Math 230A: Algebra
Midterm 2 Solutions
Wednesday, November 16, 2022.

1. State the Sylow Theorem.
(You can label the parts I,II,III, and III*, but you don't have to state it this way.)

Solution: Let G be a finite group and p be a prime dividing $|G|$. We can write $|G| = p^\alpha \cdot m$ where $p \nmid m$.

   (a) There exists a $P \leq G$ with $|P| = p^\alpha$. (This is a Sylow p-subgroup of G. Let $\mathrm{Syl}_p(G)$ denote the set of Sylow p-subgroups of G.)
   (b) If $P, Q \in \mathrm{Syl}_p(G)$, then there exists $g \in G$ such that $Q = gPg^{-1}$.
   (c) Let $n_p = |\,\mathrm{Syl}_p(G)|$. Then $n_p \equiv 1 \pmod{p}$ and $n_p \mid m$.
   (d) Let $P \in \mathrm{Syl}_p(G)$. Then $n_p = [G \colon N_G(P)]$.

2. Classify groups of order 99 up to isomorphism.
That is, give a list of groups such that every group of order 99 is isomorphic to exactly one of the groups in your list.

Solution: By Sylow III, $n_3 \mid 11$ and $n_3 \equiv 1 \pmod{3}$. So $n_3 = 1$. Similarly, $n_{11} \mid 9$ and $n_{11} \equiv 1 \pmod{11}$, so $n_{11} = 1$. Let $P \in \mathrm{Syl}_3(G)$ and $Q \in \mathrm{Syl}_{11}(G)$. Since $n_3 = 1$, $P \trianglelefteq G$. Similarly, $Q \trianglelefteq G$. So $PQ \leq G$. By Lagrange's theorem $P \cap Q = \{1\}$. This implies $|PQ| = |P| \cdot |Q| = |G|$, so $PQ = G$.

The Recognition Theorem for Direct Products implies that $G \cong P \times Q$. Since $|Q| = 11$, which is prime, we see that $Q \cong \mathbb{Z}/11\mathbb{Z}$. Since $|P| = 3^2$, we know that P is abelian, which implies that $P \cong \mathbb{Z}/9\mathbb{Z}$ or $P \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. (Every group of order p^2 is abelian– this follows from the fact that the center of a p-group is nontrivial and the fact that if $G/Z(G)$ is cyclic then G is abelian.)

We conclude that $G \cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$ or $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$. These groups are not isomorphic to each other– one is cyclic and the other is not.

3. (a) State the Fundamental Theorem for Finitely Generated Abelian Groups (also called the Classification Theorem for Finitely Generated Abelian Groups).
Solution: Let G be a finitely generated abelian group. Then

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \mathbb{Z}/n_t\mathbb{Z}$$

where $r, t \geq 0$, each $n_i \geq 2$ for each $i \in \{1, 2, \ldots, t\}$, and $n_{i+1} \mid n_i$ for each $i \in \{1, 2, \ldots, t-1\}$. Moreover, this decomposition is unique in the sense that if

$$G \cong \mathbb{Z}^u \times \mathbb{Z}/m_1\mathbb{Z} \times \cdots \mathbb{Z}/m_v\mathbb{Z}$$

where $u, v \geq 0$, each $m_i \geq 2$, and $m_{i+1} \mid m_i$, then $u = r,\ v = t$, and $n_i = m_i$ for each i.

(b) Classify abelian groups of order 100 up to isomorphism.
That is, give a list of abelian groups such that every abelian group of order 100 is isomorphic to exactly one of the groups in your list.

Solution: Since $100 = 2^2 \cdot 5^2$ By the fundamental theorem, we have G is isomorphic to one of the following groups:

$$\mathbb{Z}/100\mathbb{Z},\ \mathbb{Z}/50\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z},\ \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}.$$

(c) How many isomorphism classes are there are abelian groups of order $27000 = 2^3 \cdot 3^3 \cdot 5^3$?
You only need to write a number. No additional explanation is needed.

Solution: It is easier to do this count using the Primary Decomposition Theorem. Let $|G| = 27000$. The number of possibilities for the Sylow 2-subgroup of G is equal to the number of partitions of 3, which is 3. (This group could be isomorphic to $\mathbb{Z}/2^3\mathbb{Z}$ or $\mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.) The number of choices for the other two Sylow subgroups is the same. So the total number of possibilities is $3 \cdot 3 \cdot 3 = 27$.

4. (a) Let R be a ring with identity 1. Let u be a unit in R.
Prove that the multiplicative inverse of u in R is unique.

Solution: Since u is a unit, there exists a $v \in R$ such that $uv = vu = 1$. Suppose $uw = 1$. Then $v(uw) = v \cdot 1 = v$. But we also have $v(uw) = (vu)w = 1 \cdot w = w$. So $v = w$.

(b) What is the inverse of the element $2 + \sqrt{2}$ in $\mathbb{Q}(\sqrt{2})$?
Give a **brief explanation** for how you know this is the inverse.

Solution: We have that $(2+\sqrt{2})(2-\sqrt{2}) = 2^2 - (\sqrt{2})^2 = 2$. Therefore, $(2+\sqrt{2}) \cdot (1 - \frac{1}{2} \cdot \sqrt{2}) = 1$. So $(2+\sqrt{2})^{-1} = 1 - \frac{1}{2}\sqrt{2}$.

5. Let p be a prime and H be a subgroup of S_p of order p.
What is $|N_{S_p}(H)|$, the order of the normalizer of H?
Prove that your answer is correct.

Solution: Since $|S_p| = p!$ is not divisible by p^2, a Sylow p-subgroup of S_p has order p. Every such subgroup is cyclic because p is prime. The order of an element is S_n is the least common multiple of the lengths of the cycles that occur in the decomposition into a product of disjoint cycles. The only elements of order p in S_p are therefore the p-cycles.

There are $(p-1)!$ p-cycles in S_p. (Write your cycle with 1 listed first. There are $(p-1)!$ to arrange the remaining numbers.) Each subgroup of order p contains $p-1$ of these p-cycles. The intersection of any pair of these subgroups is trivial by Lagrange's theorem. We recall that if G has k subgroups of order p then it has $k(p-1)$ elements of order p. Since S_p has $(p-1)!$ elements of order p, it must have $\frac{(p-1)!}{p-1} = (p-2)!$ subgroups of order p.

We see that $H \in \mathrm{Syl}_p(S_p)$. By Sylow III*, $n_p = (p-2)! = [S_p \colon N_{S_p}(H)]$. This implies that $(p-2)! = \frac{p!}{|N_{S_p}(H)|}$. Therefore, $|N_{S_p}(H)| = p(p-1)$.

6. Prove that no group of order $150 = 2 \cdot 3 \cdot 5^2$ is simple.

   Solution: Suppose G is a simple group with $|G| = 150$. By Sylow III, $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 6$. If G is simple, then $n_5 \neq 1$, which means $n_5 = 6$. Let $P \in \mathrm{Syl}_5(G)$. By Sylow III*, $6 = n_5 = [G \colon N_G(P)]$.

   Therefore, $N_G(P) \leq G$ has index 6. Let G act on the cosets of this subgroup by left multiplication. This is a group action, which gives a homomorphism $\varphi \colon G \to S_{G/N_G(P)} \cong S_6$.

   The kernel of this homomorphism is contained in $N_G(P)$. This is because $g \in \ker(\varphi)$ implies $g \cdot 1N_G(P) = gN_G(P) = 1N_G(P)$. Since $\ker(\varphi) \trianglelefteq G$ and G is simple, we have $\ker(\varphi) = \{1\}$.

   By the First Isomorphism Theorem, we have $|G| = |\varphi(G)| \mid |S_6| = 720$. Since 150 does not divide 720, this is a contradiction.

7. (a) Define what it means for a group G to be solvable.

   Solution: G is solvable if there is a chain of subgroups,

   $$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$$

   such that G_{i+1}/G_i is abelian for all $i \in \{0, 1, \ldots, n-1\}$.

   (b) Give an example of a nonabelian group of order 60 that is solvable.

   Solution: D_{60} is a nonabelian group of order 60. It is solvable because

   $$\{1\} \trianglelefteq \langle r \rangle \trianglelefteq D_{60}$$

   and $D_{60}/\langle r \rangle \cong \mathbb{Z}/2\mathbb{Z}$ (this quotient has order 2), and $\langle r \rangle/\{1\} \cong \langle r \rangle$ is abelian.

8. Let H and K be groups and $\varphi \colon K \to \mathrm{Aut}(H)$ be a homomorphism. Let $G = H \rtimes_\varphi K$.

   (a) Let $(h_1, k_1), (h_2, k_2) \in G$. What is $(h_1, k_1) \cdot (h_2, k_2)$?

   Solution: We have $(h_1, k_1) \cdot (h_2, k_2) = (h_1 \varphi_{k_1}(h_2), k_1 k_2)$, where φ_{k_1} is just different notation for $\varphi(k_1)$.

   (b) Let $(a, x), (b, y), (c, z) \in G$. Prove that

   $$((a, x) \cdot (b, y)) \cdot (c, z) = (a, x) \cdot ((b, y) \cdot (c, z)).$$

   Solution: We have $(a, x) \cdot (b, y) = (a\varphi_x(b), xy)$ and $(b, y) \cdot (c, z) = (b\varphi_y(c), yz)$. Therefore,

   $$((a, x) \cdot (b, y)) \cdot (c, z) = (a\varphi_x(b), xy) \cdot (c, z) = (a\varphi_x(b)\varphi_{xy}(c), (xy)z).$$

Also,

$$(a,x)\cdot((b,y)\cdot(c,z)) = (a,x)\cdot(b\varphi_y(c), yz) = (a\varphi_x((b\varphi_y(c))), x(yz)).$$

We have $(xy)z = x(yz)$ since K is a group. Therefore, we need only show that

$$a\varphi_x(b)\varphi_{xy}(c) = a\varphi_x(b\varphi_y(c)).$$

Since $\varphi_x \in \mathrm{Aut}(H)$ we have $\varphi_x(\varphi_y(c)) = \varphi_{xy}(c)$ and so $a\varphi_x(b)\varphi_{xy}(c) = a\varphi_x(b\cdot\varphi_y(c))$.

9. (a) Define what it means for a commutative ring with identity $1 \neq 0$ to be an integral domain.

   Solution: A commutative ring with identity $1 \neq 0$ is an integral domain if and only if it has no zero divisors. (A zero divisor is a nonzero element $a \in R$ such that there exists a nonzero element b with $a \cdot b = 0$.)

   (b) Which of the following rings are integral domains?
   No explanation is needed. Just say whether each ring is or is not an integral domain.

   i. $\mathbb{Z}[x]$.
   ii. $\mathbb{Z}/10\mathbb{Z}$.
   iii. $M_2(\mathbb{R})$.

   Solution: $\mathbb{Z}[x]$ is an integral domain. $\mathbb{Z}/10\mathbb{Z}$ is not because 5 is a zero divisor. $M_2(R)$ is not because $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is a zero divisor.