Math 521A Final Exam Solutions

Dec 15, 2009

1. (10 pts) Let p be prime and $a, b \in \mathbb{Z}$. Prove that

$$(a+b)^p \equiv a^p + b^p \mod p.$$

By the Binomial Theorem,

$$(a+b)^p = \sum_{n=0}^{p} \binom{p}{n} a^n b^{p-n}$$

where

$$\binom{p}{n} = \frac{p!}{n!(p-n)!}.$$

Suppose $1 < n < p$. Notice that since $n < p$, none of the factors in $n! = n(n-1)\cdots 1$ are divisible by p. Since $1 < n$, none of the factors in $(n-p)! = (n-p)(n-p-1)\cdots 1$ are divisible by p either. Hence p and $n!(n-p)!)$ are relatively prime.

On the other hand, we know $\binom{p}{n}$ is an integer, so $n!(n-p)!$ divides $p! = p(p-1)!$. Therefore $n!(n-p)!$ must divide $(p-1)!$ (by Prop 1.2.3(b)). That is $\frac{(p-1)!}{n!(p-n)!} \in \mathbb{Z}$ and

$$\binom{p}{n} = \frac{p!}{n!(p-n)!} = p\,\frac{(p-1)!}{n!(p-n)!}$$

is a multiple of p and

$$\binom{p}{n} \equiv 0 \mod p.$$

We can now conclude

$$(a+b)^p \equiv \sum_{n=0}^{p} \binom{p}{n} a^n b^{p-n} \equiv a^p + \sum_{n=1}^{p-1} \underbrace{\binom{p}{n}}_{\equiv 0} a^n b^{p-n} + b^p \equiv a^p + b^p \mod n.$$

2. (10 pts) Let $f : A \to B$ be a function. Prove that f is onto if and only $h \circ f = k \circ f$ implies $h = k$, for every set C and all choices of functions $h, k : B \to C$.

Suppose f is onto. Let C be any nonempty set and $h, k : B \to C$ where C such that $h \circ f = k \circ f$. This means that for any $h \circ f(a) = k \circ f(a)$ for all $a \in A$. Let b be any element in B. Since f is onto, there exists some $a \in A$ such that $f(a) = b$. Then

$$h(b) = h \circ f(a) = k \circ f(a) = k(b).$$

Since this can be done for any $b \in B$, $h = k$.

Conversely, suppose f is not onto. Then there exists a $b \in B$ such that $f(a) \neq b$ for any $a \in A$. Let $C = \{0, 1\}$ and define $h, k : B \to C$ by

$$h(x) = 0 \qquad \text{and} \qquad k(x) = \begin{cases} 0 & x \neq b \\ 1 & x = b \end{cases}$$

Now observe that $h \circ f(a) = 0$ for all $a \in A$. Also $k \circ f(a) = 0$ for all $a \in A$ since $f(a) \neq b$. Therefore $h \circ f = k \circ f$. But $h \neq k$. So it is not true that $h \circ f = k \circ f$ implies $h = k$, for every set C and all choices of functions $h, k : B \to C$.

3. (10 pts) Let $G = \{x \in \mathbb{R} \mid x > 0 \text{ and } x \neq 1\}$. Define the operation $*$ on G by $a * b = a^{\ln(b)}$, for all $a, b \in G$. Prove that G is an abelian group under the operation $*$.

Notice that $a * b = a^{\ln(b)} = e^{\ln(a)\ln(b)}$. Let $a, b \in G$. Then

$$a, b > 0 \implies \ln(a), \ln(b) \in \mathbb{R} \implies a * b = e^{\ln(a)\ln(b)} \in \mathbb{R}.$$

Also

$$a, b \neq 1 \implies \ln(a), \ln(b) \neq 0 \implies \ln(a)\ln(b) \neq 0 \implies a * b \neq e^0 = 1.$$

Therefore G is closed under $*$.

If $a, b \in G$, then

$$a * b = e^{\ln(a)\ln(b)} = e^{\ln(b)\ln(a)} = b * a.$$

Hence $*$ is commutative.

If $a, b, c \in G$, then

$$(a * b) * c = e^{(\ln(a)\ln(b))\ln(c)} = e^{\ln(a)(\ln(b)\ln(c))} = a * (b * c).$$

Hence $*$ is associative.

If $a \in G$, then $e * a = e^{\ln(a)} = a$ and $a * e = a$ follows by commutativity. Hence e, which is obviously in G, is an identity for $*$.

If $a \in G$, then $\ln(a) \in R^*$. Therefore $1/\ln(a) \in \mathbb{R}^*$. Hence $b = e^{1/\ln(a)} \in \mathbb{R} \setminus \{1\}$. Notice that

$$a * b = e^{\ln(a)\ln(b)} = e^{\ln(a)\frac{1}{\ln(a)}} = e^1 = e$$

and $b * a = e$ follows by commutativity. Hence b is an inverse of a in G. This can be done for any $a \in G$, therefore every element in G has an inverse.

We can now conclude that G is an abelian group under $*$.

4. (10 pts) Let G be a group. Prove that G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

Suppose G is abelian. Let $a, b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$.

Conversely, suppose $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$. We want to prove $xy = yx$ for all $x, y \in G$. So let $x, y \in G$ and set $a = x^{-1}$ and $b = y^{-1}$. Then $x = a^{-1}$, $y = b^{-1}$, and

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

5. (10 pts) Let $a, b \in \mathbb{Z}$ not both 0. Prove that a and b have a greatest common divisor d and d is the smallest positive linear combination of a and b.

See the proof of Theorem 1.1.6 in your textbook.

6. (10 pts) Let $a, n \in \mathbb{Z}$ with $n > 1$. Prove that there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \mod n$ if and only if a and n are relatively prime.

See the proof of Proposition 1.4.5(a) in your textbook.

7. (2 pts each) Let $\sigma \in S_9$ be

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 5 & 2 & 9 & 3 & 6 & 4 & 1 & 7 \end{pmatrix}.$$

(a) Write σ as a product of independent cycles.

$$\sigma = (1\,8)(2\,5\,3)(4\,9\,7)$$

(b) Write σ as a product of transpositions.

$$\sigma = (1\,8)(2\,5)(5\,3)(4\,9)(9\,7)$$

(c) Find σ^{-1} as a product of independent cycles.

$$\sigma^{-1} = \big((1\,8)(2\,5\,3)(4\,9\,7)\big)^{-1} = (1\,8)(2\,3\,5)(4\,7\,9)$$

(d) Find σ^{-1} as a product of transpositions.

$$\sigma^{-1} = \big((1\,8)(2\,5)(5\,3)(4\,9)(9\,7)\big)^{-1} = (9\,7)(4\,9)(5\,3)(2\,5)(1\,8)$$

(e) Find the order of σ.

By Prop 2.3.8,

$$|\sigma| = \operatorname{lcm}(2,3,3) = 6.$$

8. (10 pts)

(a) Define what a subgroup is.

See Definition 3.2.1.

Note that 3.2.2 is a proposition, not a definition, so stating that is not a correct answer.

(b) Prove or disprove: the set $H = \{\sigma \in S_5 \mid \sigma(1) = 5\}$ is a subgroup of S_5.

H fails to be a subgroup in just about every way it can. For one, $() \notin H$ because the identity does not send 1 to 5. For two, $(1\,5\,2) \in H$ but $(1\,5\,2)^2 = (1\,2\,5) \notin H$, so H is not closed under composition. Finally, $(1\,5\,2) \in H$ but $(1\,5\,2)^{-1} = (1\,2\,5) \notin H$ so not every element in H has an inverse.

9. **Extra credit problem.** Let

$$A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\}.$$

(a) (4 pts) Find the elements of A_4.

S_4 has five kinds of elements: the identity, 2-cycles, 3-cycles, 4-cycles, and elements of the form (12)(34). We know that () is even, 3-cycles are even, and elements of the form (12)(34) are even. So these are in A_4. On the other hand, 2-cycles and 4-cycles are odd, so these are not in A_4. Hence

$$\begin{aligned} A_4 = \{&(), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3),\\ &(1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3)\}. \end{aligned}$$

(b) (8 pts) Prove that A_n is a subgroup of S_n.

A_n certainly contains the identity (). Let $\sigma, \tau \in A_n$. Then

$$\sigma = \sigma_1\sigma_2\cdots\sigma_m$$
$$\tau = \tau_1\tau_2\cdots\tau_n$$

where the σ_i and τ_j are transpositions and m, n are even. Hence

$$\sigma\tau = \sigma_1\sigma_2\cdots\sigma_m\tau_1\tau_2\cdots\tau_n.$$

This shows that $\sigma\tau$ can be written as a product of $m+n$ transpositions. Since m, n are even, so is $m+n$. Therefore $\sigma\tau \in A_n$. Hence A_n is closed under composition. Also

$$\sigma^{-1} = (\sigma_1\sigma_2\cdots\sigma_m)^{-1} = \sigma_m^{-1}\sigma_{m-1}^{-1}\cdots\sigma_1^{-1} = \sigma_m\sigma_{m-1}\cdots\sigma_1,$$

which shows that σ^{-1} is a product of m transpositions. Hence $\sigma^{-1} \in A_n$. Therefore A_n is a subgroup of S_n (by Prop 3.2.2).

(c) (8 pts) Prove that $|A_n| = |S_n|/2$. (Hint: set up a one-to-one correspondence between A_n and $S_n \setminus A_n$.)

Let $f : A_n \to S_n \setminus A_n$ be the map $f(\sigma) = \sigma(1\,2)$. First, notice that f is really a map from A_n to $S_n \setminus A_n$. This is because if $\sigma \in A_n$, then σ is a product of an even number of transpositions and hence $\sigma(1\,2)$ is a product of an odd number of transpositions. Similarly, define $g : S_n \setminus A_n \to A_n$ by $g(\sigma) = \sigma(12)$ and observe that g is indeed a map from $S_n \setminus A_n$ to A_n. Finally, it is clear that $gf = 1_{A_n}$ and $fg = 1_{S_n \setminus A_n}$. Therefore f is a one-to-one correspondence from $A_n \to S_n \setminus A_n$. So A_n has the same number of elements as its complement. Therefore $|A_n| = |S_n|/2$.