Chapter 3 Selected Solutions Math 145, Abstract Algebra, Duchin

3.1.2 For each binary operation $*$, does the set with $*$ define a group?

(a),(c),(e) are in the back of the book, so I'll just do the others. Note: I will often use the letter e for the identity element.

(b) [$a * b = \max\{a, b\}$ on $\mathbb{Z}$] This is not a group because there is no identity. There's no integer e such that $\max\{a, e\} = a$ for all a. To see this, suppose there were such an integer e, and let $a = e - 1$. Then

$$a * e = \max\{a, e\} = \max\{e - 1, e\} = e \neq a.$$

(d) [$a*b = |ab|$ on $\mathbb{Z}$] Again, there is clearly no identity, which would be an integer e such that $|ae| = a$ for all a. To see this, note that $|ae|$ is always nonnegative, so can't equal a if $a < 0$.

(f) [$a * b = ab$ on $\mathbb{Q}$] So close and yet so far! This can't be a group because 0 has no inverse (there's nothing to multiply by 0 to get back to 1, which is clearly the multiplicative identity). However, this is the only obstruction: if you removed 0, then it would form a group.

3.1.9 Let $G = \{x \in \mathbb{R} : x > 0,\ x \neq 1\}$. Define $a * b = a^{\ln b}$. Prove it's an abelian group.

We need to show that this is a binary operation, so we check that the output is real: yes. Next, we need associativity, identity, and inverses.

Associativity: $a * (b * c) = a^{\ln(b*c)} = a^{\ln(b^{\ln c}} = a^{\ln c \cdot \ln b}$. On the other hand, $(a * b) * c) = (a^{\ln b}) * c = (a^{\ln b})^{\ln c} = a^{\ln b \cdot \ln c}$ by laws of exponents. These are equal.

Identity: this is kind of convenient, because we often write e for the identity, and here the identity is the actual number $e = 2.71828....$ Check: $e * a = e^{\ln a} = a$ and $a * e = a^{\ln e} = a^1 = a$ by laws of exponents.

Inverses: given a, we need to solve $a^{\ln b} = e$ for b. Taking ln of both sides, I get $\ln b \cdot \ln a = 1$, so $\ln b = 1/\ln a$, so $b = e^{1/\ln a}$. (And we note that this b is a positive real not equal to 1.) So we've found a b for which $a * b = e$. Now let's check that for this same value, $b * a = e$. We have: $b * a = (e^{1/\ln a})^{\ln a} = e^1 = e$ ✓

Abelian: why does $a^{\ln b} = b^{\ln a}$? Because if you take the ln of either side, you get $\ln a \cdot \ln b$. If two numbers have the same result when you take their natural log, they are equal (ln is injective).

3.1.11 Show that the set of all 2×2 real matrices of the form $\left[\begin{smallmatrix} m & b \\ 0 & 1 \end{smallmatrix}\right]$ with $m \neq 0$ forms a group under matrix multiplication.

Well, since these matrices have determinant m which is not 0, the set of all of them is a subset of $GL_2(\mathbb{R})$, so we get associativity for free since we know that $GL_2(\mathbb{R})$ is a group.

Closure: $\left[\begin{smallmatrix} m & b \\ 0 & 1 \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} n & c \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} mn & mc+b \\ 0 & 1 \end{smallmatrix}\right]$ ✓ (note: $mn \neq 0$ since $m, n \neq 0$.)

Identity: $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ is the multiplicative identity for 2×2 matrices, and it's in there. ✓

Inverses: $\left[\begin{smallmatrix} m & b \\ 0 & 1 \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} 1/m & -b/m \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, this is of the right form (note: $1/m \neq 0$), and we already know that inverses are unique in $GL_2(\mathbb{R})$. ✓

3.1.12 In the group from the last exercise, find all elements that commute with $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$.

Well, $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2m & 2b \\ 0 & 1 \end{bmatrix}$ while $\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2m & b \\ 0 & 1 \end{bmatrix}$, so these are equal iff $b = 2b$, i.e., $b = 0$. Thus the set of such matrices is those of the form $\begin{bmatrix} m & 0 \\ 0 & 1 \end{bmatrix}$.

3.1.13 Let $S = \mathbb{R} \setminus \{-1\}$. Define $a * b = a + b + ab$. Show that $(S, *)$ is a group.

To see that it's a binary operation, we just have to check that $a + b + ab \neq -1$ whenever $a, b \neq -1$. We have

$$a + b + ab = -1 \iff a(1 + b) = -1 - b = -1(1 + b) \iff (1 + a)(1 + b) = 0.$$

The only solutions to this are $a = -1$ or $b = -1$.
Associativity: On one hand, $a*(b*c) = a*(b+c+bc) = a+b+c+bc+ab+ac+abc$. On the other hand, $(a * b) * c = (a + b + ab) * c = a + b + ab + c + ac + bc + abc$. These are equal.
Identity: $e = 0$. We have $a * e = a + 0 + 0 = a$; $e * a = 0 + a + 0 = a$.
Inverses: Given a, we must solve $a + b + ab = 0$ for b. We have

$$b(1 + a) = -a \implies b = \frac{-a}{1 + a}.$$

(Note: for this to equal -1, we would have to have $a/(1 + a) = 1$, or $a = 1 + a$, which is impossible.) We have found a solution for $a * b = 0$, and it only remains to check $b * a = 0$ for this b. But the operation is clearly commutative because addition and multiplication of reals are commutative, so we are done.

3.1.16 Show that a nonabelian group must have at least five distinct elements.

First let us prove a simple lemma.

Lemma: *If a and b are not the identity, then their product ab can't equal a or b.*
Proof: If $ab = a$, then cancellation gives $b = e$. Likewise $ab = b \implies a = e$. □
This makes things pretty easy. There's nothing to check for a one-element group. For a two element group $\{e, a\}$, there's also nothing to check, because $ea = ae$ by definition of identity anyway.
How about a three-element group $\{e, a, b\}$? Well, here we must have $ab = e$ by the lemma, and for the same reason $ba = e$, so the group is abelian.
Finally, we consider a four-element group $\{e, a, b, c\}$. We know that e commutes with everything, and of course everything commutes with itself, so we only need to show that $gh = hg$ for all choices of g, h as distinct nonidentity letters. Without loss of generality, it suffices to show $ab = ba$. But there are only two possibilities, $ab = e$ or $ab = c$. Suppose $ab = e$. Then $b = a^{-1}$, so $ba = e$, and they commute. The last case is $ab = c$. But then we also have $ba = e$ or c. If $ba = e$, then they are inverses, contradicting $ab = c$. So $ba = c = ab$, and we've shown that they commute.

3.1.17 Let G be a group. For $a, b \in G$, prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$ iff $ab = ba$.

Backward direction: suppose $ab = ba$. Then for $n > 0$, we can take any expression $(ab)^n = (ab)(ab)\cdots(ab)$ and swap the a letters to the left past each of the b letters, obtaining $a^n b^n$. For $n = 0$ there is nothing to prove, since $e = e$. For $n < 0$, we must show that $(ab)^{-m} = a^{-m}b^{-m}$ where $m = -n > 0$. But the meaning of raising something to the $-m$ power is raising its inverse to the m power, so the left-hand side becomes $(b^{-1}a^{-1})^m$ and the right-hand side becomes $(a^{-1})^m(b^{-1})^m$. We can now just swap them past each other once we check that they commute. But we know that $ab = ba$. Taking the inverse of both sides gives us $b^{-1}a^{-1} = a^{-1}b^{-1}$, so the inverses commute and we are done.

Forward direction: if the identity is true for all n, then in particular it's true for $n = 2$. So we can assume that $(ab)^2 = a^2b^2$, or in other words $abab = aabb$. Canceling an a on the left and a b on the right, we get $ba = ab$, as desired.

3.2.5 Find all cyclic subgroups of... (b) $\mathbb{Z}_8$; (d) S_4

For $\mathbb{Z}_8$: We have $\langle 0\rangle = \{0\}$. For anything relatively prime to 8, it generates the full group, so we have $\langle 1\rangle = \langle 3\rangle = \langle 5\rangle = \langle 7\rangle = \mathbb{Z}_8$. We know that a generates the same subgroup as a^{-1} in general, so we have $\langle 2\rangle = \langle 6\rangle = \{0, 2, 4, 6\}$. And finally $\langle 4\rangle = \{0, 4\}$. We've found four distinct cyclic subgroups in all.
For S_4: there are $4! = 24$ elements. There is 1 identity, there are 6 transpositions, there are 8 3-cycles, 6 4-cycles, and three remaining elements like $(12)(34)$ that are products of two disjoint transpositions. Of course we have the trivial subgroup $\langle e\rangle = \{e\}$. And clearly each transposition, such as (12), generates its own two-element cyclic subgroup, such as $\langle(12)\rangle = \{e, (12)\}$. So there are six of these. Now the ones generated by 3-cycles can be generated two ways, such as $\langle(123)\rangle = \langle(132)\rangle = \{e, (123), (132)\}$, so there are four of these, since there are 8 3-cycles. The four-cycles also double up: $\langle(1234)\rangle = \langle(1432)\rangle = \{e, (1234), (13)(24), (1432)\}$. Note that, importantly, even though $(13)(24)$ *appears in* this subgroup, it does not generate it! So there are 3 distinct cyclic subgroups generated by 4-cycles. Finally, the double transpositions like $(13)(24)$ have order two, so they generate subgroups of the form $\langle(13)(24)\rangle = \{e, (13)(24)\}$, and there are three of them. So in all, we have classified the cyclic subgroups into $1 + 6 + 4 + 3 + 3 = 17$ different ones, out of a possible 24.

3.2.9 Show that $H := \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \right\}$ is a subgroup of $GL_3(\mathbb{R})$.

In fact, this H is a famous group called the **Heisenberg group**. As we learned in Prop 3.2.2, we need only check for closure, identity, and inverses to check H is a subgroup. Clearly the identity is in H (letting $a = b = c = 0$). Closure:

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+x & b+y+az \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{bmatrix} \quad \checkmark$$

Inverses:

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \checkmark$$

(We already know that in $GL_3(\mathbb{R})$, a right-hand inverse is also a left-hand inverse.)

3.2.11 For fixed $a \in S$, show $\{\sigma \in Sym(S) : \sigma(a) = a\}$ is a subgroup.

Again, we check closure, identity, and inverses for the collection of permutations of S that fix our element a.
If σ, τ both fix a, then $\sigma\tau(a) = \sigma(a) = a$, so $\sigma\tau$ fixes a as well, which shows closure.
The identity map fixes every element, so in particular it fixes a.
Finally, if σ fixes a, consider σ^{-1}. This must exist because $Sym(S)$ is a group. But $\sigma(a) = a \implies \sigma^{-1}(a) = a$, so the inverse fixes a as well.

Note: a permutation of S fixing a is in obvious correspondence with a permutation of $S \setminus \{a\}$: to specify such a map, you only need to know what it does to all the other elements! So since $Sym(S \setminus \{a\})$ is a group, this is another way to approach this question.

3.2.14 If G is abelian, show that the set of finite-order elements forms a subgroup.

Let $F = \{a \in G : o(a) < \infty\}$ be the set of finite-order elements. The identity has order 1, so it's in F. Any element has the same order as its inverse, so $a \in F \implies o(a) < \infty \implies o(a^{-1}) < \infty \implies a^{-1} \in F$.
Finally, let's check closure. Suppose $a, b \in F$ and suppose $o(a) = k$ and $o(b) = m$. Then $(ab)^{km} = a^{km}b^{km}$ by commutativity, and this equals $(a^k)^m(b^m)^k = e^m e^k = e$. This means that $o(ab) \leq km < \infty$, so $ab \in F$. And we're done!

3.2.18 Let $G = (\mathbb{Q}, +)$ and suppose H, K are subgroups of G. Prove that if $H, K \neq \{0\}$, then $H \cap K \neq \{0\}$.

Well, by hypothesis, each of H and K contains some nonzero rational number. And since H, K contain inverses, if they contain any number they contain its negative as well, so each contains some positive rational number. So we can consider some $a/b \in H$ and $p/q \in K$, where a, b, p, q are positive integers, without loss of generality. By closure under addition, the sum of a/b with itself any number of times is also in H, so add it to itself b times, concluding that $a \in H$. Likewise $p \in K$. But then add a to itself p times to find that $pa \in H$, and add p to itself a times to find that $pa \in K$. So both groups contain the nonzero integer pa. □

3.2.20 Compute the centralizer in $GL_2(\mathbb{R})$ of the matrix $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$.

Recall that the *centralizer* of g is the set of all elements commuting with g. Let's take a matrix $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$; we'll suppose this commutes with $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ and see what this tells us about A.

$$\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} a & a+b \\ c & c+d \end{smallmatrix}\right] \; ; \qquad \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] = \left[\begin{smallmatrix} a+c & b+d \\ c & d \end{smallmatrix}\right].$$

Setting upper left corners equal, we have $a = a + c$, so $c = 0$. This also makes the lower right corners equal. From the upper right, we get $a + b = b + d$, which means $a = d$. So the centralizer is all matrices of the form $\left[\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right]$; that is, diagonal matrices.

3.2.23 Let G be a cyclic group, and let a, b be elements s.t. neither $a = x^2$ nor $b = x^2$ has a solution in G. Show that $ab = x^2$ does have a solution in G.

We know that G is cyclic, so let's suppose $G = \langle g \rangle$. Then a and b are powers of g, so say $a = g^\alpha$ and $b = g^\beta$. We know that the exponents α and β are odd, because for instance if $a = g^{2k}$, then $x = g^k$ would be a solution to $x^2 = a$. But then $ab = g^{\alpha+\beta}$ has an even exponent, which means that $x = g^{(\alpha+\beta)/2}$ is a solution to $x^2 = ab$.

3.2.26 For $a, b \in G$, assume that $o(a)$ and $o(b)$ are relatively prime and that $ab = ba$. Show that $o(ab) = o(a)o(b)$.

Let $k = o(a)$ and $m = o(b)$. We saw above that $o(ab) \leq o(a)o(b)$, just because the commutativity ensures that $(ab)^{km} = e$. What remains to show is that $o(ab) \geq o(a)o(b)$; that is, if $(ab)^\ell = e$, we must show that $\ell \geq km$.
So, begin with $(ab)^\ell = e$ for some positive ℓ, which means that $a^\ell b^\ell = e$ by commutativity. Thus $a^\ell = b^{-\ell}$. Since these things are equal, they of course have the same order, and since the order of an element is equal to the order of its inverse, it follows that $o(a^\ell) = o(b^\ell)$.
However, recall that for any g, we have that $o(g) = |\langle g \rangle|$ and that $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$. Clearly the powers of a^ℓ are a subset of the powers of a, so $\langle a^\ell \rangle$ is a subgroup of $\langle a \rangle$, and by Lagrange's theorem (the order of a subgroup divides the order of the group), this means that $o(a^\ell)$ divides $o(a)$ and likewise $o(b^\ell)$ divides $o(b)$. But $o(a^\ell) = o(b^\ell)$, so if the same integer divides both k and m, which are relatively prime, we conclude that $o(a^\ell) = o(b^\ell) = 1$. That means $a^\ell = b^\ell = e$. But then ℓ is a multiple of k and a multiple of m, and since they are relatively prime, it is thus a multiple of km. We have successfully proved that $\ell \geq km$.

3.3.4 Find the cyclic subgroup generated by $\left[\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right]$ in $GL_2(\mathbb{Z}_3)$.

Let $M = \left[\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right]$. Then $M^2 = \left[\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right]\left[\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$, and $M^3 = \left[\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right]$.
We note that M^3 is $-I$, so we can see that $M^6 = I$.
That means that $M^4 = -M = \left[\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right]$, and $M^5 = -M^2 = \left[\begin{smallmatrix} 2 & 2 \\ 0 & 2 \end{smallmatrix}\right]$.
So $\langle M \rangle = \{I, M, M^2, M^3, M^4, M^5\}$, where the matrix values are listed above.

3.3.6 Construct an abelian group of order 12 that is not cyclic.

The easiest answer is $G = \mathbb{Z}_6 \times \mathbb{Z}_2$. Elements of $\mathbb{Z}_6$ have order $1, 2, 3, 6$ and elements of $\mathbb{Z}^2$ have order 1,2. By Proposition 3.3.4, the order of an element of G is the lcm of the orders of the individual elements of the factor groups, so the largest possible order in G is 6. Since $|G| = 12$ but it has no element of order 12, it is not cyclic.

3.3.9 Consider subsets of $\mathbb{Z} \times \mathbb{Z}$. Let C_1 be the "diagonal subset" consisting of pairs (a, a). For $n \geq 2$, let C_n be the subset consisting of pairs (a, b) for which $a \equiv b \pmod{n}$. Show that each of these is a subgroup, and show that any PROPER subgroup of $\mathbb{Z} \times \mathbb{Z}$ which contains C_1 has the form C_n for some integer n.

One way to say what it means to be in C_n is that the two coordinates must differ by a multiple of n. Now suppose H is some subgroup of $\mathbb{Z} \times \mathbb{Z}$ containing C_1. Then let n be the smallest difference between a and b for any $(a, b) \in H$. I claim that if $n \geq 2$, then $H = C_n$ for this value n; if $n = 1$, then $H = \mathbb{Z} \times \mathbb{Z}$ itself; and finally it is clear that if there is never any difference between the coordinates, then $H = C_1$.
Consider the case $n = 1$. Then there is some $(a, a + 1) \in H$, so by closure we have $(a, a+1) - (a, a) = (0, 1) \in H$, and thus all its powers, which means $(0, m) \in H$ for all $m \in \mathbb{Z}$. But then for any $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, we have $(a, b) = (a, a) + (0, b - a) \in H$, showing that $H = \mathbb{Z} \times \mathbb{Z}$.
Now suppose $n > 1$. Then there is some $(a, a + n) \in H$, which means $(0, n) \in H$, but we don't have $(0, 1), \cdots, (0, n - 1)$ or n would not be the smallest difference of coordinates. Since $(0, n) \in H$, we have $(0, kn) \in H$ for all $k \in \mathbb{Z}$, and therefore $(a, a + kn) \in H$ for all $a \in \mathbb{Z}, k \in \mathbb{Z}$. This is all of C_n, so we've shown that $C_n \subseteq H$.
We're trying to show $C_n = H$, so suppose not; then there is some (a, b) in H which is not in C_n. Thus $n \not| \, b - a$, and so $b - a = kn + r$ for some remainder $0 < r < n - 1$.
But we have

$$(a, b) - (a, a) - (0, kn) = (a, a + kn + r) - (a, a) - (0, kn) = (0, r) \in H,$$

and this contradicts the minimality of n. This shows that $H = C_n$, as needed.

3.3.10 Consider the subset X of $S_n \times S_n$ consisting of pairs (σ, τ) for which $\sigma(1) = \tau(1)$. Show X is not a subgroup.

In fact, this subset neither has inverses nor is closed under multiplication. Let's see that with an example. Consider $\sigma = (123)$ and $\tau = (124)$, both elements of S_4. Let $g = (\sigma, \tau)$. This is an element of X because $\sigma(1) = \tau(1) = 2$. However, $g^2 = (\sigma^2, \tau^2) = \big(\ (132),\ (142)\ \big)$, and this is not in X because 1 is mapped to 3 by the first coordinate permutation and to 4 by the second. (In fact, in this example, $g^{-1} = g^2$, so this shows the failure of inverses and closure at the same time.)

EC: 3.2.2 Let $A = \left[\begin{smallmatrix} 1 & -1 \\ -1 & 0 \end{smallmatrix}\right] \in GL_2(\mathbb{R})$. Show that A has infinite order by proving that $A^n = \left[\begin{smallmatrix} F_{n+1} & -F_n \\ -F_n & F_{n-1} \end{smallmatrix}\right]$.

This problem isn't hard but it uses proof by induction; that's why it's extra credit!
Recall that the Fibonacci sequence starts out $F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2$, and continues by the recursive rule $F_{n+1} = F_n + F_{n-1}$.
Base case $(n = 1)$: $A^1 = \left[\begin{smallmatrix} F_2 & -F_1 \\ -F_1 & F_0 \end{smallmatrix}\right]$ ✓
Inductive hypothesis: Assume $A^{n-1} = \left[\begin{smallmatrix} F_n & -F_{n-1} \\ -F_{n-1} & F_{n-2} \end{smallmatrix}\right]$.
Inductive step: Consider A^n. It is equal to

$$A \cdot A^{n-1} = \left[\begin{smallmatrix} 1 & -1 \\ -1 & 0 \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} F_n & -F_{n-1} \\ -F_{n-1} & F_{n-2} \end{smallmatrix}\right] = \left[\begin{smallmatrix} F_n + F_{n-1} & -(F_{n-1} + F_{n-2}) \\ -F_n & F_{n-1} \end{smallmatrix}\right] = \left[\begin{smallmatrix} F_{n+1} & -F_n \\ -F_n & F_{n-1} \end{smallmatrix}\right] \quad ✓$$

Since the F_n are increasing, no power of A can ever equal I.