Math 3140 — Fall 2012
Exam #1 – Rejected problems

Exercise 1. Verify that if $\varphi : A \to B$ and $\psi : B \to C$ are homomorphisms of groups then $\psi \circ \varphi : A \to C$ is also a homomorphism.

Exercise 2. Prove that an abelian group G and a non-abelian group H cannot be isomorphic to each other.

Exercise 3. Find all solutions to the equation $10x \equiv 6 \pmod{12}$ in $\mathbf{Z}/12\mathbf{Z}$.

Exercise 4. Show that the group of **rotational** symmetries of a regular tetrahedron centered at the origin is A_4.

Exercise 5. Let V be a vector space. Let G be the set of invertible linear transformations from V to itself. Show that G is a group with the group operation being composition of functions.

Exercise 6. Let X be an infinite set and let G be the set of injective functions from X to itself. If $f, g \in G$, define fg to be the composition of functions $f \circ g$. Show that G is **not** a group.

Exercise 7. Show that any subgroup of an abelian group is abelian.

Exercise 8. Verify that if A is a subgroup of B and B is a subgroup of C then A is a subgroup of C.

Exercise 9. Let $V = \mathbf{R}^n$. Let G be the set of *bijective, linear* functions $f : V \to V$. For $f, g \in G$, let $f * g$ be the composition $f \circ g$.

(a) Show that G is a group with operation $*$.

(b) Let $|\mathbf{x}|$ denote the length of a vector $\mathbf{x} \in V$. Let $H \subset G$ be the subset of all $f \in G$ such that $|f(\mathbf{x})| = |x|$. Symbolically,
$$H = \big\{ f \in G \bigm| \forall \mathbf{x} \in V,\ \big|f(\mathbf{x})\big| = \big|\mathbf{x}\big| \big\}.$$
Show that H is a subgroup of G.

Exercise 10. Let G be a set with an operation $*$. Suppose that $*$ is associative and commutative. For each $x \in G$, let $L_x : G \to G$ be the function $L_x(y) = x * y$. Assume that for all $x \in G$ the function L_x is a **bijection**. Show that G is an abelian group.

Definitions

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; use 1 to denote the identity elements. 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 $\ker(\varphi) = \{x \in G \,|\, \varphi(x) = 1\}$.

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

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.

$\mathrm{GL}(n, \mathbf{R})$ is the set of invertible $n \times n$ matrices with real coefficients.

$\gcd\{a_1, \ldots, a_n\}$ 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 $\operatorname{sgn}(\sigma) = \displaystyle\prod_{1 \le i < j \le n} \frac{x_{\sigma(i)} - x_{\sigma(j)}}{x_i - x_j}$. An element of S_n is called a **transposition** if it exchanges two numbers and leaves all others unchanged.

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, (ix) $\mathrm{GL}(n, \mathbf{R})$ under matrix multiplication, if $n \ge 2$.

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) $\operatorname{im}(\varphi)$ is a subgroup of H.*

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

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.*