Homework #3, due 9/16/09 = **1.1.1, 1.1.2, 1.1.3, 1.1.5, 1.1.6, 1.1.11, 1.1.12, 1.1.22, 1.1.25**; **1.2.2, 1.2.3, 1.2.18**; **1.3.1, 1.3.5, 1.3.7, 1.3.13, 1.3.14**; **1.4.1, 1.4.2, 1.4.3, 1.4.4**; **1.5.1**;

1.1.1(a) The operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a - b$ is NOT associative, since $(a \star b) \star c = a - b - c$ but $a \star (b \star c) = a - (b - c) = a - b + c$, hence $(a \star b) \star c \neq a \star (b \star c)$ whenever $c \neq 0$.

1.1.1(b) The operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a + b + ab$ IS associative, since

$$\begin{aligned}(a \star b) \star c &= (a + b + ab) \star c \\ &= (a + b + ab) + c + (a + b + ab)c \\ &= a + b + c + ab + ac + bc + abc \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a \star (b + c + bc) \\ &= a \star (b \star c)\end{aligned}$$

1.1.1(c) The operation $\star$ on $\mathbb{Z}$ defined by $a \star b = (a + b)/5$ is NOT associative, since

$$(a \star b) \star c = ((a + b)/5) \star c = \frac{1}{5}(\frac{1}{5}(a + b) + c) = \frac{1}{25}a + \frac{1}{25}b + \frac{1}{5}c$$

but

$$a \star (b \star c) = a \star ((b + c)/5) = \frac{1}{5}(a + \frac{1}{5}(b + c)) = \frac{1}{5}a + \frac{1}{25}b + \frac{1}{25}c$$

hence $(a \star b) \star c \neq a \star (b \star c)$ whenever $a \neq c$.

1.1.1(d) The operation $\star$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \star (c, d) = (ad + bc, bd)$ IS associative. The definition of $\star$ is just a notationally altered form of multiplication of fractions, since

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ad + bc}{bd}.$$

Multiplication of fractions is associative, so $\star$ is associative.

1.1.1(e) The operation $\star$ defined on $\mathbb{Q} - \{0\}$ by $a \star b = \frac{a}{b}$ is NOT associative, since $(a \star b) \star c = \frac{a}{b} \star c = \frac{a}{bc}$ but $a \star (b \star c) = a \star \frac{b}{c} = \frac{ac}{b}$, hence $(a \star b) \star c \neq a \star (b \star c)$ whenever $c^2 \neq 1$.

1.1.2(a) The operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a - b$ is NOT commutative, since $a \star b = a - b$ but $b \star a = b - a$.

1.1.2(b) The operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a + b + ab$ IS commutative, since

$$b \star a = b + a + ba = a + b + ab = a \star b$$

by the commutativity of ordinary addition and multiplication.

1.1.2(c) The operation $\star$ on $\mathbb{Z}$ defined by $a \star b = (a + b)/5$ IS commutative, since $a \star b = (a + b)/5 = (b + a)/5 = b \star a$ by the commutativity of ordinary addition.

1.1.2(d) The operation $\star$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \star (c, d) = (ad + bc, bd)$ IS commutative, since $(a, b) \star (c, d) = (ad + bc, bd) = (cb + da, db) = (c, d) \star (a, b)$ by the commutativity of ordinary addition and multiplication.

1.1.2(e) The operation $\star$ defined on $\mathbb{Q}$ by $a \star b = \frac{a}{b}$ is NOT commutative, since $a \star b = \frac{a}{b}$ but $b \star a = \frac{b}{a}$.

1.1.3 Addition of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is defined by $\overline{a} + \overline{b} = \overline{a+b}$ for all $a, b \in \mathbb{Z}$, where $\overline{a} = \{a + nk : k \in \mathbb{Z}\}$ for all $a \in \mathbb{Z}$. Then, by the associativity of ordinary addition on $\mathbb{Z}$,

$$\begin{aligned}(\overline{a} + \overline{b}) + \overline{c} &= \overline{a+b} + \overline{c} \\ &= \overline{(a+b)+c} \\ &= \overline{a+(b+c)} \\ &= \overline{a} + \overline{b+c} \\ &= \overline{a} + (\overline{b} + \overline{c})\end{aligned}$$

1.1.5 Multiplication of residue classes in $\mathbb{Z}/n\mathbb{Z}$ cannot be the operation of a group because cancellation fails: $\overline{0} \cdot \overline{1} = \overline{0} \cdot \overline{0}$ but $\overline{1} \neq \overline{0}$.

1.1.6 Determine which of the following sets are groups under addition.

1.1.6(a) The set of rational numbers in lowest terms whose denominators are odd: This set contains 0 (since $0 = \frac{0}{1}$) and is clearly closed under $-$. So it forms a group if is closed under addition. If we add two fractions with odd denominators we get another fraction with an odd denominator because

$$\frac{a}{2n+1} + \frac{b}{2m+1} = \frac{2am + a + 2bn + b}{4nm + 2n + 2m + 1}$$

In reducing this fraction to lowest terms we cancel common factors from the numerator and denominator. The denominator $4nm + 2n + 2m + 1$ is odd, hence is not divisible by 2, and cancelling factors from it cannot add a factor of 2, so even after reduction to lowest terms the denominator is still not divisible by 2, hence is still odd. So these numbers DO form a group.

1.1.6(b) The set of rational numbers in lowest terms whose denominators are even: As in part (a) we only need to check closure, but this fails since, for example,

$$\frac{1}{2} + \frac{1}{2} = \frac{1}{1}$$

1.1.6(c) The set of rational numbers of absolute value < 1: This set is not closed under addition. E.g. $4/5$ is in this set, but the sum $4/5 + 4/5 = 8/5$ is not. Hence this set does NOT form a group under addition.

1.1.6(d) The set of rational numbers of absolute value ≥ 1 together with 0: This set does NOT form a group under addition because it is not closed. For example, $5/2$ is in this set, and so is -2, but their sum $5/2 + (-2) = 1/2$ is not in this set.

1.1.6(e) The set of rational numbers with denominators equal to 1 or 2: This set is the union of $\mathbb{Z}$ with $\{n/2 : n \in \mathbb{Z}\}$. This set is closed under addition and forms a group isomorphic to $\mathbb{Z}$ under addition. (The isomorphism is either doubling of halving, depending on which way it goes.)

1.1.6(f) The set of rational numbers with denominators equal to 1, 2, or 3: This set cannot form a group because it is not closed under addition. For example, $1/2 + 1/3 = 5/6$ and $5/6$ is not a fraction with denominator 1, 2, or 3.

1.1.11 The orders of the elements in the additive group $\mathbb{Z}/12\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{11}\}$ are as follows:

$x =$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$\lvert x\rvert =$	1	12	6	4	3	12	2	12	3	4	6	12

1.1.12 Compute the orders of $\overline{1}$, $\overline{-1}$, $\overline{5}$, $\overline{7}$, $\overline{-7}$, $\overline{13}$ in the multiplicative group $(\mathbb{Z}/12\mathbb{Z})^\times$. First note that

$$(\mathbb{Z}/12\mathbb{Z})^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$$

$\overline{1}$ is the identity element of this group and has order 1. $\overline{-1} = \overline{11}$ and the order of $\overline{11}$ is 2 because $\overline{11}^2 = \overline{121} = \overline{1}$. $\overline{5}^2 = \overline{25} = \overline{1}$, so $\overline{5}$ has order 2. $\overline{7}^2 = \overline{49} = \overline{4 \cdot 12 + 1} = \overline{1}$, so $\overline{7}$ has order 2. $\overline{-7} = \overline{5}$ has order 2, as computed above. Finally $\overline{13} = \overline{1}$, so $\overline{13}$ has order 1.

1.1.22 If x and g are elements of the group G prove that $|x| = |gxg^{-1}|$. Deduce that $|ab| = |ba|$ for all $a, b \in G$. First note that

$$\begin{aligned}
(gxg^{-1})^n &= \overbrace{(gxg^{-1})(gxg^{-1})(gxg^{-1})\cdots(gxg^{-1})}^{n} \\
&= gx\overbrace{(g^{-1}g)x(g^{-1}g)x\cdots(g^{-1}g)x}^{n-1}g^{-1} \\
&= gx\overbrace{1x1x1\cdots1x}^{n-1}g^{-1} \\
&= g\overbrace{xxx\cdots x}^{n}g^{-1} \\
&= gx^ng^{-1}
\end{aligned}$$

If $x^n = 1$ then $(gxg^{-1})^n = gx^ng^{-1} = g1g^{-1} = gg^{-1} = 1$. Conversely, if $(gxg^{-1})^n = 1$ then $1 = gx^ng^{-1}$, hence

$$1 = g^{-1}g = g^{-1}1g = g^{-1}(gx^ng^{-1})g = (g^{-1}g)x^n(g^{-1}g) = 1x^n1 = x^n.$$

Thus $x^n = 1$ iff $gx^ng^{-1} = 1$, so the orders of x and gxg^{-1} must be the same, i.e., $|x| = |gxg^{-1}|$. Apply this with $x = ab$ and $g = b$ to get $|ab| = |x| = |gxg^{-1}| = |b(ab)b^{-1}| = |ba(bb^{-1})| = |ba|$.

1.1.25 Prove that is $x^2 = 1$ for every x in a group G then G is abelian.

Let $a, b \in G$. Then

$$\begin{aligned}
ab &= a1b \\
&= a(ab)^2b && \text{by hypothesis } x^2 = 1 \\
&= a(ab)(ab)b \\
&= (aa)(ba)(bb) \\
&= a^2(ba)b^2 \\
&= 1(ba)1 && \text{by hypothesis } x^2 = 1 \\
&= ba
\end{aligned}$$

1.2.2 Use generators and relations to show that if an element x of D_{2n} that is not a power of r then $rx = xr^{-1}$.

It was shown in the text that $D_{2n} = \{1, r, r^2, \cdots, r^{n-1}, s, sr, sr^2, \cdots, sr^{n-1}\}$. Since x is not a power of r it cannot be in $\{1, r, r^2, \cdots, r^{n-1}\}$ and must therefore be in $\{s, sr, sr^2, \cdots, sr^{n-1}\}$, say $x = sr^i$ for some $i \in \{0, \cdots, n-1\}$. Then, using laws of exponents and the relation $rs = sr^{-1}$, we have

$$rx = rsr^i = sr^{-1}r^i = sr^{i-1} = (sr^i)r^{-1} = xr^{-1}$$

1.2.3 Use generators and relations to show that if an element x of D_{2n} that is not a power of r then $|x| = 2$. Deduce that D_{2n} is generated by s and sr, both of which have order 2.

By our assumption that x is not a power of r we know (as in the previous problem) that there is some $i \in \{0, \cdots, n-1\}$ such that $x = sr^i$. Then

$$x^2 = (sr^i)^2 = (sr^i)(sr^i) = s(r^i s)r^i = s(sr^{-i})r^i = (ss)(r^{-i}r^i) = s^2 r^{-i+i} = 1r^0 = 1$$

Now neither s nor sr are powers of r, hence they both have order 2. Furthermore, s and sr generate D_{2n} because they generate two other elements that are already known to generate D_{2n}, namely s itself and $r = s(sr)$.

1.2.18 Let $Y = \langle u, v | u^4 = v^3 = 1, uv = v^2u^2 \rangle$. Then $1 = v$ because

$$\begin{aligned}
1 &= u^4 && u^4 = 1 \\
&= u^2 1 u^2 \\
&= u^2 v^3 u^2 && v^3 = 1 \\
&= u(uv)v^2u^2 \\
&= u(v^2u^2)v^2u^2 && uv = v^2u^2 \\
&= (uv)vu^2v^2u^2 \\
&= (v^2u^2)vu^2v^2u^2 && uv = v^2u^2 \\
&= v^2u(uv)u^2v^2u^2 \\
&= v^2u(v^2u^2)u^2v^2u^2 && uv = v^2u^2 \\
&= v^2uv^2(u^4)v^2u^2 \\
&= v^2uv^2v^2u^2 && u^4 = 1 \\
&= v^2uvv^3u^2 \\
&= v^2(uv)u^2 && v^3 = 1 \\
&= v^2(v^2u^2)u^2 && uv = v^2u^2 \\
&= vv^3u^4 \\
&= v && v^3 = u^4 = 1
\end{aligned}$$

From $1 = v$ and $uv = v^2u^2$ we get $u = u1 = 1^2u^2 = u^2$, so by cancellation we also have $u = 1$. Thus $u = v = 1$, and since Y is generated by u and v it follows that $Y = \{1\}$. All the other relations between u and v that are stated in parts (a)–(e) are trivial consequences of $u = v = 1$.

1.3.1 Let σ be the permutation $1 \mapsto 3$, $2 \mapsto 4$, $3 \mapsto 5$, $4 \mapsto 2$, $5 \mapsto 1$, and let τ be the permutation $1 \mapsto 5$, $2 \mapsto 3$, $3 \mapsto 2$, $4 \mapsto 4$, $5 \mapsto 1$. Find the cycle decompositions of the following permutations: σ, τ, σ^2, $\sigma\tau$, $\tau\sigma$, and $\tau^2\sigma$.

$$\begin{aligned}
\sigma &= (135)(24) \\
\tau &= (15)(23) \\
\sigma^2 &= ((135)(24))^2 = (135)^2(24)^2 = (153) \\
\sigma\tau &= (135)(24)(15)(23) = (2534) \\
\tau\sigma &= (135)(24)(15)(23) = (2534) \\
\tau^2\sigma &= ((15)(23))^2\sigma = \sigma = (135)(24)
\end{aligned}$$

1.3.5 Find the order of $\sigma = (1, 12, 8, 10, 4)(2, 13)(5, 11, 7)(6, 9)$. Notice that σ is given as the product of disjoint cycles of sizes 5, 2, 3, and 2. The order of σ is the least common multiple of these numbers, so $|\sigma| = 30$.

1.3.7 Write out the cycle decomposition of each element of order 2 in S_4.

The six transpositions all have order 2. They are (12), (13), (14), (23), (24), and (34). Products of pairs of disjoint 2-cycles also have order 2. They are (12)(34), (13)(24), and (14)(23). All the other elements of S_4 have the form of either a 3-cycle, which has order 3, or a 4-cycle, which has order 4.

1.3.13 Show that an element σ in S_n has order 2 iff the cycle decomposition of σ is a product of commuting 2-cycles.

Assume σ has order 2. Then $\sigma^2 = 1$, so for every $i \in \{1, \ldots, n-1\}$, we have $\sigma(\sigma(i)) = i$, so the cycle decomposition of σ has the 2-cycle $(i, \sigma(i))$ or $(\sigma(i), i)$ in it.

If the cycle decomposition of σ contains another such 2-cycle $(j, \sigma(j))$ then $(i, \sigma(i))$ and $(j, \sigma(j))$ must be disjoint. To see this, note that if $i = j$ then $\sigma(i) = \sigma(j)$ and the two cycles are the same, contrary to assumption, if $i = \sigma(j)$ then $\sigma(i) = \sigma(\sigma(j) = j$, and again the two cycles are the same, contrary to assumption. Thus $i \notin \{j, \sigma(j)\}$. Similarly, if $\sigma(j) \in \{i, \sigma(i)\}$ then either $\sigma(j) = i$, hence $j = \sigma(\sigma(j)) = \sigma(i)$ and the two 2-cycles are the same, or else $\sigma(j) = \sigma(i)$, which implies $i = j$ and again the two 2-cycles are the same, contrary to assumption.

Conversely, the product of disjoint 2-cycles has order 2. Each 2-cycle clearly has order 2, and the fact that disjoint cycles commute implies that the square of a product of disjoint 2-cycles is the product of the squares of the 2-cycles, all of which are 1, so the square of a product of 2-cycles is 1. Hence the order of a product of disjoint 2-cycles is 2.

1.3.14 Let p be a prime. Let σ be in S_n. Show that σ has order p if and only if σ is the product of disjoint p-cycles. Show by explicit example that this may not be the case if p is not prime.

Suppose σ is the product of disjoint p-cycles. The pth power of σ is the product of the pth powers of all the cycles in σ, since disjoint cycles commute. The pth powers of the p-cycles in σ are all 1, so their product is 1. Thus $\sigma^p = 1$. A p-cycle has order p, so no smaller power of σ can be 1, hence $|\sigma| = p$.

Suppose the order of σ is p. Since $|\sigma|$ is the least common multiple of the sizes of the disjoint cycles in the cycle decomposition of σ, all of these cycles must have sizes that divide p, either 1 or p. Sincew 1-cycles are omitted from the notation for

the cycle decomposition of σ, the cycle decomposition consists entirely of p-cycles. Thus σ is the product of disjoint commuting p-cycles.

For an example showing these conclusions may fail when p is not prime, let $p = 6$ and $\sigma = (12)(345)$. The order of σ is the least common multiple of 2 and 3, hence $|\sigma| = 6$, but σ is not the product of commuting 6-cycles.

1.4.1 Prove $|GL_2(\mathbb{F}_2)| = 6$. **1.4.2** Write out all the elements of $|GL_2(\mathbb{F}_2)|$ and compute their orders. **1.4.3** Show that $|GL_2(\mathbb{F}_2)|$ is not abelian.

We do all three problems together. First we just enumerate the 2×2 matrices of elements of $\mathbb{F}_2$ (0 or 1) that have non-zero determinant. There are $4^2 = 16$ matrices altogether, and the ones that have determinant equal to 0 are $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$, and $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. The remaining matrices, which have non-zero determinant, are $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. There are six such matrices, so $|GL_2(\mathbb{F}_2)| = 6$. The identity matrix is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, which has order 1. $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ have order 3. $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ have order 2.

1.4.4 Prove that if n is not a prime then $\mathbb{Z}/n\mathbb{Z}$ is not a field.

Since n is not prime there are $a, b \in \mathbb{Z}$ such that $1 < a < n$, $1 < b < n$, and $n = ab$. Then $\overline{0} = \overline{n} = \overline{ab} = \overline{a}\overline{b}$. But a field cannot have two non-zero elements whose product is zero. Thus $\mathbb{Z}/n\mathbb{Z}$ is not a field.

1.5.1 Compute the orders of the elements of the quaternion group Q_8.

The order of 1 is 1. The order of -1 is 2 since $(-1)(-1) = 1$. The order of i is 4 since $i^4 = i^2 i^2 = (-1)(-1) = 1$ but $i^3 = -i \neq 1$ and $i^2 = -1 \neq 1$. Similarly, the order of j is 4 and the order of k is also 4. The order of the inverse of an element of a group is the same as the order of the element, so $-i$, $-j$, and $-k$ have order 4. Thus Q_8 has one element of order 1, one of order 2, and six of order 4.