Updated April 4, 2024

Homework problems for AMAT 327 (Elementary Abstract Algebra), Spring 2024. Over the course of the semester I'll add problems to this list, with each problem's due date specified. Each problem is worth 2 points.

Solutions will be gradually added (and may be hastily written without proofreading).

(These first three problems are just to make sure everyone's on the same page with proof techniques and so forth.)

Problem 1 (due Thurs 1/25): Let $f\colon A \to B$ and $g\colon B \to C$ be functions. Prove that if f and g are one-to-one then so is $g \circ f$.

Solution: Let $a, a' \in A$ such that $g(f(a)) = g(f(a'))$. Since g is injective, $f(a) = f(a')$. Then since f is injective, $a = a'$. We conclude that $g \circ f$ is injective. $\square$

Problem 2 (due Thurs 1/25): Use proof by contradiction to prove that the intersection $\{28a - 21b \mid a, b \in \mathbb{Z}\} \cap \{7c + 1 \mid c \in \mathbb{Z}\}$ is empty.

Solution: Suppose it is non-empty, say x is an element of both sets. Then $x = 28a - 21b$ for some $a, b \in \mathbb{Z}$, and $x = 7c+1$ for some $c \in \mathbb{Z}$. Thus $28a-21b = 7c+1$, so $1 = 7(4a-3b-c)$, which contradicts that 7 does not divide 1. $\square$

Problem 3 (due Thurs 1/25): Use mathematical induction to prove that $n^2 - n$ is even for all $n \in \mathbb{N}$. (Don't just split into the cases when n is even/odd, actually use induction.)

Solution: Base case $n = 1$: We check that $1^2-1 = 0$ is even. Now suppose $n \geq 2$, and assume that $(n-1)^2-(n-1)$ is even, say it equals $2k$ for some $k \in \mathbb{Z}$. Then $n^2-2n+1-n+1 = 2k$, so $n^2 - n = 2k + 2n - 2 = 2(k + n - 1)$ is even. $\square$

Problem 4 (due Thurs 2/1): Compute the inverse of $\sigma \in S_6 = \mathrm{Sym}(\{1, 2, 3, 4, 5, 6\})$, where σ is expressed in cycle notation as $\sigma = (1\ 4\ 5)(2\ 6)$. (Write your answer in cycle notation.)

Solution: It's $(1\ 5\ 4)(2\ 6)$.

Problem 5 (due Thurs 2/1): Let $R = \{(x, y) \in \mathbb{R}^2 \mid y \geq |x|\}$. Prove that R has exactly two symmetries (the identity and one other symmetry).

Solution: The identity and the reflection across the y-axis are two symmetries. To see that these are the only ones, note that any symmetry must fix the origin since that's the only point in R that does not lie in the interior of a line segment contained in R (and isometries of R must take line segments to/from line segments). This implies that every symmetry of R is induced by an isometric linear transformation $\mathbb{R}^2 \to \mathbb{R}^2$ (so rotations and reflections), and it is easy to see that none of these take R bijectively to R except the identity and the y-axis reflection. $\square$

Problem 6 (due Thurs 2/1): Let $\sigma, \tau \in S_5$ such that σ and τ are both 3-cycles. Prove that if $\sigma \circ \tau = \tau \circ \sigma$ then either $\sigma = \tau$ or $\sigma = \tau^{-1}$. [Hint: The contrapositive might be easier. (Maybe.)]

Solution: Suppose $\sigma \neq \tau$ and $\sigma \neq \tau^{-1}$. Say without loss of generality that $\sigma = (1\ 2\ 3)$, and say $\tau = (a\ b\ c)$ for some $a < b < c$ in $\{1, \dots, 5\}$. Our hypotheses ensure that $a \leq 3$ and $c \geq 4$, so in particular $\sigma(a) \neq a$ and $\sigma(c) = c$. Now observe that $\sigma \circ \tau(c) = \sigma(a) \neq a$, and $\tau \circ \sigma(c) = \tau(c) = a$, so $\sigma \circ \tau \neq \tau\sigma$. $\square$

Problem 7 (due Thurs 2/8): Which elements of $\mathbb{Z}_{12}$ are zero divisors? Which are invertible? For those that are invertible, compute their inverses.

Solution: You can compute that 2, 3, 4, 6, 8, 9, and 10 are zero divisors mod 12, and 1, 5, 7, and 11 are invertible mod 12, in fact they are each their own inverses mod 12.

Problem 8 (due Thurs 2/8): Prove that the set $\mathbb{N}$ with the product $(m, n) \mapsto \mathrm{lcm}(m, n)$ (meaning least common multiple) is not a group.

Solution: Suppose it is a group, and let e be the identity element. Then $\mathrm{lcm}(e, 1) = 1$, so 1 is a multiple of e, which implies $e = 1$. But now if n is the inverse of 2, we have $\mathrm{lcm}(2, n) = 1$, but 1 is not a multiple of 2, so this is a contradiction. $\square$

Problem 9 (due Thurs 2/8): Let $\phi \colon G \to H$ be an isomorphism of groups. Prove that the inverse $\phi^{-1} \colon H \to G$ is also an isomorphism.

Solution: It is clearly bijective, so we need to prove it is a homomorphism. Let $h, h' \in H$. Let $g = \psi^{-1}(h)$ and $g' = \psi^{-1}(h')$. Then $\psi^{-1}(hh') = \psi^{-1}(\psi(g)\psi(g')) = \psi^{-1}(\psi(gg')) = gg' = \psi^{-1}(h)\psi^{-1}(h')$. Since h and h' were arbitrary, ψ^{-1} is a homomorphism. $\square$

Problem 10 (due Thurs 2/15): Let G and H be groups, with identity elements 1_G and 1_H respectively. Let $\phi \colon G \to H$ be a homomorphism. Prove that $\phi(1_G) = 1_H$.

Solution: We have $\phi(1_G) = \phi(1_G \cdot 1_G) = \phi(1_G) \cdot \phi(1_G)$, so multiplying by $\phi(1_G)^{-1}$ we get $1_H = \phi(1_G)$. $\square$

Problem 11 (due Thurs 2/15): Write down an isomorphism from S_3 to the group G of symmetries of an equilateral triangle.

Solution: Number the vertices 1,2,3, and now any symmetry of the triangle induces a permutation of $\{1, 2, 3\}$. You can write down the correspondence, like reflecting through the line connecting 3 to the midpoint of the edge from 1 to 2 corresponds to (1 2), and so forth. (Easy to draw, hard to type.) $\square$

Problem 12 (due Thurs 2/15): Let $\psi\colon G \to H$ be a homomorphism. Let $K = \{g \in G \mid \psi(g) = 1_H\}$. Prove that K is a subgroup of G. [Hint: You can use the "easy subgroup criterion" that I forgot to mention in class today but will hopefully remember to mention on Tuesday.]

Solution: Since $\psi(1_G) = 1_H$, we know $1_G \in K$. Now let $g, g' \in K$, so $\psi(g) = \psi(g') = 1_H$. Then $\psi(g^{-1}g') = \psi(g)^{-1}\psi(g') = 1_H \cdot 1_H = 1_H$. We conclude that $g^{-1}g' \in K$. $\square$

Problem 13 (due Thurs 2/22): Let $H = \{\sigma \in S_n \mid \sigma(1) = 1\}$. Prove that H is a subgroup of S_n.

Solution: Since $\mathrm{id}(1) = 1$ we know $\mathrm{id} \in H$. Now let $\sigma, \tau \in H$, so $\sigma(1) = 1$ and $\tau(1) = 1$. Then $(\sigma^{-1} \circ \tau)(1) = \sigma^{-1}(1) = 1$, so $\sigma^{-1} \circ \tau \in H$. $\square$

Problem 14 (due Thurs 2/22): Let $\psi\colon G \to H$ be a homomorphism. Let $K = \{g \in G \mid \psi(g) = 1_H\}$. Prove that if $K = \{1\}$ [oops should have written $K = \{1_G\}$, hopefully this was clear] then ψ is injective.

Solution: Let $g, g' \in G$ such that $\psi(g) = \psi(g')$. Then $\psi(g^{-1}g') = \psi(g)^{-1}\psi(g') = 1_H$, so $g^{-1}g' \in K$. But $K = \{1_G\}$, so $g^{-1}g' = 1_G$, i.e., $g = g'$. $\square$

Problem 15 (due Thurs 2/22): Let G be a group and $H_\alpha \leq G$ a family of subgroups, indexed by some $\alpha \in I$. Prove that the intersection $\bigcap\limits_{\alpha \in I} H_\alpha$ is a subgroup of G.

Solution: Since $1 \in H_\alpha$ for all α (by virtue of each H_α being a subgroup), we have that 1 is in this intersection. Now let g and g' be in the intersection, so $g, g' \in H_\alpha$ for all α. Since each H_α is a subgroup, $g^{-1}g' \in H_\alpha$ for all α, and so $g^{-1}g'$ is in the intersection. $\square$

Problem 16 (due Thurs 2/29): Compute the order of $[1265]_{2024}$ in $\mathbb{Z}_{2024}$. [Hint: The relevant prime factorizations are $1265 = 5 \cdot 11 \cdot 23$ and $2024 = 2 \cdot 2 \cdot 2 \cdot 11 \cdot 23$.]

Solution: It's $2024/gcd(2024, 1265) = 2024/(11 \cdot 23) = 8$.

Problem 17 (due Thurs 2/29): Let G be a group and $S \subseteq G$ a subset such that $st = ts$ for all $s, t \in S$. Prove that the subgroup $\langle S \rangle \leq G$ is abelian.

Solution: Let $x, y \in \langle S \rangle$, say $x = s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n}$ and $y = t_1^{\delta_1} \cdots t_m^{\delta_m}$ for some $s_i, t_i \in S$ and $\varepsilon_i, \delta_i \in \{1, -1\}$. We know that $s_i t_j = t_j s_i$ for all i, j, and multiplying this equation by appropriate s_i^{-1} and t_j^{-1} on either side, we get $s_i t_j^{-1} = t_j^{-1} s_i$, $s_i^{-1} t_j = t_j s_i^{-1}$, and $s_i^{-1} t_j^{-1} = t_j^{-1} s_i^{-1}$ as well. Now in the product xy we can move every $t_j^{\delta_j}$ to the left of every $s_i^{\varepsilon_i}$, one at a time, until $xy = yx$. $\square$

Problem 18 (due Thurs 2/29): Let $\phi\colon G \to H$ be a group homomorphism. Let $S \subseteq G$. Prove that $\phi(\langle S \rangle) = \langle \phi(S) \rangle$.

Solution: ($\subseteq$): Let $h \in \phi(\langle S \rangle)$, say $h = \phi(g)$ for $g \in \langle S \rangle$. Write $g = s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n}$ for some $s_i \in S$ and $\varepsilon_i \in \{1, -1\}$. Now $h = \phi(g) = \phi(s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n}) = \phi(s_1)^{\varepsilon_1} \cdots \phi(s_n)^{\varepsilon_n}$, so $h \in \langle \phi(S) \rangle$.
($\supseteq$): Let $h \in \langle \phi(S) \rangle$, say $h = \phi(s_1)^{\varepsilon_1} \cdots \phi(s_n)^{\varepsilon_n}$. Then $h = \phi(g)$ for $g = s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n}$, so $g \in \langle S \rangle$, which shows that $h \in \phi(\langle S \rangle)$. $\square$

Problem 19 (due Thurs 3/7): Let G be an abelian group. Prove that every subgroup $H \leq G$ is normal.

Solution: For any $g \in G$ we have $gHg^{-1} = \{ghg^{-1} \mid h \in H\} = \{hgg^{-1} \mid h \in H\} = H$. $\square$

Problem 20 (due Thurs 3/7): Let $\phi\colon \mathbb{Z}_{12} \to \mathbb{Z}_9$ be the homomorphism $\phi([a]_{12}) := [3a]_9$. (Note that this is well defined, since if $a - b$ is a multiple of 12 then $3a - 3b$ is a multiple of 9.) Compute the kernel of ϕ.

Solution: Applying ϕ to each element of $\mathbb{Z}_{12}$, we see that the ones that map to $[0]_9$ are $\{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}$.

Problem 21 (due Thurs 3/7): Let $H \leq S_n$ be the subgroup from homework problem #13. Prove that if $n \geq 3$ then H is not a normal subgroup.

Solution: Let $\sigma = (2\ 3) \in H$ and let $\tau = (1\ 2)$. Then $\tau\sigma\tau^{-1} = (1\ 2)(2\ 3)(1\ 2) = (1\ 3) \notin H$. $\square$

Problem 22 (due Thurs 3/14): For $m \leq n$, view S_m as a subgroup of S_n via $S_m = \{\sigma \in S_n \mid \sigma(i) = i \text{ for all } m < i \leq n\}$. Compute the index $[S_n : S_m]$.

Solution: Since the groups involved are finite, the index is the quotient of the orders, i.e., $[S_n : S_m] = |S_n|/|S_m| = n!/m!$.

Problem 23 (due Thurs 3/14): View S_4 as a subgroup of S_5 as above, so $S_4 = \{\sigma \in S_5 \mid \sigma(5) = 5\}$. Let $T = \{\mathrm{id}, (1\ 5), (2\ 5), (3\ 5), (4\ 5)\}$. Prove that every coset of S_4 in S_5 contains an element of T.

Solution: Let σS_4 be a coset. Set $i = \sigma(5)$, and we claim that $(i\ 5) \in \sigma S_4$ (if $i = 5$ this means $\mathrm{id} \in \sigma S_4$). It suffices to prove that $\sigma^{-1}(i\ 5) \in S_4$. Indeed, $\sigma^{-1}(i\ 5)$ sends 5 to $\sigma^{-1}(i) = 5$, so $\sigma^{-1}(i\ 5) \in S_4$. $\square$

Problem 24 (due Thurs 3/14): Let G be a group and N a normal subgroup of G. Prove that if G is abelian then the quotient group G/N is abelian. Give an example to show that the converse is false.

Solution: Suppose G is abelian. Let $gN, hN \in G/N$. Then $(gN)(hN) = (gh)N = (hg)N = (hN)(gN)$, so G/N is abelian. For the converse being false, let $G = N = S_3$ (or any non-abelian group), so G is non-abelian but G/N is trivial, hence abelian. $\square$

Problem 25 (due Thurs 4/4): Let A and B be abelian groups. Prove that the direct product $G = A \times B$ is abelian.

Problem 26 (due Thurs 4/4): Prove that for any non-trivial subgroups A and B of $\mathbb{Q}$ (this is the group of rational numbers with operation $+$), the intersection $A \cap B$ is non-trivial. Explain why this proves that $\mathbb{Q}$ cannot be isomorphic to any direct product of non-trivial groups.

Problem 27 (due Thurs 4/4): Let G be a group. Let $H \leq G$ be a subgroup and $N \triangleleft G$ a normal subgroup. Let $HN := \{hn \mid h \in H \text{ and } n \in N\} \subseteq G$. Prove that HN is a subgroup of G. [Hint: The proof should look like, "Let $hn, h'n' \in HN$. Then blah blah blah hence $(hn)^{-1}(h'n') \in HN$."]

Problem 28 (due Thurs 4/11): Prove that $S = \{p(x) \in \mathbb{R}[x] \mid p(2) = 0 \text{ and } p(3) = 0\}$ is a subring of $\mathbb{R}[x]$.

Problem 29 (due Thurs 4/11): Prove that $S = \{p(x) \in \mathbb{R}[x] \mid p(2) = 0 \text{ or } p(3) = 0\}$ is not subring of $\mathbb{R}[x]$.

Problem 30 (due Thurs 4/11): Let R be a ring. Call an element $a \in R$ *idempotent* if $a^2 = a$. Say R has *characteristic 2* if $a + a = 0$ for all $a \in R$. Prove that if R is a commutative ring with characteristic 2, then the set of all idempotent elements forms a subring.
