

MATH 521A EXAM 3 SOLUTIONS

Nov 14, 2007

1. (10 pts) Let $f : S \rightarrow T$ be a function. Prove that f is one-to-one if and only if there exists $g : T \rightarrow S$ such that $gf = \text{Id}_S$.

Suppose f is one-to-one. We will construct $g : T \rightarrow S$ so that $gf = \text{Id}_S$. Let $t \in T$. If $t \in \text{im}(f)$, then there exists some $s \in S$ such that $f(s) = t$. Note that since f is one-to-one, this s is actually the unique such element of S . We will need this later. Let $g(t) = s$. If $t \notin \text{im}(f)$, then pick any $s \in S$ and let $g(t) = s$. We now have a function $g : T \rightarrow S$.

We claim $gf = \text{Id}_S$. Let $s \in S$. Let $t = f(s)$. Since $t \in \text{im}(f)$, $g(t)$ is an element of S such that $f(g(t)) = t$. As we remarked before, there is exactly one such element of S , namely s . So $g(f(s)) = g(t) = s$. This shows that gf maps every $s \in S$ to itself, hence $gf = \text{id}_S$.

Conversely, let $g : T \rightarrow S$ be such that $gf = \text{id}_S$. We actually proved in class that if gf is one-to-one then f must be one-to-one. Since Id_S is obviously one-to-one, f is one-to-one. The proof went like this. Let $s_1 \neq s_2$ be elements in S . Since

$$g(f(s_1)) = \text{Id}_S(s_1) = s_1 \neq s_2 = \text{Id}_S(s_2) = g(f(s_2))$$

therefore $f(s_1) \neq f(s_2)$.

Actually, if you look carefully, there is a problem in the pathological case that $S = \emptyset$ and $T \neq \emptyset$. In this case we cannot choose an arbitrary element of S to send all the elements of T to when we construct g . In fact, there exists no function $g : T \rightarrow S$. But there exists a function $f : S \rightarrow T$. It is a function that does nothing. Since S has no two different elements, f cannot send two different elements of S to the same element of T , hence f is one-to-one. So in this one uninteresting case, there is no $g : T \rightarrow S$ such that $gf = \text{Id}_S$ even though f is one-to-one. Noticing something like this can earn you generous extra credit. But no one did notice because no one knew how to construct g .

2. (10 pts) Let G be a group with the following property: whenever $a, b, c \in G$ and $ab = ca$, then $b = c$. Prove that G is abelian.

We need to show $ab = ba$ for any $a, b \in G$. So let $a, b \in G$ be arbitrary elements. Let $c = aba^{-1}$. Now

$$ca = (aba^{-1})a = ab(a^{-1}a) = ab.$$

By the assumed property, $b = c = aba^{-1}$. Now multiply by a on the right to get $ba = (aba^{-1})a = ab(a^{-1}a) = ab$. This shows G is abelian.

3. (5 pts) Let G be a group and $a, b \in G$. Prove that $(ab)^{-1} = b^{-1}a^{-1}$.

Notice that

$$\begin{aligned} (ab)(b^{-1}a^{-1}) &= a(b^{-1}b)a^{-1} = aea^{-1} = aa^{-1} = e \\ (b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e. \end{aligned}$$

Hence $(ab)^{-1} = b^{-1}a^{-1}$.

4. (10 pts)

(a) Let $f : A \rightarrow B$ and $g : B \rightarrow C$ be onto functions. Prove that $g \circ f$ is onto.

Since f and g are onto

$$\begin{aligned}f(A) &= \{f(a) \mid a \in A\} = B \\f(B) &= \{g(b) \mid b \in B\} = C.\end{aligned}$$

Hence $g(f(A)) = g(B) = C$. This shows $g \circ f$ is onto.

Here is another proof. Let $c \in C$. Since g is onto, there exists $b \in B$ such that $g(b) = c$. Since f is onto, there exists $a \in A$ such that $f(a) = b$. Hence $g(f(a)) = c$. This can be done for any $c \in C$, so $g \circ f$ is onto.

- (b) Give an example of a function which is onto but not one-to-one. Prove that your example is indeed onto and not one-to-one.

There are zillions of examples. Here is one you saw in class. Let $f : \mathbb{R} \rightarrow \mathbb{R}^{\geq 0}$ be given by $f(x) = x^2$. Then f is onto since for any $y \in \mathbb{R}^{\geq 0}$, $f(\sqrt{y}) = y$. But f is not one-to-one because $f(-1) = 1 = f(1)$.

5. (12 pts) In your answers to this problem, you don't need to prove that your examples are indeed what they are. But do explain carefully what your groups are, including what the group operation is. It is not enough to give only a notation like D_4 .
- (a) State the definition of group.

A group G is a nonempty set G with a binary operation on it such that

Associativity: $(ab)c = a(bc)$ for all $a, b, c \in G$,

Identity: there exists an element $e \in G$ such that $ae = ea = a$ for all $a \in G$,

Inverses: for each $a \in G$ there is an element $b \in G$ such that $ab = ba = e$.

- (b) Give an example of a finite abelian group.

One such example is \mathbb{Z}_n , the integers modulo n under addition (for $n \geq 1$). Another is the trivial group $G = \{e\}$. See Examples 3, 11, 14, and 19 in Ch. 2 of your textbook too.

- (c) Give an example of a finite nonabelian group.

One such example is D_n , the symmetries of a regular n -gon under composition (for $n \geq 3$). Another is the trivial group $G = \{e\}$. See Examples 3, 11, and 19 in Ch. 2 of your textbook too. Also, see $SL(2, \mathbb{Z}_p)$ and $GL(2, \mathbb{Z}_p)$ in Examples 17 and 18.

- (d) Give an example of an infinite abelian group.

One such example is \mathbb{Z} , the integers under addition. See Examples 4, 6, 8, 15, 16, 20 for others.

- (e) Give an example of an infinite nonabelian group.

One example we gave in class was the set of invertible functions $\mathbb{R} \rightarrow \mathbb{R}$ under composition. See Examples 9, 17, 18 for others.

6. (8 pts) Let G be a group.
- (a) Let $x \in G$. Prove that x has a unique inverse in G .

By the definition of a group, x must have at least one inverse in G . Suppose that $y, z \in G$ are both inverses of x . Then

$$y = ye = y(xz) = (yx)z = ez = z.$$

This shows that x has exactly one inverse in G .

(b) Let $x \in G$. Prove that $(x^{-1})^{-1} = x$.

Notice $xx^{-1} = e$ and $x^{-1}x = e$. Hence x indeed works as an inverse of x^{-1} . By uniqueness of the inverse, $(x^{-1})^{-1} = x$.

7. (15 pts) **Extra credit problem.** Let G be a finite group with identity e . Let

$$S = \{x \in G \mid x^3 = e\}.$$

Prove that S has an odd number of elements. (Hint: show that all but one of the elements of S come in pairs as x, x^2 and that two such pairs are either the same or disjoint.)

First, observe that $e \in S$ since $e^3 = e$. We will do the rest of the proof in a few steps.

Claim: if $x \in S$ then $x^2 \in S$. Proof: if $x \in S$ then $x^3 = e$, hence $(x^2)^3 = x^6 = (x^3)^2 = e^2 = e$. So $x^2 \in S$.

Claim: if x is a nonidentity element, $x \neq x^2$. If $x = x^2$, then by left (or right) cancellation, $e = x$.

Hence if $x \in S$ is a nonidentity element, we can pair it up with x^2 . We will now look at the pairs $\{x, x^2\} \in S$.

Claim: if $x, y \in S$, then $\{x, x^2\}$ and $\{y, y^2\}$ are either the same or disjoint. Let $P = \{x, x^2\}$ and $Q = \{y, y^2\}$. Now there are three cases:

$x = y$: In this case, obviously $P = Q$.

$x = y^2$: Now

$$x^2 = (y^2)^2 = y^4 = (y^3)y = ey = y.$$

Hence $P = Q$ again.

$x \neq y$ and $x \neq y^2$: If $x^2 = y$ then $y^2 = (x^2)^2 = x^4 = x$. But we know this is not the case.

If $x^2 = y^2$, then

$$x = x^4 = (x^2)^2 = (y^2)^2 = y^4 = y.$$

But we know this is not the case either. Therefore P and Q are disjoint.

Now notice that S is a disjoint union of the sets $\{x, x^2\}$ as x runs through the elements of S . Almost all of these sets have two elements, except for $\{e, e^2\} = \{e\}$. Hence S has an odd number of elements.