Solutions to Extra Practice Problems for Midterm Exam 1

Saracino #2.1(d,e,h) [but now allowed to use later sections]: Which of the following are groups, and why?

Solutions. (d): $\{1, -1\}$ under multiplication. $\boxed{\text{YES, GROUP}}$

This set $H = \{\pm 1\}$ is a subset of the group $\mathbb{R}^\times$, and in fact it is the cyclic subgroup $\langle -1 \rangle$, i.e., all integer powers of -1. Thus, it is a subgroup, by a theorem from class [which is also Example 2 of Section 5], and hence a group. QED

(e): $\{x \in \mathbb{Q} \,|\, x > 0 \text{ and } x \text{ has a rational square root}\}$ under multiplication. $\boxed{\text{YES, GROUP}}$

Call this set H; it is a subset of the group $\mathbb{Q}^\times$.

Nonempty: $1 \in H$ since $1 \in \mathbb{Q}$, $1 > 0$, and $1 = 1^2$.

Closure: Given $x, y \in H$, then $x, y \in \mathbb{Q}$ with $x, y > 0$ and there exist $s, t \in \mathbb{Q}$ such that $s^2 = x$ and $t^2 = y$. Then $xy \in \mathbb{Q}$, and $xy > 0$, and $xy = (st)^2$ is the square of $st \in \mathbb{Q}$. So $xy \in H$.

Inverses: Given $x \in H$, then $x \in \mathbb{Q}$ with $x > 0$, and there exists $t \in \mathbb{Q}$ such that $t^2 = x$. Then $1/x \in \mathbb{Q}$ with $1/x > 0$ as well. We have $t \neq 0$, since otherwise $x = 0$, a contradiction; thus, $1/t \in \mathbb{Q}$, and $1/x = (1/t)^2$. So $1/x \in H$.

Thus, H is a subgroup of $\mathbb{Q}^\times$ and hence is a group. QED

(h): $\mathbb{R} \smallsetminus \{1\}$, under $a * b = a + b - ab$. $\boxed{\text{YES, GROUP}}$

Call this set G; but it's not a subset of an obvious group with that same operation, so we work from scratch. Also note that $a * b = 1 - (a-1)(b-1)$.

Bin Op: Given $a, b \in G$, we have $a, b \in \mathbb{R}$, so $a * b = a + b - ab \in \mathbb{R}$. In addition, we have $a \neq 1$ and $b \neq 1$, so $(a-1)(b-1) \neq 0$, and hence $a * b \neq 1$. Thus, $a * b \in G$, as desired.

Assoc: Given $a, b, c \in G$, we have

$$\begin{aligned}(a * b) * c &= \big(1 - (a-1)(b-1)\big) * c = 1 - \big(-(a-1)(b-1)\big)(c-1) \\ &= 1 - (a-1)\big((b-1)(c-1)\big) = a * \big(1 - (b-1)(c-1)\big) = a * (b * c)\end{aligned}$$

Identity: Let $e = 0 \in G$. Then for any $a \in G$, we have $e * a = 0 + a - 0(a) = a$, and $a * e = a + 0 - a(0) = a$, as desired.

Inverses: Given $a \in G$, let $b = \dfrac{a}{a-1}$. Then $b \in \mathbb{R}$ because $a \neq 1$. In addition, $b \neq 1$, because otherwise we would have $a = a - 1$, a contradiction. Thus, $b \in G$. We compute

$$b * a = a * b = a + \frac{a}{a-1} - \frac{a^2}{a-1} = \frac{(a^2 - a) + a - a^2}{a-1} = 0 = e$$

QED

Saracino #2.10 [but now allowed to use later sections]: Let G be the set of a 2×2 matrices $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, where $a, b \in \mathbb{R}$ and $a^2 + b^2 \neq 0$. Prove that G forms a group under multiplication.

Proof. The condition $a^2 + b^2 \neq 0$ says $\det A \neq 0$, where $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, and hence A is invertible. Thus, G is a subset of $GL(2, \mathbb{R})$. We now prove it's a subgroup:

Nonempty: We have $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G$, with $a = 1$ and $b = 0$, since then $a^2 + b^2 = 1 \neq 0$.

Closure: Given $A, B \in G$, write $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ and $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$ with $\det A, \det B \neq 0$. Then $\det(AB) = \det A \det B \neq 0$, and

$$AB = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -bc - ad & -bd + ac \end{pmatrix},$$

which has the same entries in the $(1,1)$ and $(2,2)$ positions, and the entries in the other two positions are negatives of one another. Thus, $AB \in G$.

Inverses: Given $A \in G$, write $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ with $\det A \neq 0$. Then $\det(A^{-1}) = 1/\det A \neq 0$, and

$$A^{-1} = \frac{1}{a^2+b^2}\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

has the same entries in the $(1,1)$ and $(2,2)$ positions, and the entries in the other two positions are negatives of one another. Thus, $A^{-1} \in G$. QED

Saracino #4.4: Find the orders of the elements 3, 4, 6, 7, and 18 in C_{30}.

Solution. Since C_{30} is generated by 1, which has order 30, and since each m is $m(1)$, a theorem on orders gives $o(m) = 30/(m, 30)$, so

$$o(3) = \frac{30}{(3,30)} = \frac{30}{3} = \boxed{10} \quad o(4) = \frac{30}{(4,30)} = \frac{30}{2} = \boxed{15} \quad o(6) = \frac{30}{(6,30)} = \frac{30}{6} = \boxed{5}$$

$$o(7) = \frac{30}{(7,30)} = \frac{30}{1} = \boxed{30}, \quad o(18) = \frac{30}{(18,30)} = \frac{30}{6} = \boxed{5}$$

Saracino #4.7: Let $G = \langle x \rangle$ be a cyclic group of order 24. List all the elements in G that are of order 4.

Solution. By a theorem, we have $o(x^m) = \dfrac{24}{(m,24)}$, and hence $o(x^m) = 4$ if and only if $(m, 24) = 6$.

The multiples m of 6 with $0 \le m < 24$ are $0, 6, 12, 18$. But $(0, 24) = 24$ and $(12, 24) = 12$. We are left with $m = 6, 18$ as the only such integers with $(m, 24) = 6$.

Thus, the desired elements of G are $\boxed{x^6 \text{ and } x^{18}}$

Saracino #4.19: Prove Theorem 4.4(i): Let G be a group and $x \in G$. Then $o(x) = o(x^{-1})$.

Proof. Let $S = \{n \ge 1 : x^n = e\}$ and $T = \{n \ge 1 : (x^{-1})^n = e\}$. We claim that $S = T$.

($\subseteq$): Given $n \in S$, we have $(x^{-1})^n = x^{-n} = (x^n)^{-1} = e^{-1} = e$, so $n \in T$.

($\supseteq$): Given $n \in T$, we have $x^n = (x^{-1})^{-n} = ((x^{-1})^n)^{-1} = e^{-1} = e$, so $n \in S$.

Having proven our claim that $S = T$, it follows that these sets are either both empty, in which case $o(x^{-1}) = \infty = o(x)$, or else they are both nonempty, in which case $o(x^{-1}) = \min T = \min S = o(x)$. QED

Saracino #4.22: Let G be an abelian group and let $x, y \in G$. Suppose that x and y are of finite order. Show that xy is of finite order and that, in fact, $o(xy)$ divides $o(x)o(y)$.

Proof. Let $m = o(x)$ and $n = o(y)$, both of which are positive integers, by hypothesis. Then mn is also a positive integer, and

$$(xy)^{mn} = x^{mn}y^{mn} = (x^m)^n(y^n)^m = e^n e^m = ee = e,$$

where the first equality is because G is abelian. So $o(xy)$ is finite, because there is *some* positive integer (namely mn) for which $x^{mn} = e$. Let $k = o(xy)$. Then by a theorem [specifically, Theorem 4.4(ii)], we have $k|mn$. QED

Saracino #5.1(b,g): Determine whether or not H is a subgroup of G:

Solutions. (b): $G = (\mathbb{Q}, +)$, $H = \mathbb{Z}$: $\boxed{\text{YES, SUBGROUP}}$

Nonempty: $0 \in \mathbb{Z}$, so $\mathbb{Z} \neq \varnothing$.

Closure: Given $m, n \in \mathbb{Z}$, then $m + n \in \mathbb{Z}$.

Inverses: Given $n \in \mathbb{Z}$, then $-n \in \mathbb{Z}$. QED

(g): $G = Q_8$, $H = \{1, i, j\}$: $\boxed{\text{NO, NOT SUBGROUP}}$

We have $i, j \in H$ but $ij = k \notin H$. QED

Note: Alternatively, H is not closed under inverses, e.g. $i \in H$ but $i^{-1} = -i \notin H$. There are other products and inverses that also cause problems.

Notation note: Saracino wrote $\{I, J, K\}$, but recall that Saracino's I, J, K are my $1, i, j$, respectively.

Saracino #5.4(c): How many subgroups does C_{36} have? What are they?

Solution. The positive divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$, and $1 \in C_{36}$ is a generator for this cyclic group.
By a theorem [specifically, Corollary 5.6], there is one subgroup of C_{36} for each of the above divisors, i.e., there are $\boxed{\text{nine subgroups}}$

By the same result, they are $\boxed{\langle 1\rangle = C_{36}, \langle 2\rangle, \langle 3\rangle, \langle 4\rangle, \langle 6\rangle, \langle 9\rangle, \langle 12\rangle, \langle 18\rangle, \langle 36\rangle = \{0\}}$

Saracino #5.9: Let $m\mathbb{Z}$ and $n\mathbb{Z}$ be subgroups of $(\mathbb{Z}, +)$. What condition on m and n is equivalent to $m\mathbb{Z} \subseteq n\mathbb{Z}$? What condition on m, n is equivalent to $m\mathbb{Z} \cup n\mathbb{Z}$ being a subgroup of $(\mathbb{Z}, +)$?

Answer/Proof. First question: the desired condition is $n|m$. We must now prove $n|m \Leftrightarrow m\mathbb{Z} \subseteq n\mathbb{Z}$.

($\Rightarrow$): Given $x \in m\mathbb{Z}$, there is some $k \in \mathbb{Z}$ such that $x = mk$. Since $n|m$, there is some $\ell \in \mathbb{Z}$ such that $m = \ell n$. Thus, $x = n(k\ell) \in n\mathbb{Z}$.

($\Leftarrow$): Since $m \in m\mathbb{Z} \subseteq n\mathbb{Z}$, there is some $k \in \mathbb{Z}$ such that $m = nk$. That is, $n|m$. QED

Second question: the desired condition is that $n|m$ or $m|n$. We now prove this condition holds if and only if $m\mathbb{Z} \cup n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

($\Rightarrow$): By the first part of this problem, we have $m\mathbb{Z} \subseteq n\mathbb{Z}$ or $n\mathbb{Z} \subseteq m\mathbb{Z}$. In the former case, the union is $n\mathbb{Z}$, and in the latter case it is $m\mathbb{Z}$. In either case, the union is a subgroup.

($\Leftarrow$): By a theorem, the fact that $m\mathbb{Z} \cup n\mathbb{Z}$ is a subgroup means that either $m\mathbb{Z} \subseteq n\mathbb{Z}$ or $n\mathbb{Z} \subseteq m\mathbb{Z}$. By the first part of this problem, then, we have $n|m$ or $m|n$. QED

Saracino #5.12: Find the center of (a) V_4 and (b) Q_8

Solution. (a): V_4 is abelian, so $\boxed{Z(V_4) = V_4}$ because every element commutes with every element.

(b): We have $i, j, k \notin Z(Q_8)$ because $ij = k \neq -k = ji$, and similarly $ik = -j \neq j = ki$, and hence for each of i, j, k, there is (at least one) element of Q_8 it doesn't commute with.
We also have $-i, -j, -k \notin Z(Q_8)$ because $(-i)(-j) = k \neq -k = (-j)(-i)$ and $(-i)(-k) = -j \neq j = (-k)(-i)$.
However, $1 \in Z(Q_8)$ because it's the identity. Checking -1, we see

$$(-1)i = -i = i(-1), \quad (-1)j = -j = j(-1), \quad (-1)k = -k = k(-1),$$
$$(-1)(-i) = i = (-i)(-1), \quad (-1)(-j) = j = (-j)(-1), \quad (-1)(-k) = k = (-k)(-1),$$

and of course -1 commutes with both itself and the identity. That is, -1 commutes with all 8 elements of Q_8, so $-1 \in Z(Q_8)$.
Summarizing, then, we have $\boxed{Z(Q_8) = \{\pm 1\}}$

Saracino #5.13: Find $Z(H)$ where H be the group in Example 7 (page 46), i.e.

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad \neq 0 \right\} \subseteq GL(2, \mathbb{R}).$$

Solution. We claim that $Z(H) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \neq 0 \right\}$, i.e., the set of all nonzero scalar multiples of the identity. We now prove this claim.

($\subseteq$): Let $A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, both of which belong to H.

Given $M \in Z(H)$, write $M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. Then M commutes with every element of H, so

$$\begin{pmatrix} 2a & 2b \\ 0 & d \end{pmatrix} = AM = MA = \begin{pmatrix} 2a & b \\ 0 & d \end{pmatrix},$$

so that $2b = b$ and hence $b = 0$; and also,

$$\begin{pmatrix} a & b+d \\ 0 & d \end{pmatrix} = BM = MB = \begin{pmatrix} a & a+b \\ 0 & d \end{pmatrix},$$

so that $b+d=a+b$, and hence $d=a$. (And recall $ad \neq 0$, so $a \neq 0$.) That is, $M = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ with $a \neq 0$, as desired.

($\supseteq$): Given M in the RHS, we have $M = aI$ for some $a \in \mathbb{R}^\times$, and where I is the 2×2 identity matrix. Then for any $C \in H$, we have

$$CM = C(aI) = a(CI) = aC = a(IC) = (aI)C = MC,$$

and hence $M \in Z(H)$ QED

Saracino #5.16: Give an example of a group G and a subset H of G such that H is closed under multiplication but H is *not* a subgroup of G.

Solution/Proof. Let $G = \mathbb{Z}$, and let $H = \{n \in \mathbb{Z} \,|\, n \geq 1\}$. Since "multiplication" by the operation means what we'd normally call "addition," observe that H has the desired property. Specifically, for any $m, n \in H$, we have $m+n \geq 1$, so $m+n \in H$. However, $1 \in H$ but $-1 \notin H$, so H is not a subgroup. QED

Saracino #5.17: Suppose H is a nonempty finite subset of a group G and H is closed under inverses. Must H be a subgroup of G?

Solution/Proof. $\boxed{\text{NO}}$

For example, let $G = \mathbb{Z}$, and let $H = \{\pm 1\}$. Then H is closed under inverses, because -1 and 1 are inverses of each other. However, $1 \in H$ but $1+1 = 2 \notin H$, so H is not a subgroup of G.

Saracino #5.22: Let G be a group. Prove that its center $Z(G)$ is a subgroup of G.

Proof. [Clearly $Z(G) \subseteq G$.]

Nonempty: For all $g \in G$, we have $eg = g = ge$, and hence $e \in Z(G)$.

Closure: Given $x, y \in Z(G)$. [We'll show that $xy \in Z(G)$.] Given $g \in G$, we have

$$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy).$$

Thus, $xy \in Z(G)$.

Inverses: Given $x \in Z(G)$. [We'll show that $x^{-1} \in Z(G)$.] Given $g \in G$, we have

$$x^{-1}g = x^{-1}gxx^{-1} = x^{-1}xgx^{-1} = gx^{-1}.$$

Thus, $x^{-1} \in Z(G)$. QED

Saracino #5.26: Let H be a subgroup of a group G and let $N(H) = \{a \in G \,|\, aHa^{-1} = H\}$. Prove that $N(H)$ is a subgroup of G.

Proof. **Nonempty**: We claim $e \in N(H)$. Indeed, $eHe^{-1} = eHe = H$, so yes, $e \in N(H)$.

Closure: Given $a, b \in N(H)$, then

$$(ab)H(ab)^{-1} = a\big(bHb^{-1}\big)a^{-1} = aHa^{-1} = H,$$

so $ab \in H$.

Inverses: Given $a \in N(H)$, then
mallskip

$$(a^{-1})H(a^{-1})^{-1} = a^{-1}Ha = a^{-1}\big(aHa^{-1}\big)a = eHe = H,$$

so $a^{-1} \in H$.

Saracino #6.1(a,b): Calculate the order of (a): $(4,9)$ in $C_{18} \times C_{18}$ and (b): $(7,5)$ in $C_{12} \times C_8$.

Solution/Proof.

(a): By a theorem [specifically, 4.4(iii)], we have $o(4) = \dfrac{18}{(4,18)} = \dfrac{18}{2} = 9$ and $o(9) = \dfrac{18}{(9,18)} = \dfrac{18}{9} = 2$ in C_{18}. Thus, by another Theorem [specifically, 6.1(a)], we have $o((4,9)) = \mathrm{lcm}(9,2) = \boxed{18}$

(b): By the same theorems, we have $o(7) = \dfrac{12}{(7,12)} = \dfrac{12}{1} = 12$ in C_{12} and $o(5) = \dfrac{8}{(5,8)} = \dfrac{8}{1} = 8$ in C_8.

Thus, by another Theorem [specifically, 6.1(a)], we have $o((7,5)) = \text{lcm}(12,8) = \boxed{24}$

Saracino #6.2(c): Is the group $C_4 \times C_{25} \times C_6$ cyclic?

Solution/Proof. By a Theorem [specifically, 6.2(ii)], this product of finite cyclic groups is itself cyclic iff the orders 4, 25, 6 are pairwise relatively prime. However, $(4,6) = 2 \neq 1$, so they are not pairwise relatively prime. Therefore, $\boxed{C_4 \times C_{25} \times C_6 \text{ is not cyclic}}$

Saracino #6.3: Is $\mathbb{Z} \times \mathbb{Z}$ cyclic?

Solution/Proof. $\boxed{\text{NO}}$

We must show that for any $(a,b) \in \mathbb{Z} \times \mathbb{Z}$, the cyclic subgroup $\langle (a,b) \rangle = \{n(a,b) \,|\, n \in \mathbb{Z}\}$ generated by (a,b) is *not* all of $\mathbb{Z} \times \mathbb{Z}$, i.e., there is some $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ with $(x,y) \notin \langle (a,b) \rangle$.

So: given $(a,b) \in \mathbb{Z} \times \mathbb{Z}$, we consider two cases:

Case 1: Suppose $a = 0$. Then for any $n \in \mathbb{Z}$, we have $n(a,b) = (0,nb) \neq (1,0)$, so $(1,0) \notin \langle (a,b) \rangle$.

Case 2: Suppose $a \neq 0$. Then for any $n \in \mathbb{Z}$, we claim that $n(a,b) \neq (0,1)$. To prove the claim, note that if $n = 0$, then $n(a,b) = (0,0) \neq (0,1)$. And if $n \neq 0$, then $na \neq 0$, so $n(a,b) = (na,nb) \neq (0,1)$, proving our claim.

Either way, we have shown $\langle (a,b) \rangle$ is not all of $\mathbb{Z} \times \mathbb{Z}$ QED

Note: There are *many* ways to do this proof; this is just one way to do it.

Saracino #6.5: Let G, H be groups with subgroups $A \subseteq G$ and $B \subseteq H$. Prove that $A \times B$ is a subgroup of $G \times H$.

Proof. (**Nonempty**): Let e_G and e_H be the identity elements of G and H, respectively. Then $e_G \in A$ and $e_H \in B$, so $(e_G, e_H) \in A \times B$.

(**Closure**): Given (a_1, b_1) and (a_2, b_2) in $A \times B$, then $a_1 a_2 \in A$ and $b_1 b_2 \in B$ since A, B are subgroups. Thus, $(a_1 a_2, b_1 b_2) \in A \times B$.

(**Inverses**): Given $(a,b) \in A \times B$, then $a^{-1} \in A$ and $b^{-1} \in B$ since A, B are subgroups. Thus, $(a^{-1}, b^{-1}) \in A \times B$. QED

Saracino #6.7: Construct a nonabelian group of order 16, and one of order 24.

Solution/Proof. Let $G = Q_8 \times C_2$. Then $|G| = |Q_8| \cdot |C_2| = 8 \cdot 2 = 16$, but G is nonabelian because Q_8 is nonabelian.

Let $H = Q_8 \times C_3$. Then $|G| = |Q_8| \cdot |C_3| = 8 \cdot 3 = 24$, but H is nonabelian because Q_8 is nonabelian.

Saracino 7.7: Let G be a group, and let $a \in G$. Define a function $f : G \to G$ by $f(x) = axa^{-1}$ for all $x \in G$. Is f one-to-one? Is f onto?

Answer/Proof. $\boxed{\text{YES, ONE-TO-ONE AND ONTO}}$

1-1: Given $x, y \in G$ with $f(x) = f(y)$, we have $axa^{-1} = aya^{-1}$. Cancelling on the right gives $ax = ay$, so cancelling on the left gives $x = y$.

Onto: Given $y \in G$, let $x = a^{-1}ya \in G$. Then

$$f(x) = a\big(a^{-1}ya\big)a^{-1} = eye = y$$

as desired. QED

Saracino 7.10(b): Prove that $f : S \to T$ is onto if and only if there exists a function $g : T \to S$ such that $f \circ g = \text{id}_T$.

Proof. $(\Rightarrow)$: Define $g : T \to S$ by

$$g(t) = \text{ some particular element of } S \text{ such that } f(s) = t.$$

That is, for each $t \in T$, pick an $s \in S$ such that $f(s) = t$, and define $g(t)$ to be that s. (For each $t \in T$, such $s \in S$ exists since f is onto.)

To show that $f \circ g = \mathrm{id}_T$, first note that both of these functions are maps from T to T, so they already share the same domain and the same target set. Given $t \in T$, let $s = g(t)$, so that by our definition above, we have $f(s) = t$. Thus,

$$f \circ g(t) = f(s) = t = \mathrm{id}_T(t).$$

Hence, $f \circ g = \mathrm{id}_T$.
($\Leftarrow$): Given $t \in T$, define $s = g(t)$. Then $f(s) = f(g(t)) = f \circ g(t) = \mathrm{id}_T(t) = t$. QED

[**Note**: In the forward implication part, if T is infinite, technically we have to assume the Axiom of Choice from set theory to make the infinitely many choices we made in defining g. But never mind.]

Saracino #7.11: Let $f : S \to T$ and $g : T \to U$.
(a) If $g \circ f$ is one-to-one, must both f and g be one-to-one?
(b) If $g \circ f$ is onto, must both f and g be onto?

Solution/Proof. (a): $\boxed{\text{NO}}$: g need not be one-to-one.
For example, let $S = U = \{1\}$ and $T = \{1, 2\}$, and define $f : S \to T$ by $f(1) = 1$, and $g : T \to U$ by $g(1) = g(2) = 1$.
Then g is not one-to-one, because $g(1) = g(2)$ but $1 \neq 2$, whereas $g \circ f : S \to U$ is the identity map, which *is* one-to-one

---

(b): $\boxed{\text{NO}}$: f need not be onto
Use the same example as in part (a). Then f is not onto, because $2 \in T$ but there is no $x \in S$ with $f(x) = 2$. However, $g \circ f$ is the identity map, which *is* onto.