$ and $1+i$.

This results in an equation of the form

⊛ $a+bi = (c+di)(1+i) + (e+fi)$ where $N(e+fi) < N(1+i) = 2$.

So, $N(e+fi) = 0$ or 1 and it can't be 0 since $a+bi \notin (1+i)$.

Thus, $N(e+fi) = 1$. So $e+fi = \pm 1, \pm i$ (units in $\mathbb{Z}[i]$).

If we reduce ⊛ by $(1+i)$, we get $a+bi+(1+i) = (e+fi)+(1+i)$, where $e+fi$ is a unit $\Rightarrow 1+i$ is special.

- To show 3 is not special consider $2+(3)$ in $\mathbb{Z}[i]/(3)$.

The only units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$.

$2+(3) \neq 0+(3) \Rightarrow 2 = 3(a+bi) \Rightarrow 4 = 9N(a+bi)$, no soln. in $\mathbb{Z}$

$2+(3) \neq 1+(3) \Rightarrow 2-1 = 1 = 3(a+bi) \Rightarrow 1 = 9N(a+bi)$, no soln. in $\mathbb{Z}$

$2+(3) \neq -1+(3) \Rightarrow 2+1 = 3 = 3(a+bi) \Rightarrow 9 = 9N(a+bi)$ no

$2+(3) \neq i+(3) \Rightarrow 2-i = 3(a+bi) \Rightarrow N(2-i) = 3 = 9N(a+bi)$ no

$2+(3) \neq -i+(3) \Rightarrow 2+i = 3(a+bi) \Rightarrow N(2+i) = 5 = 9N(a+bi)$ no

Therefore, 3 is not special. □

(c) Prove that there are no special elements in $\mathbb{Z}[x]$. (Hint: Apply the definition of special with $a = 2$ and with $a = x$.)

Pf: Let's assume $f(x) \in \mathbb{Z}[x]$ is special. Consider $2 \in \mathbb{Z}[x]$.

Since $f(x)$ is special, either $2 \equiv 0 \mod f(x)$ or $2 \equiv u \mod f(x)$ (u is a unit).

Note that ± 1 are the only units in $\mathbb{Z}[x]$.

$2 \equiv 0 \mod f(x) \Rightarrow 2 \in (f(x))$

$2 \equiv 1 \mod f(x) \Rightarrow 1 \in (f(x))$ } cannot happen b/c special elts are not units

$2 \equiv -1 \mod f(x) \Rightarrow 3 \in (f(x))$

↳ $2 = f(x)g(x) \Rightarrow f(x) = \pm 2$ or ± 1

↳ $3 = f(x)h(x) \Rightarrow f(x) = \pm 3$ or ± 1

} $f(x)$ cannot be ± 1, so the only options are $f(x) = \pm 2, \pm 3$ (2, 3 are irred.)

Using the elt. $x \in \mathbb{Z}[x]$

$x \equiv 0 \mod f(x) \Rightarrow x = f(x)q(x)$

$x \equiv 1 \mod f(x) \Rightarrow x - 1 = f(x)h(x)$

$x \equiv -1 \mod f(x) \Rightarrow x + 1 = f(x)g(x)$

} these can't happen b/c leading term will have coeff. ± 2 or ± 3, but these all have coeff. 1. □

⑥ Give examples as requested, with justification.

(a) A finite group of even order that does not have a subgroup of index 2.

Pf: Consider the group A_5.

$|A_5| = \frac{5!}{2} = 60$, so A_5 is a finite group of even order.

If a gp. has a subgp. of index 2, then that subgp. is normal.

The gp. A_5 is simple, which means that the only normal subgps are the trivial gp. and itself, neither of which have index 2.

Therefore, A_5 is a fin. gp. of even order that does not have a subgp. of index 2. □

(b) A generator of the character group of $\mathbb{Z}/4\mathbb{Z}$.

(c) An irreducible polynomial of degree 3 in $(\mathbb{Z}/3\mathbb{Z})[x]$.

Pf: Consider the polynomial $x^3 + 2x + 1$:

$0^3 + 2 \cdot 0 + 1 \equiv 1 \mod 3$

$1^3 + 2 \cdot 1 + 1 \equiv 1 \mod 3$

$2^3 + 2 \cdot 2 + 1 \equiv 1 \mod 3$

(For a quadratic or cubic, if the poly. has no root $\Rightarrow$ irred.)

Therefore, $x^3 + 2x + 1$ is irreducible in $(\mathbb{Z}/3\mathbb{Z})[x]$. □

(d) A prime factorization of 10 in $\mathbb{Z}[i]$.

Pf: $10 = 2 \cdot 5$

$2 = (1+i)(1-i)$ in $\mathbb{Z}[i]$

$5 = (1+2i)(1-2i)$ in $\mathbb{Z}[i]$

$N(1+i) = 2$ which is prime, so $1+i$ is irred.

$N(1+2i) = 5$ which is prime, so $1+2i$ is irred.

Therefore, $10 = (1+i)(1-i)(1+2i)(1-2i)$ in $\mathbb{Z}[i]$. □