MATH 3063 ABSTRACT ALGEBRA — Project 2 — Name:
PROF. PAUL BAILEY — February 12, 2007

Complete and turn in on Friday, February 16. Write neatly on this handout. You may reprint the handout from the web page www.saumag.edu/pbailey.

Proving Things

Use the definitions. Follow the following frameworks. Fill in the blanks of the outlined proofs, or fill in the gaps of the partially outlined proofs. Your proof MUST USE THE GIVEN SENTENCES.

Definition 1. Let $f : A \to B$.

If $C \subset A$, the *image* of C under f is

$$f(C) = \{b \in B \mid b = f(c) \text{ for some } c \in C\}.$$

If $D \subset B$, the *preimage* of D under f is

$$f^{-1}(D) = \{a \in A \mid f(a) \in D\}.$$

We say that f is *injective* if, for every $a_1, a_2 \in A$, we have

$$f(a_1) = f(a_2) \quad \Rightarrow \quad a_1 = a_2.$$

We say that f is *surjective* if

$$\forall b \in B \exists a \in A \quad \ni \quad f(a) = b.$$

We say that f is *bijective* if it is injective and surjective.

Type 1. Let A and B be sets. Show that $A \subset B$.

Method. Let $a \in A$. [work; use the defining property of A] Thus $a \in B$. Therefore $A \subset B$. □

Type 2. Let A and B be sets. Show that $A = B$.

Method. We show that $A \subset B$ and $B \subset A$.
($A \subset B$) Let $a \in A$. [work] Thus $a \in B$.
($B \subset A$) Let $b \in B$. [work] Thus $b \in A$.
Since $A \subset B$ and $B \subset A$, we have $A = B$. □

Type 3. Let $f : A \to B$. Show that f is injective.

Method. Let $a_1, a_2 \in A$ such that $f(a_1) = f(a_2)$. [work; using definition of f, show that $a_1 = a_2$] Therefore $a_1 = a_2$. Since $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$, f is injective. □

Type 4. Let $f : A \to B$. Show that f is surjective.

Method. Let $b \in B$. [work; using definition of f, find a such that $f(a) = b$] Therefore $f(a) = b$. Since $\forall b \in B \exists a \in A \ni f(a) = b$, f is surjective. □

Type 5. Let p and q be propositions. Show that $p \Leftrightarrow q$.

Method. We show that $p \Rightarrow q$ and $q \Rightarrow p$.
($p \Rightarrow q$) [work]
($q \Rightarrow p$) [work]
Since $p \Rightarrow q$ and $q \Rightarrow p$, we have $p \Leftrightarrow q$. □

Problem 1. Let $f : A \to B$ and let $D_1, D_2 \subset B$. Show that $f^{-1}(D_1 \cap D_2) = f^{-1}(D_1) \cap f^{-1}(D_2)$.

Proof. We show containment in both directions.

($\subset$) Let $x \in f^{-1}(D_1 \cap D_2)$.

Then ______________ $\in D_1 \cap D_2$.

Thus $f(x) \in$ ______________ and $f(x) \in$ ______________.

Thus $x \in$ ______________ and $x \in$ ______________.

Therefore, $x \in$ ______________.

($\supset$) Let $x \in f^{-1}(D_1) \cap f^{-1}(D_2)$.

Then $x \in$ ______________ and $x \in$ ______________.

Thus ______________ $\in D_1$ and ______________ $\in D_2$.

Thus $f(x) \in$ ______________ $\cap$ ______________.

Therefore, $x \in$ ______________. □

Problem 2. Let $f : A \to B$ and let $D_1, D_2 \subset B$. Show that $f^{-1}(D_1 \cup D_2) = f^{-1}(D_1) \cup f^{-1}(D_2)$.

Proof. We show containment in both directions.
($\subset$) Let $x \in f^{-1}(D_1 \cup D_2)$; we wish to show that $x \in f^{-1}(D_1) \cup f^{-1}(D_2)$.

Therefore $x \in f^{-1}(D_1) \cup f^{-1}(D_2)$.

($\supset$) Let $x \in f^{-1}(D_1) \cup f^{-1}(D_2)$; we wish to show that $x \in f^{-1}(D_1 \cup D_2)$.

Therefore $x \in f^{-1}(D_1 \cup D_2)$. □

Problem 3. Let $f : A \to B$ and $g : B \to C$. Suppose that f is surjective and $g \circ f$ is injective. Show that g is injective.

Proof. Let $b_1, b_2 \in B$ such that $g(b_1) = g(b_2)$. We wish to show that $b_1 = b_2$.

Since f is surjective, there exist $a_1, a_2 \in$ ______________ such that

$f(a_1) =$ ______________ and $f(a_2) =$ ______________.

Applying g to these equations gives $g(f(a_1)) =$ ______________ and $g(f(a_2)) =$ ______________.

But $g(b_1) = g(b_2)$, and since $g \circ f$ is injective, $a_1 =$ ______________.

Thus $f(a_1) =$ ______________, that is, $b_1 = b_2$.

Therefore f is injective. □

Problem 4. Let $f : A \to B$ and $g : B \to C$. Suppose that g is injective and $g \circ f$ is surjective. Show that f is surjective.

Proof. Let $b \in B$. We wish to find $a \in A$ such that $f(a) = b$.

Let $c = g($______________$)$.

Since $g \circ f$ is surjective, there exists $a \in A$ such that ______________ $= c$,

that is, $g(f(a)) = g(b)$.

Since g is injective, ______________ $= b$.

Therefore f is surjective. □

Problem 5. Let $f : \mathbb{Z} \to \mathbb{Z}$ be given by $f(a) = 3a + 2$. Show that f is injective but not surjective.

Proof. To show that f is injective, let $a_1, a_2 \in \mathbb{Z}$ such that $f(a_1) = f(a_2)$.

Therefore, $a_1 = a_2$, so f is injective.

To see that f is not surjective, it suffices to find $b \in \mathbb{Z}$ such that b is not in the image of $\mathbb{Z}$ under f.

Let $b =$ ______________;

then $f(a) = b$ if and only if $a =$ ______________ $\in \mathbb{Q}$.

But this a is not an integer. Therefore f is not surjective. □

Problem 6. Let $f : \mathbb{Z} \to \mathbb{N}$ be given by

$$f = \begin{cases} 2a & \text{if } a \text{ is positive ;} \\ 1 - 2a & \text{if } a \text{ is zero or negative.} \end{cases}$$

Show that f is bijective.

Proof. We show that f is injective and surjective.

(*Injectivity*) Let $a_1, a_2 \in \mathbb{Z}$ such that $f(a_1) = f(a_2)$. Let $n = f(a_1) = f(a_2)$.

Case 1: Suppose n is odd.

Case 2: Suppose n is even.

In either case, $a_1 = a_2$. Therefore f is injective.

(*Surjectivity*) Let $n \in \mathbb{N}$. We wish to find $a \in \mathbb{Z}$ such that $f(a) = n$.

Case 1: Suppose n is odd.

Case 2: Suppose n is even.

In either case, there exists $a \in \mathbb{Z}$ such that $f(a) = n$. Therefore f is surjective. □

Problem 7. Let $a, b \in \mathbb{Q}$, and define $f : \mathbb{Q} \to \mathbb{Q}$ by $f(x) = ax + b$. Show that f is bijective.

Definition 2. Let $\sim$ be a relation on a set A. We say that $\sim$ is an *equivalence relation* if

- *Reflexivity* $a \sim a$ for all $a \in A$;
- *Symmetry* $a \sim b$ implies $b \sim a$ for all $a, b \in A$;
- *Transitivity* $a \sim b$ and $b \sim c$ implies $a \sim c$ for all $a, b, c \in A$.

Problem 8. Let n be a positive integer and let $G = S_n$ be the set of permutations of the set $\{1, \dots, n\}$. Let H be a subset of G satisfying

(S0) $e \in H$ (it contains the e, where e denotes the identity);

(S1) $h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$ (it is closed under composition);

(S2) $h \in H \Rightarrow h^{-1} \in H$ (it is closed under inverses).

Define a relation $\sim$ on G by

$$g_1 \sim g_2 \quad \Leftrightarrow \quad g_1 g_2^{-1} \in H.$$

Show that $\sim$ is an equivalence relation.

Proof. We show that $\sim$ is reflexive, symmetric, and transitive.

(*Reflexivity*) Let $g \in G$.

Now $gg^{-1} =$ ______________, which is in H by property ______________.

Thus $g \sim g$. Therefore, $\sim$ is reflexive.

(*Symmetry*) Let $g_1, g_2 \in G$ such that $g_1 \sim g_2$. Then $g_1 g_2^{-1} \in H$, so $g_1 g_2^{-1} = h$ for some $h \in H$.

Now $h^{-1} \in H$ by property ______________; but $h^{-1} =$ ______________, because

$$h(g_2 g_1^{-1}) = (g_1 g_2^{-1})(g_2 g_1^{-1}) = g_1(g_2^{-1} g_2) g_1^{-1} = g_1 e g_1^{-1} = g_1 g_1^{-1} = e.$$

Thus ______________ $\in H$.

Thus $g_2 \sim g_1$. Therefore, $\sim$ is symmetric.

(*Transitivity*) Let $g_1, g_2, g_3 \in G$ such that $g_1 \sim g_2$ and $g_2 \sim g_3$. Then $g_1 g_2^{-1} \in H$ and $g_2 g_3^{-1} \in H$.

Thus $g_1 \sim g_3$. Therefore, $\sim$ is transitive. $\square$