HOMEWORK 2: SOLUTIONS - MATH 341
INSTRUCTOR: George Voutsadakis

Problem 1 *(a) Show that $G = \mathbf{C}^* = \mathbf{C} - \{0\}$ under complex multiplication forms a group.*

(b) Construct the group table of V and Q_8 and determine whether they are Abelian.

(c) Find two elements a, b in S_3 such that $(ab)^2 \neq a^2b^2$.

Solution:

(a) We first show closure: Let $z = a + bi$ and $w = c + di$ be both in $\mathbf{C}^*$. Then we have $zw = (a + bi)(c + di) = ac - bd + (ad + bc)i$. To show that this element is in $\mathbf{C}^*$, we compute

$$\begin{aligned}(ac - bd)^2 + (ad + bc)^2 &= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= a^2(c^2 + d^2) + b^2(c^2 + d^2) \\ &= (a^2 + b^2)(c^2 + d^2).\end{aligned}$$

Now $z, w \in \mathbf{C}^*$ imply that $a^2+b^2 > 0$ and $c^2+d^2 > 0$, whence $(ac-bd)^2+(ad+bc)^2 > 0$ and $zw \in \mathbf{C}^*$.

To show associativity, let $z = a + bi, w = c + di$ and $u = e + fi$. Then

$$\begin{aligned}(zw)u &= [(a + bi)(c + di)](e + fi) \\ &= [(ac - bd) + (ad + bc)i](e + fi) \\ &= [(ac - bd)e - (ad + bc)f] + [(ac + bd)f + (ad + bc)e]i \\ &= (ace - bde - adf - bcf) + (acf - bdf + ade + bce)i \\ &= [(a(ce - df) - b(cf + de)] + [a(cf + de) + b(ce - df)]i \\ &= (a + bi)[(ce - df) + (cf + de)i] \\ &= (a + bi)[(c + di)(e + fi)] \\ &= z(wu).\end{aligned}$$

It is not difficult to check that $1 + 0i$ acts as a unit in multiplication and that $(a + bi)^{-1} = \frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i \in \mathbf{C}^*$, since $(\frac{a}{a^2+b^2})^2 + (\frac{b}{a^2+b^2})^2 = \frac{a^2+b^2}{(a^2+b^2)^2} = \frac{1}{a^2+b^2} > 0$.

Since all the group axioms hold, $\langle \mathbf{C}^*, \cdot \rangle$ is a group under multiplication.

(b) The following is the multiplication table for V, where $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, a = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, b =$

$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, c = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

The table is symmetric with respect to the first diagonal, whence V is an abelian group. For the quaternions Q_8 we have

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Observe that many pairs of elements do not commute. So the quaternions form a noncommutative group.

(c) Many elelemnts would provide examples: Take, for instance, $a = (123)$ and $b = (23)$. Then we have $((123)(23))^2 = (12)^2 = 1$, whereas $(123)^2(23)^2 = (132)1 = (132) \neq 1$. ■

Problem 2 *(a) Show that if every element of a group G is equal to its inverse, then G is Abelian.*

(b) Let G be a finite Abelian group such that for all $a \in G, a \neq e$, we have $a^2 \neq e$. If $a_1, a_2, \ldots, a_n$ are all the elements of G with no repetitions, evaluate the product $a_1 a_2 \ldots a_n$.

Solution:

(a) This is a very nice problem. Given that $a^{-1} = a$, for all $a \in G$, we need to show that $ab = ba$, for all $a, b \in G$. We have

$$\begin{aligned} ab &= a^{-1}b^{-1} \quad \text{(by hypothesis)} \\ &= (ba)^{-1} \quad \text{(since } (ba)^{-1} = a^{-1}b^{-1} \text{ in any group)} \\ &= ba \quad \text{(again by hypothesis).} \end{aligned}$$

(b) The assumption $a^2 \neq e$ implies that $a^2a^{-1} \neq ea^{-1}$ whence $a \neq a^{-1}$. Thus, each non identity element of G has an inverse different from itself. So if in the product of all

the elements in the *commutative* group G we pair each element with its inverse, the only element that will be left alone would be the identity element. In particular, this shows that the group must have an odd number of elements. We then have

$$a_1 a_2 \dots a_n = e^{\frac{n-1}{2}} \cdot e = e.$$

■

Problem 3 *(a) Show that the nonzero elements of* $\mathbf{Z}_p$*, where* p *is a prime, form a group under multiplication* mod p.

*(b) (***Wilson's Theorem***) Prove that if* p *is a prime, then* $(p-1)! \equiv -1 \bmod p$.

Solution:

(a) To show closure, we need to show that if $x, y \in \mathbf{Z}_p^*$, then $x \cdot y \in \mathbf{Z}_p^*$. We show here the contrapositive, i.e., that if $xy \equiv 0$, then $x \equiv 0$ or $y \equiv 0$. In fact, $xy \equiv 0$ means that $p \backslash xy$, whence, since p is prime, by Euclid's Lemma, we obtain $p \backslash x$ or $p \backslash y$, i.e., $x \equiv 0$ or $y \equiv 0$, as was to be shown.

Associativity is inherited from the multiplication in $\mathbf{Z}$ and 1 is the identity element. To show that inverses exist, let $x \in \mathbf{Z}_p^*$. Since p is a prime, x and p are relatively prime. Therefore, there exist integers y and k, such that $xy + pk = 1$. This implies that $xy \equiv 1$ modulo p, i.e., that $[x]^{-1} = [y]$.

(b) Suppose that p is a prime and that $a \in \mathbf{Z}_p$. Then we have $a^2 \equiv 1$ implies $a^2 - 1 \equiv 0$ whence $(a+1)(a-1) \equiv 0$. Now by part (a), $a + 1 \equiv 0$ or $a - 1 \equiv 0$, i.e., $a = 1$ or $a = -1$. This shows that in the product of all the elements in $\mathbf{Z}_p^*$ every element will be paired off with its inverse, except for 1 and -1 which are their own inverses. Hence $(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-1) = 1 \cdot (-1) = -1$ in $\mathbf{Z}_p$, i.e., $(p-1)! \equiv -1$ modulo p. ■

Problem 4 *(a) Let* $G = \{a + b\sqrt{2} : a, b \in \mathbf{Q}\}$*. Show that* G *is a subgroup of* $\mathbb{R}$ *under addition.*

(b) Let $G = \{a + bi : a, b \in \mathbb{R}, a^2 + b^2 = 1\}$*. Determine whether or not* G *is a subgroup of* $\mathbf{C}^*$ *under multiplication.*

Solution:

(a) We use one of our subgroup criteria: Suppose $a + b\sqrt{2}$ and $c + d\sqrt{2}$ are in G. Then

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

But both $a - c$ and $b - d$ are rationals since a, b, c, d are rationals, whence $(a + b\sqrt{2}) - (c + d\sqrt{2}) \in G$ and therefore $\langle G, + \rangle$ is a subgroup of $\langle \mathbb{R}, + \rangle$ by one of our subgroup criteria.

(b) We apply the same criterion here: Let $z = a + bi$ and $w = c + di$ be elements of G, i.e., $a^2 + b^2 = 1 = c^2 + d^2$. Then we have $(a+bi)(c+di)^1 = (a+bi)(\frac{c}{c^2+d^2} - \frac{d}{c^2+d^2}i) = (a + bi)(c - di) = (ac + bd) + (bc - ad)i$. We check that this is also an element of G: We have

$$\begin{aligned}(ac+bd)^2 + (bc-ad)^2 &= a^2c^2 + 2abcd + b^2d^2 + b^2c^2 - 2abcd + a^2d^2 \\ &= a^2c^2 + b^2d^2 + b^2c^2 + a^2d^2 \\ &= a^2(c^2+d^2) + b^2(c^2+d^2) \\ &= (a^2+b^2)(c^2+d^2) \\ &= 1 \cdot 1 \\ &= 1.\end{aligned}$$

Hence $zw^{-1} \in G$ and $\langle G, \cdot\rangle \leq \langle \mathbf{C}^*, \cdot\rangle$. ■

Problem 5 *(a) Show that if H and K are subgroups of G, then $H \cap K$ is also a subgroup of G.*

(b) Let G be a group, $a \in G$. Show that the centralizer $C(a) = G$ if and only if $a \in Z(G)$, the center of G.

Solution:

(a) This is also a very nice problem! Clearly, $H \subseteq G$ and $K \subseteq G$ imply $H \cap K \subseteq G$. So, by our subgroup criterion, we need to show that, if $x, y \in H \cap K$, then $xy^{-1} \in H \cap K$. Suppose that $x, y \in H \cap K$. Then $x, y \in H$ and $x, y \in K$. Since both H and K are subgroups of G, we must have, by the subgroup criterion, that $xy^{-1} \in H$ and $xy^{-1} \in K$. But then $xy^{-1} \in H \cap K$ and $H \cap K$ is a subgroup of G.

(b) We have $C(a) = G$ if and only if every element of G commutes with a if and only if $a \in Z(G)$. ■