Math 113 Homework 2
Solutions

(1) Do excercise 2.2 in Judson.

(a) *Note that $a \circ a = a = a \circ d$. If this were a group, then by left cancelation, we would get $a = d$. But a and d are different. So this is not a group.*
(b) *Here a is an identity, and each element is it's own inverse. You can check associativity by running through all the cases. You can skip the cases involving a since it's the identity.*
(c) *Again a is the identity. c and a are their own inverses and b and d are inverses of each other. Associativity is tedious like in (b).*
(d) *Note that $a \circ d = d = b \circ d$. If this were a group, by right cancelation, we would get $a = b$. So this is not a group.*

(2) Let $(J, \bullet)$ and $(K, \star)$ be groups. We can define a binary operation on $J \times K$, $\spadesuit : (J \times K) \times (J \times K) \to J \times K$ as

$$(j_1, k_1) \spadesuit (j_2, k_2) = (j_1 \bullet j_2, k_1 \star k_2)$$

Prove that $(J \times K, \spadesuit)$ is a group. This group is called the *direct product* of $(J, \bullet)$ and $(K, \star)$.

$J \times K$ is associative:

$$\begin{aligned}(j_1, k_1) \spadesuit ((j_2, k_2) \spadesuit (j_3, k_3)) &= (j_1, k_1) \spadesuit (j_2 \bullet j_3, k_2 \star k_3) = (j_1 \bullet j_2 \bullet j_3, k_1 \star k_2 \star k_3) \\ &= (j_1 \bullet j_2, k_1 \star k_2) \spadesuit (j_3, k_3) = ((j_1, k_1) \spadesuit (j_2, k_2)) \spadesuit (j_3, k_3)\end{aligned}$$

$J \times K$ had identity (e_J, e_K):

$$(j, k) \spadesuit (e_J, e_K) = (j \bullet e_J, k \star e_K) = (j, k) = (e_J \bullet j, e_K \star k) = (e_J, e_K) \spadesuit (j, k)$$

And $(j, k) \in J \times K$ has inverse (j^{-1_J}, k^{-1_K}):

$$(j, k) \spadesuit \left(j^{-1_J}, k^{-1_K}\right) = \left(j \bullet j^{-1_J}, k \star k^{-1_K}\right) = (e_J, e_K) = \left(j^{-1_J} \bullet j, k^{-1_K} \star k\right) = \left(j^{-1_J}, k^{-1_K}\right) \spadesuit (j, k)$$

(3) Do excercise 2.24 in Judson.

First, we will prove this for $n \geq 0$ by induction:
Base Case ($n = 0$): $ab^0a^{-1} = aea^{-1} = aa^{-1} = e = (aba^{-1})^0$.
Inductive step: Assume that $ab^na^{-1} = (aba^{-1})^n$. Now

$$ab^{n+1}a^{-1} = ab^nba^{-1} = ab^neba^{-1} = ab^na^{-1}aba^{-1} = \left(aba^{-1}\right)^n \left(aba^{-1}\right) = \left(aba^{-1}\right)^{n+1}$$

So the induction holds.
Checking for $n < 0$ (so $-n > 0$), we get:

$$ab^na^{-1} = a\left(b^{-1}\right)^{-n} a^{-1} = \left(ab^{-1}a^{-1}\right)^{-n} = \left(\left(ab^{-1}a^{-1}\right)^{-1}\right)^n = \left(\left(a^{-1}\right)^{-1} \left(b^{-1}\right)^{-1} a^{-1}\right)^n = \left(aba^{-1}\right)^n$$

(4) Do excercise 2.34 in Judson.

There are eight symmetries of the square (called D_4): the identity i; four reflections across lines, $\mu_{|}$, μ_{-}, $\mu_{/}$, and $\mu_{\backslash}$; and three rotations $\rho_{90^\circ CW}$, ρ_{180°, and $\rho_{90^\circ CCW}$.

We need to notice a few things. If we compose two perpendicular reflections, we get ρ_{180°. Similarly, if we compose ρ_{180° and a reflection, we get the perpendicular reflection. If we compose two reflections which are not perpendicular, we get $\rho_{90^\circ CW}$ or $\rho_{90^\circ CCW}$. Either $\rho_{90^\circ CW}$ or $\rho_{90^\circ CW}$ generates all the rotations. If you have all rotations and some reflection, you can make all the other reflections. This means any subgroup containing two nonperpendicular reflections, or any reflection and $\rho_{90^\circ CW}$ or $\rho_{90^\circ CCW}$, must be the whole group.

So the possible subgroups are:

- *The trivial subgroup, $\{i\}$, and the whole group, D_4.*
- *Subgroups with i and one reflection, $\left\{i, \mu_{|}\right\}$, $\{i, \mu_{-}\}$, $\left\{i, \mu_{/}\right\}$, and $\left\{i, \mu_{\backslash}\right\}$.*
- *The subgroup $\{i, \rho_{180^\circ}\}$.*
- *The subgroup of all rotations, $\{i, \rho_{90^\circ CW}, \rho_{180^\circ}, \rho_{90^\circ CCW}\}$*
- *The subgroups consisting of the identity, two perpendicular reflections, and the 180° degree rotation: $\left\{i, \mu_{|}, \mu_{-}, \rho_{180^\circ}\right\}$ and $\left\{i, \mu_{/}, \mu_{\backslash}, \rho_{180^\circ}\right\}$.*

So there are a total of eleven subgroups of D_4.

(5) If G is a group, H_1 and H_2 are both subgroups of G, and $H_1 \cup H_2 = G$, prove that $H_1 = G$ or $H_2 = G$.

Suppose that neither H_1 or H_2 was all of G. Then pick some $a \in G \setminus H_1$ and $b \in G \setminus H_2$. Since $G = H_1 \cup H_2$, we know $a \in H_2$ and $b \in H_1$. This means that also $a^{-1} \in H_2$ and $b^{-1} \in H_1$.

Consider ab: ab cannot be in H_1, because then $a = (ab)b^{-1}$ would be in H_1. Similarly ab cannot be in H_2 because then $b = a^{-1}(ab)$ would be in H_2. But then $ab \notin H_1 \cup H_2$, which contradicts that $H_1 \cup H_2 = G$.

So it must be that either H_1 or H_2 is G.

(6) Do excercise 2.46 in Judson.

We will check that $Z(G)$ is a subgroup by meeting the conditions in Proposition 2.9. First, by definition of the identity e, $ge = g = eg$ for all $g \in G$, so $e \in Z(g)$. Now suppose $h_1, h_2 \in Z(G)$, and let g be any element of G. Then $gh_1h_2 = h_1gh_2 = gh_1h_2$, so $h_1h_2 \in Z(G)$. Finally, if h is in $Z(G)$, then for any $g \in G$,

$$gh^{-1} = gh^{-1}e = gh^{-1}g^{-1}g = g(gh)^{-1}g = g(hg)^{-1}g = gg^{-1}h^{-1}g = eh^{-1}g = h^{-1}g$$

So $Z(G)$ meets all the conditions required to be a subgroup of G.

(7) Do excercise 2.52 in Judson.

This is false. For example, D_4 from problem (4) is not abelian. But every proper subgroup is abelian.

(8) Suppose G is a nonempty finite set and $\star : G \times G \to G$ is an associative operation on G. Furthermore, assume that $\star$ is both left and right cancellative. (I.e if $a \star b = a \star c$ then $b = c$ and if $x \star y = z \star y$ then $x = z$.) Prove that $(G, \star)$ is a group.

G is associative by assumption. Since G is nonempty, pick some $a \in G$. Since G is finite, the sequence $a, a \star a, a \star a \star a, a \star a \star a \star a, \ldots,$ must eventually have a repetition, $a^n = a^m$ for some $0 < n < m$. We will prove a^{m-n} is an identity. For any $g \in G$, $g \star a^n = g \star a^m = (g \star a^{m-n}) \star a^n$. By right cancellation, we get $g = g \star a^{m-n}$. Similarly, we can apply left cancellation to $a^n \star g = a^m \star g = a^n \star (a^{m-n} \star g)$ to get $a^{m-n} \star g = g$.

Now, for any $b \in G$, we need to find an inverse. Since G is finite, the sequence $b, b \star b, b \star b \star b, \ldots$ must eventually have a repetition $b^k = b^\ell$ for some $0 < k < \ell$. We will prove $b^{\ell-k-1}$ is the inverse of b. (If $\ell - k - 1 = 0$, put $b^0 = e$.) Since $b \star b^{\ell-k-1} \star b^k = b^l = b^k = e \star b^k$, by right cancellation, $b \star b^{\ell-k-1} = e$. Also, $b^{\ell-k-1} \star b = b \star b^{\ell-k-1} = e$. So $b^{\ell-k-1}$ is an inverse of e, and G is a group.