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.

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**.

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

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

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

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.

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

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.

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

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

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 $\ker(\varphi) = \{x \in G \mid \varphi(x) = 1\}$ where 1 is the identity in H.

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

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.*