MATH 3063 ABSTRACT ALGEBRA PROF. PAUL BAILEY Project 5 April 18, 2007 Name:

Complete these problems and turn in the solution by Wednesday, April 11, 2007. Attach this page to the front of the solutions. Solutions should be self explanatory and written in complete sentences.

Groups of Functions

Let A and B be nonempty sets. The set of all functions from A to B is denoted $\mathcal{F}(A, B)$:

$$\mathcal{F}(A, B) = \{f : A \to B\}.$$

Problem 1. Let A and B be nonempty finite sets with $|A| = m$ and $|B| = n$.

(a) Find $|\mathcal{F}(A, B)|$. Justify your answer.

(b) If $m \leq n$, how many functions $A \to B$ are injective?

(c) If $n \leq m$, how many functions $A \to B$ are surjective?

(c) Suppose $m = n$ and let $f \in \mathcal{F}(A, B)$. Explain why f is injective if and only if f is surjective.

Let G be a group. An *automorphism* of G is a bijective homomorphisms from G onto itself. Let $\text{Aut}(G)$ denote the set of all automorphisms of G. It it immediate from the definition that $\text{Aut}(G) \subset \text{Sym}(G)$.

Problem 2. Let G be a group. Show that $\text{Aut}(G) \leq \text{Sym}(G)$.

Let $n \in \mathbb{Z}$ with $n \geq 2$ and set $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$. Then $n\mathbb{Z} \triangleleft \mathbb{Z}$ under addition.
Set $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$; the elements of $\mathbb{Z}_n$ are cosets $\overline{k} = k + n\mathbb{Z} = \{k + nm \mid m \in \mathbb{Z}\}$, where $k \in \mathbb{Z}$.
Set $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid a \text{ is invertible}\}$. Recall that $a \in \mathbb{Z}_n$ is invertible if and only if a is represented by an integer which is relatively prime to n.
We have seen that

- $\mathbb{Z}_n$ is a cyclic group under addition;
- $\mathbb{Z}_n^*$ is an abelian group under multiplication.

Problem 3. Let $n \in \mathbb{Z}$ with $n \geq 2$ and let $a \in \mathbb{Z}_n^*$.
Define a function $\phi_a : \mathbb{Z}_n \to \mathbb{Z}_n$ by $\phi_a(x) = ax$.

(a) Show that ϕ_a is a homomorphism.

(b) Show that ϕ_a is injective.

(c) Show that ϕ_a is surjective.

(d) Conclude that $\phi_a \in \text{Aut}(\mathbb{Z}_n)$.

Hint 1. Compute some simple examples first; say $n = 5$, $a = \overline{3}$ and $n = 6$, $a = \overline{5}$.

Problem 4. Let $n \in \mathbb{Z}$ with $n \geq 2$ and for $a \in \mathbb{Z}_n^*$ define ϕ_a as in Problem 3.
Define a function $\phi : \mathbb{Z}_n^* \to \text{Aut}(\mathbb{Z}_n)$ by $\phi(a) = \phi_a$.

(a) Show that ϕ is a homomorphism.

(b) Show that ϕ is injective.

(c) Show that ϕ is surjective.

(d) Conclude that $\text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$.

Hint 2. You need to use the fact that $\mathbb{Z}_n$ is cyclic; what are the generators?