Kris Harper
MATH 25700
Homework 2 October 9, 2009

Problem 1 (0.3.6)**.** *Prove that the squares of the elements in $\mathbb{Z}/4\mathbb{Z}$ are just $\overline{0}$ and $\overline{1}$.*

Proof. We have

$$\begin{aligned}\overline{0}^2 &= \overline{0}\overline{0} = \overline{0\cdot 0} = \overline{0}\\ \overline{1}^2 &= \overline{1}\overline{1} = \overline{1\cdot 1} = \overline{1}\\ \overline{2}^2 &= \overline{2}\overline{2} = \overline{2\cdot 2} = \overline{4} = \overline{0}\\ \overline{3}^2 &= \overline{3}\overline{3} = \overline{3\cdot 3} = \overline{9} = \overline{1}.\end{aligned}$$

□

Problem 2 (0.3.12)**.** *Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$ with $1 \le a \le n$. Prove if a and n are not relatively prime, there exists an integer b with $1 \le b < n$ such that $ab \equiv 0 \pmod{n}$ and deduce that there cannot be an integer c such that $ac \equiv 1 \pmod{n}$.*

Proof. Since $(a, n) \neq 1$ we know there exists $d \neq 1$ such that $d \mid a$ and $d \mid n$. Thus there exist positive integers c and b such that $a = cd$ and $n = bd$. But then $cn = ab$. Since $1 < d$ we know that $b < n$ Thus $n \mid ab - 0$ so $ab \equiv 0 \pmod{n}$. Suppose there exists some other integer c such that $ac \equiv 1 \pmod{n}$. Then since $1 \le b < n$ we have $abc \equiv b \pmod{n}$. But this is impossible since we already know $ab \equiv 0 \pmod{n}$. Thus there exists no such integer c. □

Problem 3 (0.3.13)**.** *Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$ with $1 \le a \le n$. Prove if a and n are relatively prime, there exists an integer c such that $ac \equiv n \pmod{n}$.*

Proof. From the Euclidean algorithm we know we can express $(a, n) = 1 = ac + nm$ for integers x and y. Thus $n(-m) = ac - 1$ and $n \mid (ac - 1)$. Therefore $ac \equiv 1 \pmod{n}$. □

Problem 4 (0.3.14)**.** *Conclude from the previous two exercises that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of elements $\overline{a}$ of $\mathbb{Z}/n\mathbb{Z}$ with $(a, n) = 1$ and hence prove Proposition 4. Verify this directly in the case $n = 12$.*

Proof. By definition

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{there exists } \overline{c} \in \mathbb{Z}/n\mathbb{Z} \text{ with } \overline{ac} = \overline{1}\}.$$

Let $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ such that $(a, n) = 1$. Then we know from Problem 2 that there exists $c \in C$ such that $ac \equiv 1 \pmod{n}$ and so $n \mid (ac - 1)$. Therefore $\overline{1} = \overline{ac} = \overline{ac}$ and thus $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. On the other hand, let $\overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then there exists $\overline{c} \in \mathbb{Z}/n\mathbb{Z}$ such that $\overline{b}\overline{c} = \overline{1}$. But then $\overline{bc} = \overline{1}$ so $n \mid (bc - 1)$. Thus $bc \equiv 1 \pmod{n}$. But from Problem 1 we conclude that $(b, n) = 1$. Thus, the two sets are equal as both inclusions have been shown. □

Problem 5 (0.3.15)**.** *For each of the following pairs of integers a and n, show that a is relatively prime to n and determine the multiplicative inverse of $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$.*
(a) $a = 13$, $n = 20$.

Proof. Using the Euclidean algorithm:

$$20 = 13 + 713 = 7 + 67 = 6 + 16 = 6$$

So $(a, n) = 1$. Working backwards we have

$$1 = (2)20 + (-3)13.$$

Thus $\overline{13}^{-1} = \overline{-3} = \overline{17}$. □

Kris Harper
MATH 25700
Homework 2 October 9, 2009

Problem 6 (1.1.1)**.** *Determine which of the following operations are associative:*
(a) The operation $\star$ *on* $\mathbb{Z}$ *defined by* $a \star b = a - b$.
(d) The operation $\star$ *on* $\mathbb{Z} \times \mathbb{Z}$ *defined by* $(a, b) \star (c, d) = (ad + bc, bd)$.
(e) The operation $\star$ *on* $\mathbb{Q}\backslash\{0\}$ *defined by* $a \star b = \frac{a}{b}$.

Proof. (a) Here $\star$ is not associative. As a counterexample take $3, 4, 5 \in \mathbb{Z}$. Then $3 - (4 - 5) = 3 - (-1) = 4$ but $(3 - 4) - 5 = (-1) - 5 = -6$.

(d) This simply addition in $\mathbb{Q}$. Take $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in \mathbb{Z} \times \mathbb{Z}$. We have

$$\begin{aligned}(a_1, b_1) \star ((a_2, b_2) \star (a_3, b_3)) &= (a_1, b_1) \star (a_2b_3 + b_2a_3, b_2b_3)\\ &= (a_1b_2b_3 + b_1(a_2b_3 + b_2a_3), b_1b_2b_3)\\ &= (a_1b_2b_3 + b_1a_2b_3 + b_1b_2a_3, b_1b_2b_3)\\ &= (b_3(a_1b_2 + b_1a_2) + b_1b_2a_3, b_1b_2b_3)\\ &= (a_1b_2 + b_1a_2, b_1b_2) \star (a_3, b_3)\\ &= ((a_1, b_1) \star (a_2, b_2)) \star (a_3, b_3).\end{aligned}$$

(e) This is not associative. Take $1/2, 1/3, 1/6 \in \mathbb{Q}$. Then

$$\left(\frac{1}{2} \star \frac{1}{3}\right) \star \frac{1}{6} = \frac{3}{2} \star \frac{1}{6} = 9.$$

But

$$\frac{1}{2} \star \left(\frac{1}{3} \star \frac{1}{6}\right) = \frac{1}{2} \star 2 = \frac{1}{4}.$$

□

Problem 7 (1.1.2)**.** *Determine which of the binary operations in the preceding exercise are commutative.*

Proof. (a) This is not commutative. Take $1, 0 \in \mathbb{Z}$. Then $1 \star 0 = 1 - 0 = 1$ but $0 \star 1 = 0 - 1 = -1$.

(d) This is commutative as addition in $\mathbb{Q}$ is commutative. Let $(a_1, b_1), (a_2, b_2) \in \mathbb{Z} \times \mathbb{Z}$. Then

$$(a_1, b_1) \star (a_2, b_2) = (a_1b_2 + b_1a_2, b_1b_2) = (a_2b_1 + b_2a_1, b_2b_1) = (a_2, b_2) \star (a_1, b_1).$$

(e) This is not commutative. Take 1 and 2. Then $1 \star 2 = 1/2$ but $2 \star 1 = 2/1$. □

Problem 8 (1.1.6)**.** *Determine which of the following sets are groups under addition:*
(a) The set of rational numbers (including $0 = 0/1$*) in lowest terms whose denominators are odd.*
(b) The set of rational numbers in lowest terms whose denominators are even together with 0.
(c) The est of rational numbers of absolute value < 1.
(d) The set of rational numbers of absolute value ≥ 1 *together with* 0.
(e) The set of rational numbers with denominators equal to 1 *or* 2.
(f) The set of rational numbers with denominators equal to 1, 2 *or* 3.

Proof. (a) This is a group under addition. Since $\mathbb{Q}$ is already a group under addition, we just need to show that this set is a subgroup. Take a/b and c/d with b and d odd. Then $a/b + c/d = (ad + bc)/bd$. Since b and d are both odd, bd is odd. If $ad + bc$ happens to contain a factor of b or d, then reducing the fraction still results in a fraction with odd denominator since odd numbers have no even factors. We know $0 = 0/1$ is in the group. And note that inverses are in the group as well since $(a/b)^{-1} = -a/b$ which has odd denominator.

(b) This is not closed under addition. Consider $1/6 + 1/6 = 2/6 = 1/3$.

(c) This is not closed under addition. Consider $2/3 + 2/3 = 4/3$ and $|4/3| \geq 1$.

(d) This is not closed under addition. Consider $1 + -1/2 = 1/2$ and $|1/2| < 1$.

(e) This is a group under addition. Again, we must show that this is a subgroup. Take a/b and c/d with b and d equal to 1 or 2. Then $a/b + c/d = (ad + bc)/bd$. In the case that $b = 1$ or $d = 1$ we see that the sum of a/b and c/d still has denominator 1 or 2. In the case that $b = d = 2$, note that we can undistribute 2 from the numerator, resulting in a denominator of either 1 or 2. Of course $0 = 0/1$ is in the group and inverses are as well since $(a/b)^{-1} = -a/b$.

(f) This is not closed under addition. Consider $1/2 + 1/3 = 5/6$. □

Problem 9 (1.1.9)**.** *Let* $G = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$.
(a) Prove that G *is a group under addition.*
(b) Prove that the nonzero elements of G *are a group under multiplication.*

Proof. (a) Let $a + b\sqrt{2}$ and $c + d\sqrt{2}$ be two elements of G. Then using commutativity, associativity and distributivity of the reals we have

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}.$$

Since $\mathbb{Q}$ is closed under addition this expression is also in G. Thus G is closed under addition. We use 0 for the identity of G. To find $(a + b\sqrt{2})^{-1}$ take $(-a - b\sqrt{2})$ so that

$$(a + b\sqrt{2}) + (-a - b\sqrt{2}) = (a - a) + (b - b)\sqrt{2} = 0 + 0 = 0.$$

Associativity follows from the associativity of the reals.

(b) Let $a + b\sqrt{2}$ and $c + d\sqrt{2}$ be two elements of G. Then using commutativity, associativity and distributivity of the reals we have

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2}.$$

Thus G is closed under multiplication. We use 1 for the identity element of G. To find $(a + b\sqrt{2})^{-1}$ take

$$(a + b\sqrt{2})^{-1} = \frac{-a}{2b^2 - a^2} + \frac{b}{2b^2 - a^2}\sqrt{2}.$$

It's clear that when these are multiplied as above we obtain $1 + 0\sqrt{2} = 1$. Once again, associativity follows from that of the reals. □

Problem 10 (1.1.10)**.** *Prove that a finite group is abelian if and only if it's group table is a symmetric matrix.*

Proof. Let G be a group and let M be its group table. Suppose that G is abelian. The ij element of M is $g_i g_j$. Since G is abelian, $g_i g_j = g_j g_i$. But this is the ji element of M. Thus M is symmetric. Conversely, suppose M is symmetric. Then $M_{ij} = M_{ji}$ for all i and j. But $g_i g_j = M_{ij} = M_{ji} = g_j g_i$. Thus G must be abelian. □

Problem 11 (1.1.11)**.** *Find the orders of each element of the additive group* $\mathbb{Z}/12\mathbb{Z}$*.*

$|\overline{0}| = 1$, $|\overline{1}| = 12$, $|\overline{2}| = 6$, $|\overline{3}| = 4$, $|\overline{4}| = 3$, $|\overline{5}| = 12$, $|\overline{6}| = 2$, $|\overline{7}| = 12$, $|\overline{8}| = 3$, $|\overline{9}| = 4$, $|\overline{10}| = 5$, $|\overline{11}| = 12$.

Problem 12 (1.1.13)**.** *Find the orders of the following elements of the additive group* $\mathbb{Z}/36\mathbb{Z}$*:* $\overline{1}$, $\overline{2}$, $\overline{6}$, $\overline{9}$, $\overline{10}$, $\overline{12}$, $\overline{-1}$, $\overline{-10}$, $\overline{-18}$.

$|\overline{1}| = 36$, $|\overline{2}| = 18$, $|\overline{6}| = 6$, $|\overline{9}| = 4$, $|\overline{10}| = 18$, $|\overline{12}| = 3$, $|\overline{-1}| = 36$, $|\overline{-10}| = 18$, $|\overline{-18}| = 2$.

Problem 13 (1.1.16)**.** *Let* x *be an element of* G*. Prove that* $x^2 = 1$ *if an only if* $|x|$ *is either* 1 *or* 2*.*

Proof. Suppose that $x^2 = 1$. Note that $|x|$ cannot be greater than 2, because order is defined to be the least positive integer n such that $x^n = 1$. If $|x| = n$ then n can be no larger than 2. But also, if $|x| = 1$ then $x = 1$ so $x^2 = 1^2 = 1$. Thus $|x|$ is either 1 or 2. Conversely, suppose $|x|$ is either 1 or 2. We've already seen that if $|x| = 1$ then $x^2 = 1$. If $|x| = 2$ then by definition $x^2 = 1$. □

Problem 14 (1.1.17). *Let x be an element of G. Prove that if $|x| = n$ for some positive integer n then $x^{-1} = x^{n-1}$.*

Proof. Since $|x| = n$ we have $x^n = 1$. We can write this as $1 = x\cdot x\cdot\cdots\cdot x$ where there are n xs being multiplied. Now multiply both sides on the right by x^{-1}. We then have $x^{-1} = x\cdot x\cdot\cdots\cdot x\cdot x^{-1} = x\cdot x\cdot\cdots\cdot x = x^{n-1}$. □

Problem 15 (1.1.18). *Let x and y be elements of G. Prove that $xy = yx$ if and only if $y^{-1}xy = x$ if and only if $x^{-1}y^{-1}xy = 1$.*

Proof. Suppose $xy = yx$. Multiplying both sides on the left by y^{-1} gives $y^{-1}xy = y^{-1}yx = 1\cdot x = x$. Now suppose $y^{-1}xy = x$. Multiplying both sides on the left again by x^{-1} gives $x^{-1}y^{-1}xy = x^{-1}x = 1$. Finally assume $x^{-1}y^{-1}xy = x^{-1}x = 1$. Multiply both sides on the left by yx to get $yx = yxx^{-1}y^{-1}xy = yy^{-1}xy = xy$. □

Problem 16 (1.1.19). *Let $x \in G$ and let $a, b \in \mathbb{Z}^+$.*
(a) Prove that $x^{a+b} = x^a x^b$ and $(x^a)^b = x^{ab}$.
(b) Prove that $(x^a)^{-1} = x^{-a}$.
(c) Establish part (a) for arbitrary integers a and b (positive, negative or zero).

Proof. (a) By definition we have $x^{a+b} = x\cdot x\cdot\cdots\cdot x$ where there are $a+b$ xs being multiplied. By the generalized associative law, this is independent of bracketing, so group the first a xs. This is now $x^a\cdot x\cdot x\cdot\cdots\cdot x$ where there are now b xs being multiplied. But then this is just $x^a x^b$.

For the second part, fix $a \in \mathbb{Z}^+$. Note that for $b = 1$ we have $(x^a)^1 = x^a = x^{a\cdot 1}$. Assume the statement holds for some $b \in \mathbb{Z}^+$. Consider $(x^a)^{b+1}$. From above we know this is $(x^a)^b(x^a)$. Inductively this is $(x^{ab})x^a$ and from above again this is $x^{ab+a} = x^{a(b+1)}$. By induction, the statement holds.

(b) Consider the product $x^a x^{-a}$. Note that for $a = 1$ we have $xx^{-1} = 1$. Thus $(x^1)^{-1} = x^{-1}$. Now suppose the statement holds for some $a \in \mathbb{Z}^+$. Consider $x^{a+1}x^{-(a+1)}$. By definition this is $x\cdot x\cdot\cdots\cdot x\cdot x^{-1}\cdot x^{-1}\cdot\cdots\cdot x^{-1}$ where there are $a+1$ xs and $a+1$ x^{-1}s. Ignoring the first and last terms, we see that the remaining product is simply $x^a x^{-a}$ which we inductively know is 1. Thus, the product simplifies to $xx^{-1} = 1$. Therefore $x^{a+1}x^{-(a+1)} = 1$. The statement is thus proved by induction.

(c) First assume a and b are both negative. Note that $-(a+b)$ is positive. Then

$$x^{b+a} = \left(x^{-(a+b)}\right)^{-1} = \left(x^{(-a)+(-b)}\right)^{-1} = \left(x^{-a}x^{-b}\right)^{-1} = \left(x^{-b}\right)^{-1}\left(x^{-a}\right)^{-1} = x^b x^a.$$

Commuting $a+b$ reverses the final order. To show the product rule we need the fact that $(x^{-1})^a = x^{-a}$ for positive a. To see this note that $(x^{-1})^a$ is simply x^{-1} product a times. But this is exactly x^{-a}. Now for $a < 0$ and $b < 0$ we have

$$(x^a)^b = \left(\left(\left(x^{-a}\right)^{-1}\right)^{-b}\right)^{-1} = \left(\left(x^{-a}\right)^b\right)^{-1} = (x^{-a})^{-b} = x^{(-a)(-b)} = x^{ab}.$$

In the case that $a = 0$ we have $x^{0+b} = x^b = 1\cdot x^b = x^0 x^b$. Also $(x^0)^b = 1^b = 1 = x^0 = x^{0\cdot b}$. A similar argument holds for $b = 0$. Now suppose that $a < 0$, $b > 0$ and $a+b > 0$. From part (b) we know that $x^a x^{-a} = x^{-a}x^a = 1$. Then we have

$$x^{b+a} = x^{b+a}(x^{-a}x^a) = x^{b+a-a}x^a = x^b x^a.$$

On the other hand, if $a+b<0$ then we have

$$\left(x^{b+a}\right)^{-1} = x^{-(a+b)} = x^{(-a)+(-b)}(x^bx^{-b}) = x^{(-a)+(-b)+b}x^{-b} = x^{-a}x^{-b} = (x^a)^{-1}\left(x^b\right)^{-1} = \left(x^bx^a\right)^{-1}.$$

Multiplying by x^{b+a} on the left and x^bx^a on the right gives the result. A similar argument holds for $a>0$ and $b<0$.

For the second part of (a) assume first that $a<0$ and $b>0$. Then we have

$$(x^a)^b = \left(\left(x^{-a}\right)^{-1}\right)^b = \left(\left(x^{-1}\right)^{-a}\right)^b = \left(x^{-1}\right)^{-ab} = x^{ab}.$$

Finally, if $a>0$ and $b<0$ then we have

$$(x^a)^b = \left((x^a)^{-b}\right)^{-1} = \left(x^{-ab}\right)^{-1} = x^{ab}.$$

□

Problem 17 (1.1.20)**.** *For x an element in G show that x and x^{-1} have the same order.*

Proof. Let $|x|=n$. Then $x^n=1$. Multiply both sides by x^{-n} to obtain $(x^{-1})^n = x^{-n} = x^nx^{-n} = x^{n-n} = 1$. Thus $|x^{-1}| \leq n$. Suppose that $|x-1| = m < n$. Then $(x^{-1})^m = 1$. This is $x^{-m}=1$. Multiplying both sides by x^m gives a contradiction since n is the least positive integer for which $x^n=1$. This also shows that if x has infinite order but x^{-1} has finite order, we arrive a contradiction. Thus $|x| = |x^{-1}|$. □

Problem 18 (1.1.22)**.** *If x and g are elements of the group G, prove that $|x| = |g^{-1}xg|$. Deduce that $|ab| = |ba|$ for all $a,b \in G$.*

Proof. Let $|x|=n$. Then $x^n=1$. Now multiply on the left by g^{-n} and on the right by g^n. We have

$$(g^{-1}xg)^n = (g^{-1})^nx^ng^n = g^{-n}x^ng^n = g^{-n}g^n = g^{n-n} = 1.$$

Thus $|g^{-1}xg| \leq n$. Suppose that $|g^{-1}xg| = m < n$. Then we have $g^{-m}x^mg^m = 1$. Multiplying by g^m on the left and g^{-m} on the right gives the same contradiction as above. Once again, if $|x|$ is infinite, this shows that $|g^{-1}xg|$ cannot be finite. Therefore $|x| = |g^{-1}xg|$. If $|ab|=n$ then $a^nb^n=1$ and so $1 = b^{-n}a^{-n} = ((ba)^{-1})^n$. But we know that elements and their inverses have the same order. If ab has infinite order then a similar argument as above will produce a contradiction if ba doesn't have infinite order. Thus $|ab|=|ba|$. □

Problem 19 (1.1.24)**.** *If a and b are* commuting *elements of G, prove that $(ab)^n = a^nb^n$ for all $n \in \mathbb{Z}$.*

Proof. We know that $(ab)^0 = 1 = a^0b^0$. Now suppose that $(ab)^na = a^{n+1}b^n$ for some $n \in \mathbb{Z}_0^+$. Using Problem 16 and the commutativity of a and b we have

$$(ab)^{n+1}a = (ab)^n(ab)a = (a^nb^n)(ab)a = (a^{n+1}b^n)(b)a = a^{n+1}(b^{n+1})a = a^{n+1}b^{n+1}a.$$

After canceling a, the statement then holds for all nonnegative n by induction. Now consider $n \in \mathbb{Z}^+$. We have

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

□

Problem 20 (1.1.25)**.** *Prove that if $x^2=1$ for all $x \in G$ then G is abelian.*

Proof. Let $x,y \in G$. We have $x^2y^2 = (xy)^2 = 1$. Multiply on the left by x^{-1} and on the right by y^{-1} to get $xy = x^{-1}y^{-1} = (yx)^{-1}$. But note that since $(yx)^2=1$ we can multiply by $(yx)^{-1}$ to get $yx = (yx)^{-1}$. Thus $xy=yx$. □

Kris Harper
MATH 25700
Homework 2 October 9, 2009

Problem 21 (1.1.26)**.** *Assume H is a nonempty subset of $(G, \star)$ which is closed under the binary operation on G and is closed under inverses, i.e., for all h and $k \in H$, hk and $h^{-1} \in H$. Prove that H is a group under the operation $\star$ restricted to H.*

Proof. Take $i, j, k \in H$. Then we have $i \star (j \star k) = (i \star j) \star k$ since these are also elements of G where the associativity law holds. Note that every element in H has an inverse by assumption, and the operation $\star$ is closed by assumption. We need only show that H has an identity element e. But $e \in H$ since $h^{-1} \in H$ for all $h \in H$ and we know $hh^{-1} = e$. This e is thus the same identity as for G and so it works as an identity for $\star$ for all of H. □

Problem 22 (1.1.28)**.** *Let $(A, \star)$ and $(B, \diamond)$ be groups and let $A \times B$ be their direct product. Verifty all the group axioms for $A \times B$:*
(a) Prove that the associative law holds: For all $(a_i, b_i) \in A \times B$, $i = 1, 2, 3$ $(a_1, b_1)[(a_2, b_2)(a_3, b_3)] = [(a_1, b_1)(a_2, b_2)](a_3, b_3)$.
(b) Prove that $(1, 1)$ is the identity of $A \times B$.
(c) Prove that the inverse of (a, b) is (a^{-1}, b^{-1}).

Proof. (a) We have

$$\begin{aligned}
(a_1, b_1)[(a_2, b_2)(a_3, b_3)] &= (a_1, b_1)(a_2 \star a_3, b_2 \diamond b_3) \\
&= (a_1 \star (a_2 \star a_3), b_1 \diamond (b_2 \diamond b_3)) \\
&= ((a_1 \star a_2) \star a_3, (b_1 \diamond b_2) \diamond b_3) \\
&= (a_1 \star a_2, b_1 \diamond b_2)(a_3, b_3) \\
&= ((a_1, b_1)(a_2, b_2))(a_3, b_3).
\end{aligned}$$

(b) We have $(a, b)(1, 1) = (a \star 1, b \diamond 1) = (a, b)$.
(c) We have $(a, b)(a^{-1}, b^{-1}) = (a \star a^{-1}, b \diamond b^{-1}) = (1, 1)$. □

Problem 23 (1.1.29)**.** *Prove that $A \times B$ is an abelian group if and only if A and B are abelian.*

Proof. Suppose that $A \times B$ abelian. Then

$$(a_1 \star a_2, b_1 \diamond b_2) = (a_1, b_1)(a_2, b_2) = (a_2, b_2)(a_1, b_1) = (a_2 \star a_1, b_2, \diamond b_1).$$

Equating components we have $a_1 \star a_2 = a_2 \star a_1$ and $b_1 \diamond b_2 = b_2 \diamond b_1$. Conversely, to show A and B abelian implies $A \times B$ is abelian, we reverse the equalities. That is

$$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2) = (a_2 \star a_1, b_2, \diamond b_1) = (a_2, b_2)(a_1, b_1).$$

This shows $A \times B$ is abelian. □

Problem 24 (1.1.30)**.** *Prove that the elements $(a, 1)$ and $(1, b)$ of $A \times B$ commute and deduce that the order of (a, b) is the least common multiple of $|a|$ and $|b|$.*

Proof. We have $(a, 1)(1, b) = (a \star 1, 1 \diamond b) = (1 \star a, b \diamond 1) = (1, b)(a, 1)$. Note that $(a, 1)(1, b) = (a, b)$. From Problem 19 we know $(a, b)^n = ((a, 1)(1, b))^n = (a, 1)^n (1, b)^n$. Thus $|(a, b)$ must be the least common multiple of $(a, 1)$ and $(1, b)$ as this is the smallest positive integer n for which both $(a, 1)^n = 1$ and $(1, b)^n = 1$. □

Problem 25 (1.2.4)**.** *If $n = 2k$ is even and $n \geq 4$ show that $z = r^k$ is an element of order 2 which commutes with all elements of D_{2n}. Show also that z is the only nonidentity element of D_{2n} which commutes with all elements of D_{2n}.*

Proof. To show that $|z| = 2$ we note that $r^i \neq r^j$ for all $i \neq j$ provided $0 \leq i < n$ and $0 \leq j < n$. Also, we know $r^0 = 1$ so $|r^k| \neq 1$. But $(r^k)^2 = r^2k = r^n = 1$ from Problem 16 and so $|z| = 2$. Note this also implies that $z^{-1} = z$ since $z^2 = 1$ and so $z^{-1}z^2 = z = 1 \cdot z^{-1} = z^{-1}$. To see that z commutes with every element of D_{2n} note that $zr^i = r^k r^i = r^{k+i} = r^{i+k} = r^i r^k = r^i z$. Likewise, $zs = r^k s = sr^{-k} = sr^k = sz$. All powers of s are either s or 1 so, we've shown that z commutes with all powers of r and of s. Now we take $zr^i s = zr^i(z^{-1}z)s = (zr^i)z^{-1}(zs) = (r^i z)z^{-1}(sz) = r^i(zz^{-1}sz = r^i sz$. Therefore z commutes with all elements of D_{2n}. Now take r^i such that $r^i \neq r^k$ and $r^i \neq 1$. Then $r^i s = sr^{-i}$. For r^i to be commutative, we need $r^i = r^{-i}$, which would also imply $r^{2i} = (r^i)^2 = 1$. But we know this isn't the case since $i \nmid n$ by assumption. This shows that s and any power of r besides powers of z are not commutative. Finally, we consider sr^i. This element doesn't commute with r since $sr^i r = sr^{i+1} = r^{-i-1}s \neq rsr^i$. □

Problem 26 (1.2.8)**.** *Find the order of the cyclic subgroup of D_{2n} generated by r.*

Proof. We know that $|r| = n$. Furthermore, we know that $1, r, r^2, \dots, r^{n-1}$ are all distinct. Finally, note that $(r^i)^{-1} = r^{n-i}$ as shown in Problem 14. These facts together show that $|\langle r \rangle| = n$.

Problem 27 (1.3.4)**.** *Compute the order of each of the elements in the following groups:*
(a) S_3.
(b) S_4.

(a) $|(1)| = 1$, $|(12)| = 2$, $|(23)| = 2$, $|(13)| = 2$, $|(123)| = 3$, $|(132)| = 3$.

(b) $|(1)| = 1$, $|(12)| = 2$, $|(13)| = 2$, $|(14)| = 2$, $|(23)| = 2$, $|(24)| = 2$, $|(34)| = 2$, $|(123)| = 3$, $|(132)| = 3$, $|(124)| = 3$, $|(142)| = 3$, $|(134)| = 3$, $|(143)| = 3$, $|(234)| = 3$, $|(243)| = 3$, $|(12)(34)| = 2$, $|(13)(24)| = 2$, $|(14)(23)| = 2$, $|(1234)| = 2$, $|(1243)| = 2$, $|(1324)| = 4$, $|(1342)| = 4$, $|(1423)| = 4$, $|(1432)| = 4$.

Problem 28 (1.3.10)**.** *Prove that if σ is the m-cycle $(a_1 a_2 \dots a_m)$, then for all $i \in \{1, 2, \dots, m\}$, $\sigma^i(a_k) = a_{k+i}$, where $k + i$ is replaced by its least positive residue mod m. Deduce that $|\sigma| = m$.*

Proof. Note that for $i = 1$ we have $\sigma(a_k) = a_{k+1}$ by definition of a cycle. Suppose the statement is true for some $i \in \mathbb{Z}^+$. Consider $\sigma^{i+1}(a_k) = \sigma^i(\sigma(a_k)) = \sigma^i(a_{k+1}) = a_{k+i+1}$. Thus, the statement is true for all positive i, in particular $i \in \{1, 2, \dots, m\}$. Putting in $i = m$ we have $\sigma^m(a_k) = a_{k+m} = a_k$. Since m is the smallest positive integer for which this holds, we see that $|\sigma| = m$. □

Problem 29 (1.3.11)**.** *Let σ be the m-cycle $(12 \dots m)$. Show that σ^i is also an m-cycle if and only if i is relatively prime to m.*

Proof. Suppose that $(i, m) \neq 1$. Then there exists $d < m$ such that $i = jd$ and $m = nd$. This implies $jm = in$. This means that σ^i will have cycles of length n. To see this, note that by Problem 28 the first cycle in σ_i will be $(1\ 1 + i\ 1 + 2i \dots 1 + n(i - 1))$. The next cycle will continue in the same fashion. Since $n \mid ni$ we know $1 + ni \equiv 1 \pmod m$ and so the cycle must end with $1 + n(i - 1)$. But since $n < m$ because $d > 1$, we know this is not an m-cycle.

Conversely, suppose that $(i, m) = 1$. Again from Problem 28 we know σ^i starts with $(1\ 1 + i\ 1 + 2i \dots 1 + n(i - 1))$ where n is the smallest positive integer such that $1 + ni \equiv 1 \pmod m$. Since $(i, m) = 1$ we know that $n = m$ and so this cycle is an m-cycle. □

Problem 30 (1.3.14)**.** *Let p be a prime. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p-cycles. Show by an explicit example that this need be the case if p is not prime.*

Proof. Suppose that $\sigma \in S_n$ has order p. Then $\sigma^p = 1$. If we write $\sigma = (a_1 \dots a_{m_1}) \dots (a_{m_{k-1}+1} \dots a_{m_k})$ then since all these cycles are disjoint we have

$$1 = \sigma^p = ((a_1, \dots a_{m_1}) \dots (a_{m_{k-1}+1} \dots a_{m_k}))^p = (a_1 \dots a_{m_1})^p \dots (a_{m_{k-1}+1} \dots a_{m_k})^p.$$

But since each of these terms are disjoint, each one must evaluate to the identity. Since p is prime, p cannot be the product of any of the lengths of the cycles. Thus, each must be a p-cycle. Conversely, suppose that σ is a product of commuting p-cycles. Then $\sigma = (a_1 \dots a_{m_1}) \dots (a_{m_{k-1}+1} \dots a_{m_k})$. Raising this to the pth power by Problem 19 we have

$$\sigma^p = ((a_1 \dots a_{m_1}) \dots (a_{m_{k-1}+1} \dots a_{m_k}))^p = (a_1 \dots a_{m_1})^p \dots (a_{m_{k-1}+1} \dots a_{m_k})^p = 1.$$

Since each cycle is a p-cycle we know no smaller integer would produce the same result. Thus $|\sigma| = p$.

As an example, let $p = 6$ and take the cycle $\sigma = (1\ 2\ 3)(4\ 5)$. We can see $|\sigma| = 6$, but this isn't a decomposition of 6-cycles. □

Problem 31 (1.3.15)**.** *Prove that the order of an element in S_n equals the least common multiple of the cycles in its cycle decomposition.*

Proof. A cycle decomposition of an element in S_n is a product of disjoint cycles. Since the cycles are disjoint, they commute with each other. Let $\sigma = (a_1 \dots a_{m_1}) \dots (a_{m_{k-1}+1} \dots a_{m_k})$ be an element of S_n. We know that each term in the decomposition has order m_i, that is, the order is equal to the number of elements in the cycle. This follows from Problem 28. Let n be the least common multiple of all the m_i. Then by Problem 19 we know

$$\sigma^n = (a_1 \dots a_{m_1})^n \dots (a_{m_{k-1}+1} \dots a_{m_k})^n = ((a_1 \dots a_{m_1}) \dots (a_{m_{k-1}+1} \dots a_{m_k}))^n = 1.$$

Since n is the least integer with this property, we know $|\sigma| = n$. □

Problem 32 (1.5.1)**.** *Compute the order of each of the elements in Q_8.*

$|1| = 1$, $|-1| = 2$, $|i| = 4$, $|-i| = 4$, $|j| = 4$, $|-j| = 4$, $|k| = 4$, $|-k| = 4$.

Problem 33 (1.6.1)**.** *Let $\phi : G \to H$ be a homomorphism.*
(a) Prove that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$.
(b) Do part (a) for $n = -1$ and deduce that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$.

Proof. (a) For $n = 1$ we're done. Suppose the statement holds for some $n \in \mathbb{N}$. Then using Problem 16 we have

$$\varphi(x^{n+1}) = \varphi(x^n x) = \varphi(x^n)\varphi(x) = \varphi(x)^n \varphi(x) = \varphi(x)^{n+1}.$$

(b) We have $\varphi(e) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$. Since inverses are preserved and inverses are unique, we must have $\varphi(x^{-1}) = \varphi(x)^{-1}$. Now if $n < 0$ we again use Problem 16 to obtain

$$\varphi(x^n) = \varphi((x^{-n})^{-1}) = \varphi(x^{-n})^{-1} = (\varphi(x)^{-n})^{-1} = \varphi(x)^{-n}.$$

□

Problem 34 (1.6.3)**.** *If $\varphi : G \to H$ is an isomorphism, prove that G is abelian if and only if H is abelian. If $\varphi : G \to H$ is a homomorphism, what additional conditions on ϕ (if any) are sufficient to ensure that if G is abelian, the so is H?*

Proof. Suppose that G is abelian. For $u, v \in H$, since φ is surjective, there exists $x, y \in G$ such that $\varphi(x) = u$ and $\varphi(v) = y$. Then

$$uv = \varphi(x)\varphi(y) = \varphi(xy) = \varphi(yx) = \varphi(y)\varphi(x) = vu.$$

Conversely, supposing H is abelian, for $x, y \in G$ there exists elements $u, v \in H$ such that $\varphi^{-1}(u) = x$ and $\varphi^{-1}(v) = y$. Then

$$xy = \varphi^{-1}(u)\varphi^{-1}(v) = \varphi^{-1}(v)\varphi^{-1}(u) = yx.$$

If $\varphi : G \to H$ is a homomorphism, with G abelian, then provided φ is surjective, H will be abelian as well. The reason for this can be seen in the first part of the above proof. □

Problem 35 (1.6.9)**.** *Prove that D_{24} and S_4 are not isomorphic.*

As we saw in Problem 33, an isomorphism will preserve powers between elements of groups, which in particular means that if two groups are isomorphic, each group must have the same number of elements of a specific order. We know that in D_{24}, $|r| = 24$. But as Problem 27 showed, there is no such element in S_4. Thus, the two groups are not isomorphic. □

Problem 36 (1.6.13)**.** *Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Prove that the image of φ, $\varphi(G)$, is a subgroup of H. Prove that if ϕ is injective then $G \cong \phi(G)$.*

Proof. We know φ preserves the identity of G so $1_H \in \varphi(G)$. Take $x, y \in \varphi(G)$. Then there exists $u, v \in G$ such that $\varphi(u) = x$ and $\varphi(v) = y$. Then $\varphi(uv) = \varphi(u)\varphi(v) = xy$ and so $xy \in \varphi(G)$. Also note that from Problem 33 $\varphi(u^{-1}) = \varphi(u)^{-1} = x^{-1}$. Thus $\varphi(G)$ is closed under multiplication and inverses and so it's a subgroup of H. Assume now that ϕ is injective. We must show that $\varphi : G \to \varphi(G)$ is surjective. But this is clearly true since $y \in \varphi(G)$ only if there exists $x \in G$ such that $\varphi(x) = y$. Thus $\varphi : G \to \varphi(G)$ is a bijection and a homomorphism and so $G \cong \varphi(G)$. □

Problem 37 (1.6.14)**.** *Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Define the* kernel *of φ to be $\{g \in G \mid \varphi(g) = 1_H\}$. Prove that the kernel of φ is a subgroup of G. Prove that φ is injective if and only if the kernel of φ is the identity subgroup of G.*

Proof. We know that $e \in \ker\varphi$. Let $x, y \in \ker\varphi$. Then $\varphi(x) = 1_H = \varphi(y)$ and so $\varphi(xy) = \varphi(x)\varphi(y) = 1_H$. Also from Problem 33 we know $\varphi(x^{-1}) = \varphi(x)^{-1} = 1_H^{-1} = 1_H$. Thus $\ker\varphi$ is closed under multiplication and inverses, so it's a subgroup of G.

Assume that φ is injective. Then for all $x, y \in \ker\varphi$ with $x \neq y$ we have $\varphi(x) \neq \varphi(y)$. But this limits $|\ker\varphi| = 1$ and since $1_G \in \ker\varphi$, it must be the identity subgroup of G. Conversely, suppose that $\ker\varphi$ is the identity subgroup of G. Suppose we have $\varphi(x) = \varphi(y)$ for $x, y \in G$. Then $1_H = \varphi(x)(\varphi(y))^{-1} = \varphi(x)\varphi(y^{-1}) = \varphi(xy^{-1})$. Since identities are preserved, $xy^{-1} = 1_G$ and so $x = y$. Therefore φ is injective. □

Problem 38 (1.6.16)**.** *Let A and B be groups and let G be their direct product, $A \times B$. Prove that the maps $\pi_1 : G \to A$ and $\pi_2 : G \to B$ defined by $\pi((a, b)) = a$ and $\pi_2((a, b)) = b$ are homomorphisms and find their kernels.*

Proof. Let $(a, b), (c, d) \in G$. We have

$$\pi_1((a, b)(c, d)) = \pi_1((ac, bd)) = ac = \pi_1((a, b))\pi((c, d)).$$

A similar argument holds for π_2. Consider an element $(a, b) \in G$ such that $\pi_1(a, b) = 1$. This means $a = 1$. On the other hand, consider $\pi_1(1, b) = 1$. Therefore $\ker\pi_1 = \{(a, b) \mid a = 1\}$ and $\ker\pi_2 = \{(a, b) \mid b = 1\}$ by a similar proof. □

Problem 39 (1.6.17)**.** *Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.*

Proof. Suppose that $\varphi : G \to G$ such that $\varphi(g) = g^{-1}$ is a homomorphism. Then for $x, y \in G$ we have

$$yx = (y^{-1})^{-1}(x^{-1})^{-1} = (x^{-1}y^{-1})^{-1} = \varphi(x^{-1}y^{-1}) = \varphi(x^{-1})\varphi(y^{-1}) = xy.$$

Conversely, suppose that G is abelian. Then we have

$$\varphi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \varphi(x)\varphi(y).$$

□

Kris Harper
MATH 25700

Homework 2 October 9, 2009

Problem 40 (1.7.4)**.** *Let G be a group acting on a set A and fix some $a \in A$. Show that the following sets are subgroups of G:*
(a) The kernel of the action.
(b) $\{g \in G \mid ga = a\}$ — this subgroup is called the stabilizer *of a in G.*

Proof. (a) Let $b \in A$. We see that the identity element e of G is in the kernel of the action because $1.b = b$ by definition. Let x and y be in the kernel. Then $y.b = b$ so $x(y.b) = x.b$. But $x.b = b$ and thus $(xy).b = b$. Therefore xy is in the kernel. Also since $x.b = b$ we can multiply by x^{-1} to obtain $b = 1.b = (x^{-1}x).b = x^{-1}(x.b) = x^{-1}.b$. Thus the kernel is closed under the action and inverses so it's a subgroup of G.

(b) This proof is exactly the same as for part (a). □

Problem 41 (1.7.6)**.** *Prove that a group G acts faithfully on a set A if and only if the kernel of the action is the set consisting only of the identity.*

Proof. Suppose G acts faithfully on A. Take x, y in the kernel such that $x \neq y$. Then we know $x.a \neq y.a$ for all $a \in A$. But this limits the size of the kernel to 1 and we know the identity is in the kernel. Conversely, suppose the kernel is just the identity. Then take $\varphi(x) = \sigma_x$ and $\varphi(y) = \sigma_y$ in S_A such that $\sigma_x = \sigma_y$. Then

$$\sigma_1 = \varphi(x)\varphi(y)^{-1} = \varphi(x)\varphi(y^{-1}) = \varphi(xy^{-1}).$$

Since identities are preserved in homomorphisms we have $xy^{-1} = 1$ and $x = y$. Therefore two permutations which are the same always arise from the same elements of G and the action is faithful. □

Problem 42 (1.7.13)**.** *Find the kernel of the left regular action.*

Proof. This is the set of all $x \in G$ such that $xy = y$ for all $y \in G$. Multiplying by y^{-1} on the right gives $x = 1$. Thus the kernel is the identity group. □

Problem 43 (1.7.14)**.** *Let G be a group and let $A = G$. Show that if G is non-abelian then the maps defined by $g.a = ag$ for all $g, a \in G$ do* not *satisfy the axioms of a (left) group action of G on itself.*

Proof. Fix $a \in G$ and take $x, y \in G$. Then we have $x.a = ax$, but $(yx).a = y.(x.a) = y.ax = yax$. Since G is non-abelian this violates the group action axioms. □

Problem 44 (1.7.16)**.** *Let G be any group and let $A = G$. Show that the maps defined by $g.a = gag^{-1}$ for all $g, a \in G$* do *satisfy the axioms of a (left) group action.*

Proof. Fix $a \in G$ and let $x, y \in G$. We have

$$x.(y.a) = x.(yay^{-1}) = x(yay^{-1})x^{-1} = xyay^{-1}x^{-1} = xya(xy)^{-1} = (xy).a.$$

Also $1.a = 1a1^{-1} = a$. □

Problem 45 (1.7.17)**.** *Let G be a group and let G act on itself by left conjugation, so each $g \in G$ maps G to G by*

$$x \mapsto gxg^{-1}.$$

For fixed $g \in G$, prove that conjugation by g is an isomorphism from G to onto itself. Deduce that x and gxg^{-1} have the same order for all $x \in G$ and that for any subset A of G, $|A| = |gAg^{-1}|$.

Proof. Problem 44 shows that conjugation is an action. This means that $\sigma_g(x) = gxg^{-1}$ is a permutation of G. But permutations are isomorphisms. The fact that $|x| = |gxg^{-1}|$ follows from Problem 33 as powers and identities are preserved through isomorphisms. If $A \subseteq G$ then conjugation maps each $a \in A$ to a distinct element gag^{-1} in gAg^{-1}. Thus $|A| = |gAg^{-1}|$. □