Math 3140 — Fall 2012
Exam #1

Work alone. No materials except pen (or pencil) and paper allowed. Write your solutions on a separate paper. Justify your answers. Giving incorrect or irrelevant justification will be penalized.

Problem 1. Show that the function $\varphi : \mathbf{C}^* \to \mathbf{R}^*$ defined by

$$\varphi(z) = |z|^3$$

is a homomorphism.

Solution. We have $\varphi(zw) = |zw|^3$. But $|zw| = |z|\,|w|$ by Proposition 8 so we get

$$\varphi(zw) = |zw|^3 = \big(|z|\,|w|\big)^3 = |z|^3\,|w|^3 = \varphi(z)\varphi(w).$$

Therefore φ is a homomorphism by the definition of a homomorphism. □

Problem 2. Suppose that σ is an element of S_n that is not contained in A_n. Prove that $\mathrm{ord}(\sigma)$ is **even**.

Solution. Suppose that $\sigma^k = e$. Then $\mathrm{sgn}(\sigma)^k = \mathrm{sgn}(\sigma^k) = \sigma(e) = 1$. But if σ is not in A_n then $\mathrm{sgn}(\sigma) = -1$. Therefore $(-1)^k = 1$ so k is even. □

Solution. Here is another solution: Since σ is odd its sign is -1. We can write σ as a product of disjoint cycles σ_i. Then $\mathrm{ord}(\sigma) = \mathrm{lcm}\,\{\mathrm{ord}(\sigma_i)\}$. But remember that a cycle of odd length has sign 1 and a cycle of even length has sign -1. Therefore there must be an odd number of i-s such that the length of σ_i is even. In particular, there is at least one i such that σ_i is even. But this means that $\mathrm{lcm}\,\{\mathrm{ord}(\sigma_i)\}$ is divisible by the order of σ_i—namely its length—which is even. □

Problem 3. (a) Compute the order of $(123)(345)(567)$ in S_7.

Solution. We have $(123)(345)(567) = (1234567)$, which has order 7. □

(b) Give an element of S_7 with order 12.

Solution.

$$(123)(4567)$$

has order 12 because $((123)(4567))^n = (123)^n(4567)^n$ and if $(123)^n(4567)^n = e$ then $(123)^n = e$ and $(4567)^n = e$. The former happens if and only if n is a multiple of 3 and the latter happens if and only if n is a multiple of 4. Therefore both happen if and only if n is a multiple of 12—that is, $((123)(4567))^n = e$ if $n = 12$ and this is the smallest positive number with this property. □

(c) (Extra credit) How many elements are there in S_7 with order 12?

Solution. An element of S_7 has order 12 if and only if it is the product of a disjoint 3-cycle and 4-cycle. There are $\binom{7}{4}$ ways to choose the elements of the 3- and 4-cycles; then we have to choose how they are permuted. There are two 3-cycles of a set with 3 elements and there are six 4-cycles of a set with 4-elements. Therefore there are

$$\binom{7}{4} \cdot 2 \cdot 6 = 420$$

elements of order 12 in S_7. □

Problem 4. Let G be the subgroup of $\mathbf{Z}$ generated by $4096 = 2^{14}$ and $5832 = 2^3 \cdot 3^6$. Recall that this means G consists of all integers of the form $4096x + 5832y$ with $x, y \in \mathbf{Z}$.

(a) Is 32 in G? Justify your answer.

Solution. First notice that the gcd of 4096 and 5832 is 8. Therefore by Theorem 4 there are integers a and b such that $4096a + 5832b = 8$. But then

$$4096 \cdot 4a + 5832 \cdot 4b = 4 \cdot 8 = 32$$

so the answer is YES. $\square$

(b) List all $x \in \mathbf{Z}$ between 0 and 10 that are not in G. Justify your answer.

Solution. If $x \in \mathbf{Z}$ is in G then $\gcd\{4096, 5832\}$ divides x because the gcd divides every integral linear combination of 4096 and 5832. The gcd is 8 in this case, so x is *not*[1] in G if and only if x is not divisible by 8. The ←[1] answer is therefore $\{1, 2, 3, 4, 5, 6, 7, 9, 10\}$. $\square$

Problem 5. Let G be the set of all pairs (a, b) where $a \in \mathbf{Z}/7\mathbf{Z}$ and $b \in \mathbf{Z}/8\mathbf{Z}$. Define an operation on G by $(a, b) + (a', b') = (a + a', b + b')$.

(a) Prove that with this operation, G is a group.

Solution. Associativity:

$$\begin{aligned}((a, b) + (a', b')) + (a'', b'') &= (a + a' + a'', b + b' + b'') && \text{by associativity for } \mathbf{Z}/7\mathbf{Z} \text{ and } \mathbf{Z}/8\mathbf{Z} \\ &= (a, b) + ((a', b') + (a'', b'')).\end{aligned}$$

Identity: $(0, 0)$

$$(0, 0) + (a, b) = (0 + a, 0 + b) = (a, b) \qquad (a, b) + (0, 0) = (a + 0, b + 0) = (a, b)$$

Inverse: the inverse of (a, b) is $(-a, -b)$

$$\begin{aligned}(a, b) + (-a, -b) &= (a + (-a), b + (-b)) \\ &= (0, 0)\end{aligned} \qquad \begin{aligned}(-a, -b) + (a, b) &= (-a + a, -b + b) \\ &= (0, 0).\end{aligned}$$

$\square$

(b) Show that the order of the element $(1, 1) \in G$ is 56.

Solution. The order is 56. We have $56(1, 1) = (56, 56) = (0, 0)$ because $56 \equiv 0 \pmod 7$ and $56 \equiv 0 \pmod 8$. On the other hand, if $n(1, 1) \equiv (0, 0)$ then $n \equiv 0 \pmod 7$ and $n \equiv 0 \pmod 8$ so n is divisible by both 7 and 8. Therefore n is divisible by $7 \cdot 8 = 56$. Thus 56 is the least positive integer n such that $n(1, 1) = (0, 0)$. That is, $56 = \mathrm{ord}(1, 1)$. $\square$

(c) Show that G is isomorphic to $\mathbf{Z}/56\mathbf{Z}$.

Solution. Consider the function $\varphi : \mathbf{Z}/56\mathbf{Z} \to G$ sending n to (n, n). We have to check that this is well-defined: if $a \equiv b \pmod{56}$ then $b = a + 56k$ so $\varphi(b) = (a + 56k, a + 56k)$. But $a + 56k \equiv a \pmod 7$ and $a + 56k \equiv a \pmod 8$ so $(a + 56k, a + 56k) = (a, a)$ in G. That is, $\varphi(b) = \varphi(a)$.

We check φ is a homomorphism: if $a, b \in \mathbf{Z}/56\mathbf{Z}$ then

$$\varphi(a + b) = (a + b, a + b) = (a, a) + (b, b) = \varphi(a) + \varphi(b).$$

This holds for all $a, b \in \mathbf{Z}/56\mathbf{Z}$ so φ is a homomorphism.

We can also check that φ is injective. If $\varphi(n) = (0, 0)$ then n is a multiple of both 7 and 8 so n is a multiple of 56—that is, $n \equiv 0 \pmod{56}$.

Finally, note that both G and $\mathbf{Z}/56\mathbf{Z}$ have 56 elements. Therefore an injective function from $\mathbf{Z}/56\mathbf{Z}$ to G must be a bijection. Thus φ is an injective homomorphism, so φ is an isomorphism. $\square$

[1] I left out the word not in an earlier version of the solutions. Thanks Laura for catching this!

Solution. Another homomorphism that works is $\psi : G \to \mathbf{Z}/56\mathbf{Z}$ defined by

$$\psi(a, b) = 8a + 7b.$$

This is well-defined, for if $a \equiv a' \pmod 7$ and $b \equiv b' \pmod 8$ then $a' = a + 7k$ and $b' = b + 8\ell$ so

$$\psi(a', b') = \psi(a + 7k, b + 8\ell) = 8a + 56k + 7b + 56\ell = \psi(a, b) + 56(k + \ell) \equiv \psi(a, b) \pmod{56}.$$

Therefore $\psi(a', b') = \psi(a, b)$ if (a', b') and (a, b) represent the same element of $\mathbf{Z}/56\mathbf{Z}$.

This is injective, for if $8a + 7b = 8a' + 7b'$ then $8(a - a') = 7(b - b')$ so 8 divides $b - b'$ and 7 divides $a - a'$ (because 7 and 8 are relatively prime). This means that $a \equiv a' \pmod 7$ and $b \equiv b' \pmod 8$ so $(a, b) = (a', b')$ in G.

It is also a homomorphism, because

$$\begin{aligned}
\psi((a, b) + (a', b')) &= \psi(a + a', b + b') \\
&= 8(a + a') + 7(b + b') \\
&= (8a + 7b) + (8a' + 7b') \\
&= \psi(a, b) + \psi(a', b').
\end{aligned}$$

Thus ψ is an injective homomorphism between groups of the same size, hence an isomorphism. $\square$

Definition 1. A **group** is a set G with an operation $* : G \times G \to G$ such that (i) $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$, (ii) there is an $e \in G$ such that $e * a = a = a * e$ for all $a \in G$, and (iii) for any $a \in G$ there is an $a^{-1} \in G$ such that $aa^{-1} = e = a^{-1}a$. The group G is said to be **abelian** if $a * b = b * a$ for all $a, b \in G$.

A subset $H \subset G$ is called a **subgroup** if (i) for all $a, b \in H$ the element $a * b$ is in H, and (ii) H is a group with operation $*$.

A group is called **cyclic** if it is isomorphic $\mathbf{Z}$ or it is isomorphic to $\mathbf{Z}/n\mathbf{Z}$ for some integer n.

Definition 2. Suppose that G and H are groups with operations written multiplicatively. A **homomorphism** $\varphi : G \to H$ is a function $\varphi : G \to H$ such that $\varphi(xy) = \varphi(x)\varphi(y)$. A homomorphism is called an **isomorphism** if it is also a bijection.

The **kernel** of φ is the set $\ker(\varphi) = \{x \in G \,|\, \varphi(x) = 1\}$ where 1 is the identity in H.

The **image** of φ is the set $\mathrm{im}(\varphi) = \{y \in H \,|\, \exists x \in G,\ y = \varphi(x)\}$.

Notation

$\mathbf{Z}$ is the set of integers and $\mathbf{R}$ is the set of real numbers.

D_n is the set of rigid symmetries of a regular n-gon.

$\mathbf{Z}/n\mathbf{Z}$ is the set of equivalence classes of integers modulo n.

$\gcd\{a_1, \ldots, a_n\}$ denotes the greatest common divisor of integers $a_1, \ldots, a_n$.

A **complex number** is a symbol $x + iy$ where x and y are real numbers; the set of complex numbers is denoted $\mathbf{C}$. The basic operations on complex numbers are:

addition: $(x + iy) + (z + iw) = (x + z) + i(y + w)$

multiplication: $(x + iy)(z + iw) = (xz - yw) + i(xw + yz)$

conjugation: $\overline{x + iy} = x - iy$

absolute value: $|x + iy| = \sqrt{x^2 + y^2}$

If X is a set, S_X is the set of bijections from X to itself. If $X = \{1, 2, \ldots, n\}$ then S_X is also written S_n.

If $\sigma \in S_n$ the sign of σ is the expression $\mathrm{sgn}(\sigma) = \displaystyle\prod_{1 \le i < j \le n} \frac{x_{\sigma(i)} - x_{\sigma(j)}}{x_i - x_j}$. An element of S_n is called a **transposition** if it exchanges two numbers and leaves all others unchanged. An element of S_n is called **even** if its sign is 1 and **odd** if its sign is -1. The set of even elements of S_n is denoted A_n.

Theorems

Proposition 1. *The following are abelian groups: (i) $\mathbf{Z}$ under addition, (ii) $\mathbf{Z}/n\mathbf{Z}$ under addition, (iii) $\mathbf{R}$ under addition, (iv) $\mathbf{R}^*$ under multiplication, (v) $\mathbf{C}^*$ under multiplication, (vi) S_X if X is a set with 2 or fewer elements.*

The following are non-abelian groups: (vii) D_n, (viii) S_X if X is a set with 3 or more elements.

Theorem 2 (Cayley's theorem)**.** *Every group is isomorphic to a subgroup of the group of symmetries of some set.*

Proposition 3. *Let G be a group. A subset $H \subset G$ is a subgroup if and only if both (i) $H \neq \varnothing$, and (ii) for all $a, b \in H$ the element ab^{-1} is in H.*

Theorem 4. *If x and y are integers with greatest common divisor d there are integers a and b such that $ax + by = d$.*

Theorem 5. *If G is a cyclic group then every subgroup of G is cyclic.*

Proposition 6. *Suppose that G and H are groups with operations written multiplicatively and identity elements both called 1. If $\varphi : G \to H$ is a homomorphism of groups then (i) $\varphi(1) = 1$, (ii) $\varphi(x^{-1}) = \varphi(x)^{-1}$ for all $x \in G$, (iii) $\ker(\varphi)$ is a subgroup of G, (iv) $\mathrm{im}(\varphi)$ is a subgroup of H.*

Proposition 7. *If $\sigma \in S_n$ then $\mathrm{sgn}(\sigma) \in \{\pm 1\}$ and the function $\mathrm{sgn} : S_n \to \{\pm 1\}$ is a homomorphism. If τ is a transposition then $\mathrm{sgn}(\tau) = -1$.*

Proposition 8. *For complex numbers z and w, we have $|zw| = |z|\,|w|$.*

Proposition 9. *If $\varphi : G \to H$ is an isomorphism of groups then $\varphi^{-1} : H \to G$ is also an isomorphism.*

Proposition 10. *The inverse of a 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is given by $\dfrac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ provided $\dfrac{1}{ad - bc}$ exists.*

Proposition 11. *Let g be an element of a group G and suppose $g^n = 1$. Then $\mathrm{ord}(g)$ is finite and divides n.*