August 2017

martes, 3 de enero de 2023 2:02 p.m.

① Let G be a nontrivial finite group. A subgp. M is called a maximal subgroup of G if M is a proper subgroup, i.e., $M \neq G$, and the only subgroups of G containing M are M and G.

(a) Show each proper subgroup of a finite group G is contained in a maximal subgroup of G.

Pf: Let H be a proper subgroup of G.
If H is maximal, then $H \subset G$ and H is contained in itself.
If H is not maximal, then we H_1 s.t. $H \subset H_1 \subset G$.
If H_1 is maximal, then we are done.
If not, then we have H_2 s.t. $H \subset H_1 \subset H_2 \subset G$.
Continue the above process.
(so $H \subset H_1 \subset H_2 \subset \cdots \subset H_n \subset \cdots \subset G$ if none of the H_i are maximal.)
This cannot happen since G has finite order.
Therefore, each proper subgp. of a fin. gp. G is contained in a maximal subgp. of G. □

(b) Count the number of maximal subgroups of the dihedral group of order $2p$, where p is an odd prime.

Pf: Let $R = \langle r \rangle = \{1, r, \ldots, r^{p-1}\} \subset D_p$.
By part (a), each proper subgp. of D_p is contained in a maximal subgp. of D_p.
Let $R \subset H \subset D_p$. We have that $|R| = p$ and $|D_p| = 2p$, so
$R \subset H \subset D_p \Rightarrow$ either $H = D_p$ or $H = R$.
Let $S \subset D_p$ be a group of order 2, for ex: $\{1, s\}$. Let $S \subset H \subset D_p$.
We have that $|S| = 2$ and $|D_p| = 2p$, so
$S \subset H \subset D_p \Rightarrow$ either $H = D_p$ or $H = S$.
The index of in D_p is p : $[D_p : S] = \frac{|D_p|}{|S|} = \frac{2p}{2} = p$.

We can see that there are p groups of order 2 from observing:
$(r^k s)^2 = r^k s r^k s = r^k r^{-k} s s = 1$ for $0 \leq k \leq p-1$.
There is only one subgp. of order p and there are p subgps. of order 2, namely $\{1, r^k s\}$ $0 \leq k \leq p-1$.
So there are $p+1$ maximal subgroups.
These are the only maximal subgps. because 1 and $2p$ are the last ones. □

(c) Show that if a nontrivial finite group G has only one maximal subgroup, then G is cyclic of prime-power order. (Hint: first prove G is cyclic.)

Pf: Let G be a nontrivial fin. gp. w/ only one max. subgp. Assume G is not cyclic.
Let M be the max. subgp. and let $g \in G$ s.t. $g \notin M$.
Then $\langle g \rangle \subset G$, so $\langle g \rangle \subset M$ since M is maximal $\Rightarrow g \in M$.
Thus, every element of G is in M, so $M = G$ ↯ b/c M is maximal.
Therefore, G is cyclic.
Assume $|G| = p^a q^b$ where p, q distinct primes and $a, b \in \mathbb{Z}^+$.
By the Sylow thms, there must exist subgps. of order p^a and q^b, say P and Q, resp.
Since G is cyclic, these subgps. are cyclic: $|P| = p^a$, $|Q| = q^b$.
Note that $(p, q) = 1$, so $P \neq Q$.
Since P is the subgp. w/ the highest power of p dividing $|G|$, P is maximal.
Since Q is the subgp. w/ the highest power of q dividing $|G|$, Q is maximal.
This is a contradiction b/c G has only one maximal subgp.
Therefore, G must be cyclic of prime-power order. □

---

② Let G be a nonabelian group of order 75 and H be a 5-Sylow subgroup of G.

(a) Show H is a normal subgp. of G and is abelian.

Pf: $|G| = 75 = 3 \cdot 5^2$
Let H be a 5-Sylow subgp. of G, so $|H| = 25$.
By the third Sylow thm, we have that
$n_5 \equiv 1 \bmod 5$ and $n_5 \mid 3 \Rightarrow n_5 = 1$.
Therefore, H is normal.
$|H| = 5^2 \Rightarrow$ abelian since groups of order prime squared are abelian. □

(b) Show H is not cyclic, or equivalently $H \cong (\mathbb{Z}/5\mathbb{Z})^2$. (Hint: Show the conjugation action of G on H is not trivial.)

Pf: Since $|H| = 5^2$, we know H is abelian.
If H is cyclic, then $H \cong \mathbb{Z}/5^2 = \mathbb{Z}/25\mathbb{Z}$.
We WTS $H \cong (\mathbb{Z}/5\mathbb{Z})^2$ (so $H \not\cong \mathbb{Z}/25\mathbb{Z}$)
If H is not cyclic, then no elt. has order 5^2: all $g \neq 1$ in H have order 5. Pick $x \in H - \{1\}$, so $\langle x \rangle$ has order 5.
Pick $y \in H - \langle x \rangle$, so $\langle y \rangle$ has order 5, and $\langle x \rangle \cap \langle y \rangle = \{1\}$.
Let $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \longrightarrow H$ by $(k \bmod 5, \ell \bmod 5) \longmapsto x^k y^\ell$.
- This is a homomorphism since x and y commute (H is abelian).
- The kernel is trivial: $x^k y^\ell = 1 \Rightarrow x^k = y^{-\ell} \in \langle x \rangle \cap \langle y \rangle = \{1\}$ $\Rightarrow 5 \mid k$ and $5 \mid \ell$.
- Same size: $|\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}| = |H| = 5^2$

Therefore, $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} = (\mathbb{Z}/5\mathbb{Z})^2 \cong H$.
Suppose the conj. action of G on H is trivial $g \in C_G(H)$ (every $g \in G$ commutes w/ $h \in H$)
If action is trivial, then $gh = hg$ $\forall h \in H, g \in G$
If $Z(G) = H \Rightarrow G$ is abelian ↯ G is nonabelian.
If H is cyclic, then $|\mathrm{Aut}(H)| = 20$.
H is contained in the kernel of the conj. action (ghg^{-1})
H is maximal b/c prime index. $(|G|/|H| = 75/25 = 3$ prime$)$
$G/H \longrightarrow \mathrm{Aut}(H)$ inj. hom.
$\varphi(G/H)$ has order $3 \mid 20$ ↯
The conj. action of G on H is not trivial.
Therefore, H is not cyclic. □

(c) Determine a 2×2 matrix A with entries in $\mathbb{Z}/5\mathbb{Z}$ that has order 3. (Hint: you can find such a matrix with integer entries having complex eigenvalues equal to the primitive 3rd roots of unity ζ_3 and ζ_3^2, where $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$.)

Pf: We want $A^3 = I$, so $(\det(A))^3 = I$.
Let $x = \det(A)$. Then $x^3 = 1 \Rightarrow x^3 - 1 = 0 \Rightarrow (x-1)(x^2+x+1) = 0$.
Note that x^2+x+1 is irred. in $\mathbb{Z}/5\mathbb{Z}$ since -3 has no square roots in $\mathbb{Z}/5\mathbb{Z}$.
Since A is 2×2, it follows that x^2+x+1 is the minimal poly. for A.
We now find A.
Notice that $x^2+x+1 = x(x+1)+1 = -x(-x-1)+1$
The matrix w/ this determinant is $\begin{pmatrix} -x & -1 \\ 1 & -x-1 \end{pmatrix}$.
If we add xI to the above matrix, we get $\begin{pmatrix} -x+x & -1 \\ 1 & -x-1+x \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$,
so $A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \equiv \begin{pmatrix} 0 & 4 \\ 1 & 4 \end{pmatrix} \bmod 5$.
Check: $\begin{pmatrix} 0 & 4 \\ 1 & 4 \end{pmatrix}\begin{pmatrix} 0 & 4 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 4 & 1 \\ 4 & 0 \end{pmatrix}$, $\begin{pmatrix} 4 & 1 \\ 4 & 0 \end{pmatrix}\begin{pmatrix} 0 & 4 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so $\begin{pmatrix} 0 & 4 \\ 1 & 4 \end{pmatrix}^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ✓
So $A = \begin{pmatrix} 0 & 4 \\ 1 & 4 \end{pmatrix}$. □

(d) Construct an example of a nonabelian group w/ order 75. (The matrix in part (c) will be useful.)

Pf: From part (c), we know $\left|\begin{pmatrix} 0 & 4 \\ 1 & 4 \end{pmatrix}\right| = 3$.
Let $K = \left\langle \begin{pmatrix} 0 & 4 \\ 1 & 4 \end{pmatrix} \right\rangle$, so $|K| = 3$.
$K \cong \mathbb{Z}/3\mathbb{Z}$
Let $G = H \rtimes_\varphi K$, where $H \cong (\mathbb{Z}/5\mathbb{Z})^2$ and $\varphi: K \longrightarrow \mathrm{Aut}(H)$.
$|\varphi(1)| \mid 3 \Rightarrow \varphi(1) = 1$ or $\varphi(1) = 3$.
$\varphi(1)$ is the trivial homomorphism.
$|\mathrm{Aut}(H)| = |\mathrm{Aut}((\mathbb{Z}/5\mathbb{Z})^2)| = |GL_2(\mathbb{Z}/5\mathbb{Z})| = (5^2-1)(5^2-5) = 24 \cdot 20$
$3 \mid 24 \cdot 20$, so $\varphi(1) = 3$.
Therefore, $(\mathbb{Z}/5\mathbb{Z})^2 \rtimes_\varphi (\mathbb{Z}/3\mathbb{Z})$, $\varphi: \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}((\mathbb{Z}/5\mathbb{Z})^2)$ by $\varphi(1) = 3$, is a nonabelian group with order 75. □

---

③ The group S_9 denotes the permutations of a set with 9 elements (symmetric gp.).

(a) Prove that there is no element of order 18 in S_9.

Pf: The order of an element in S_n is the lcm of the cycle lengths.
Suppose there is an element of order 18 in S_9.
Then the lcm of its cycle lengths = 18.
We can factor 18 as $1 \cdot 18$, $2 \cdot 9$, $3 \cdot 6$.
The first case $1 \cdot 18$ is impossible b/c there is no cycle with length 18 in S_9.
The second case $2 \cdot 9$ is impossible b/c it has $2+9=11$ distinct numbers in it, but there are only 9 distinct numbers in S_9.
The third case $3 \cdot 6$ actually has $\mathrm{lcm}(3,6) = 6 \neq 18$.
Therefore, there is no element of order 18 in S_9. □

(b) Construct, with justification, an element of order 20 in S_9.

Pf: We want an elt. whose cycle lengths have lcm = 20.
$20 = \underbrace{1 \cdot 20}_{1+20=21} = \underbrace{2 \cdot 10}_{2+10=12} = \underbrace{4 \cdot 5}_{4+5=9}$
Consider the element $(1\,2\,3\,4\,5)(6\,7\,8\,9)$.
The element $(1\,2\,3\,4\,5)(6\,7\,8\,9)$ is in S_9 and it has order $\mathrm{lcm}(4,5) = 20$. □

---

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

Pf: Let $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$.
The element $\alpha \in \mathbb{Z}[\sqrt{-5}]$ is a unit iff $N(\alpha) = \pm 1$.
$N(a+b\sqrt{-5}) = (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2 + 5b^2$
$N(a+b\sqrt{-5}) = a^2+5b^2 = \pm 1 \Rightarrow a^2+5b^2 = 1$ or $a^2+5b^2 = -1$.
It is impossible for $a^2+5b^2 = -1$, because $a^2+5b^2 \geq 0$.
If $a^2+5b^2 = 1$, then $a = \pm 1$, $b = 0$ are the only $\mathbb{Z}$-solns.
Therefore, the only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1. □

(b) Justify why the equation $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ shows $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain.

Pf: In a UFD, $\{\text{primes}\} = \{\text{irreducibles}\}$.
$N(2) = 4 = 2^2$, so 2 is irreducible.
If 2 is prime, then since $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$, either $2 \mid (1+\sqrt{-5})$ or $2 \mid (1-\sqrt{-5})$.
$2 \nmid (1 \pm \sqrt{-5})$ because $2\alpha \neq 1 \pm \sqrt{-5}$ $\forall \alpha \in \mathbb{Z}$
Therefore, 2 is irreducible, but not prime in $\mathbb{Z}[\sqrt{-5}]$.
Thus, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. □

(c) Justify why the equation $(2+3i)(2-3i) = (3+2i)(3-2i)$ does not show that $\mathbb{Z}[i]$ is not a unique factorization domain.

Pf: Observe that $(2+3i) = i(3-2i)$ and $(2-3i) = -i(3+2i)$, and $\pm i$ are units of $\mathbb{Z}[i]$.
Therefore, $3-2i$ is a unit multiple of $2+3i$ and $3+2i$ is a unit multiple of $2-3i$.
Thus, these factorizations are the same.
By rewriting the LHS, we see $i(3-2i)(-i)(3+2i) = \underbrace{(3+2i)(3-2i)}_{\text{RHS}}$.
Therefore, this does not show that $\mathbb{Z}[i]$ is not a UFD. □

---

⑥ Give examples as requested, with justification.

(a) Two nonabelian groups of order 12 that are not isomorphic.

Pf: Consider the nonabelian groups A_4 and D_6.
Observe that $|A_4| = \frac{4!}{2} = 12$ and $|D_6| = 2 \cdot 6 = 12$.
Note that D_6 has an element of order 6, namely r $(r^6 = 1)$.
There is no element of order 6 in A_4.
Recall that the order of an elt. in $A_n \subseteq S_n$ is the lcm of the cycle lengths.
$A_4 \subseteq S_4$ where the orders are $\mathrm{lcm}(4) = 4$
$\mathrm{lcm}(3,1) = 3$
$\mathrm{lcm}(2,2) = 2$
$\mathrm{lcm}(2,1,1) = 2$
$\mathrm{lcm}(1,1,1,1) = 1$,
none of which has lcm = 6.
Therefore, $A_4 \not\cong D_6$. □

(b) A group that acts transitively on the plane minus the origin, $\mathbb{R}^2 - \left\{\begin{pmatrix} 0 \\ 0 \end{pmatrix}\right\}$.

Pf: If a group G acts transitively on a set S, then the action is transitive if for all $s_1, s_2 \in S$, there is $g \in G$ s.t. $g \cdot s_1 = s_2$.
(i.e., there is one orbit).
Consider the group $GL_2(\mathbb{R})$.
Rotations and dilations are included in $GL_2(\mathbb{R})$, so we can get from one point to any other for all points, i.e., there is one orbit. □

(c) A ring that is not a field and has infinitely many units.

Pf: Consider the ring $\mathbb{Z}[\sqrt{2}]$.
This is not a field since $\mathbb{Z} \neq$ field.
Then observe that for $(1+\sqrt{2})^n$ $\forall n \in \mathbb{Z}$, we have
$N((1+\sqrt{2})^n) = (N(1+\sqrt{2}))^n = ((1+\sqrt{2})(1-\sqrt{2}))^n = (1-2)^n = (-1)^n$.
Therefore, $\mathbb{Z}[\sqrt{2}]$ has infinitely many units since $(1+\sqrt{2})^n$ is a unit for all $n \in \mathbb{Z}$. □

(d) A nonzero prime ideal in $\mathbb{R}[x,y]$ that is not a maximal ideal.

Pf: Consider the ideal (x).
Then $\mathbb{R}[x,y]/(x) \cong \mathbb{R}[y]$. This is an integral domain since $\mathbb{R}$ is.
$\mathbb{R}[y]$ is not a field $(y^{-1} \notin \mathbb{R}[y])$.
Therefore, (x) is a nonzero prime ideal in $\mathbb{R}[x,y]$ that is not maximal. □