

MATH 521A FINAL EXAM SOLUTIONS

Dec 14, 2007

1. (10 pts) Suppose that a cyclic group G has exactly three subgroups: G itself, $\{e\}$, and a subgroup of order 7. What is $|G|$?

Let $n = |G|$. Since G is cyclic, if $k|n$ then G has a subgroup of order k . This means that the divisors of n are $1, 7, n$. Obviously, $n \neq 7$, otherwise G and the subgroup of order 7 would not be listed as two different things. Hence 7 is a proper divisor of n . It is also the only prime divisor of n . Therefore $n = 7^m$ for some $m \geq 2$. If $m > 2$ then 7^{m-1} would be yet another divisor of n and there would have to be a subgroup of this order. Hence $m = 2$ and $|G| = 7^2 = 49$.

2. (15 pts) For $a, b \in \mathbb{R}$, define $a \sim b$ if $a - b \in \mathbb{Z}$.

(a) Show that \sim is an equivalence relation on \mathbb{R} .

Reflexivity: If $a \in \mathbb{R}$ then $a - a = 0 \in \mathbb{Z}$, hence $a \sim a$.

Symmetry: Suppose $a, b \in \mathbb{R}$ and $a \sim b$. Then $a - b \in \mathbb{Z}$, hence $b - a = -(a - b) \in \mathbb{Z}$. Therefore $b \sim a$.

Transitivity: Suppose $a, b, c \in \mathbb{R}$ such that $a \sim b$ and $b \sim c$. Then $a - b, b - c \in \mathbb{Z}$. Hence $a - c = (a - b) + (b - c) \in \mathbb{Z}$. Therefore $a \sim c$.

- (b) Describe the equivalence classes of \sim .

Let $x \in \mathbb{R}$. The equivalence class of x is the set of all those numbers which have the same fractional part as x . E.g. the equivalence class of 0.2 is

$$\{\dots, -1.8, -0.8, 0.2, 1.2, 2.2, \dots\}.$$

Another way to describe the equivalence classes is to say that for each $x \in [0, 1)$, we have an equivalence class

$$x + \mathbb{Z} = \{x + n \mid n \in \mathbb{Z}\}.$$

These are all different and they are all the equivalence classes.

3. (15 pts)

(a) Suppose a belongs to a group and $|a| = 5$. Prove that $C(a) = C(a^3)$. (Remember that $C(a)$ is the centralizer of a .)

We need to prove $C(a) \subseteq C(a^3)$ and $C(a^3) \subseteq C(a)$. First, let $x \in C(a)$. Then $xa = ax$. So

$$xaaa = (xa)aa = (ax)aa = a(xa)a = a(ax)a = aa(xa) = aa(ax) = aaax.$$

Hence $xa^3 = a^3x$ and $x \in C(a^3)$.

Now let $x \in C(a^3)$. Then $xa^3 = a^3x$. Notice that $(a^3)^2 = a^6 = (a^5)a = a$. Hence

$$xa = xa^6 = (xa^3)(a^3) = (a^3x)a^3 = a^3(a^3x) = a^6x = ax.$$

Hence $x \in C(a)$.

- (b) Find an example of a group G and an element $a \in G$ such that $|a| = 6$ and $C(a) \neq C(a^3)$.

Let $G = D_6$. This group has two elements of order 6. One is R_{60} . Let us find $C(R_{60})$ and $C(R_{60}^3)$.

First R_{60} commutes with all the other rotations as we observed in class. It does not commute with any of the six reflections though. This is because you can easily check that $\sigma R_{60} \sigma = R_{300}$ for any reflection σ . Hence

$$C(R_{60}) = \{e, R_{60}, R_{120}, R_{180}, R_{240}, R_{300}\}.$$

Notice that $R_{60}^3 = R_{180}$. This still commutes with all the rotations. It also commutes with all the reflections, which has to do with the fact that rotating by 180° clockwise or counterclockwise are the same. Hence $C(R_{60}^3) = D_6$.

4. (20 pts)

(a) Let G be a group. Give the definition of a subgroup of G .

A subgroup of G is a subset $H \subseteq G$ which is a group with respect to the operation of G .

(b) Prove that $H \subseteq G$ is a subgroup of G if and only if H is nonempty and

(i) $xy \in H$ for all $x, y \in H$,

(ii) $x^{-1} \in H$ for all $x \in H$.

Suppose $H \subseteq G$ is nonempty and satisfies these two conditions. Since H is nonempty, we can pick an $x \in H$. By the second condition, $x^{-1} \in H$ and by the first $e = xx^{-1} \in H$. So H has an identity. Let $x, y, z \in H$ be any elements. Then $x, y, z \in G$. By associativity of the operation of G , we have $(xy)z = x(yz)$. Therefore the operation of G is also associative on H . Finally, the two conditions give closure of H under the group operation and under inverses. Hence H is a group under the operation of G .

Conversely, let $H \subseteq G$ be a group under the operation of G . Then H is nonempty because it contains an identity. Closure under the group operation and under inverses immediately yield the two conditions.

(c) Let G be a group and H, K subgroups of G . Is $H \cap K$ also a subgroup of G ? If it is, prove it is, if not, give a counterexample.

First, notice that $H \cap K \subseteq G$. Now $e \in H$ and $e \in K$ since they are both subgroups, hence $e \in H \cap K$. Now let $x, y \in H \cap K$. Then $x, y \in H$ and $x, y \in K$. Since H and K are subgroups, $xy^{-1} \in H$ and $xy^{-1} \in K$. Hence $xy^{-1} \in H \cap K$. By the one-step subgroup test, $H \cap K$ is a subgroup of G .

(d) Let G be a group and H, K subgroups of G . Is $H \cup K$ also a subgroup of G ? If it is, prove it is, if not, give a counterexample.

$H \cup K$ is not in general a subgroup of G . For example, let $G = \mathbb{Z}_6$, $H = \{\bar{0}, \bar{3}\}$ and $K = \{\bar{0}, \bar{2}, \bar{4}\}$. These are clearly subgroups of \mathbb{Z}_6 . But

$$H \cup K = \{\bar{0}, \bar{2}, \bar{3}, \bar{4}\}$$

is not a subgroup because it is not closed under addition. For example, $\bar{2} + \bar{3} = \bar{5}$ is not in $H \cup K$.

Incidentally, you can also tell that $H \cup K$ cannot possibly be a subgroup because its order is 4 and $4 \nmid 6$.

5. (10 pts) Let S, T and U be nonempty sets. Let $f : S \rightarrow T$ and $g : T \rightarrow U$ maps. Prove the following.

(a) If $g \circ f$ is one-to-one then f is one-to-one.

Suppose f is not one-to-one. Then there exist $x \neq y$ in S such that $f(x) = f(y)$. Hence $g(f(x)) = g(f(y))$. This shows $g \circ f$ is not one-to-one. We have just proved the contrapositive of the statement.

- (b) Give an example of maps f and g (including domains and codomains!) such that $g \circ f$ is one-to-one, but g is not.

Let $f : \mathbb{R}^{\geq 0} \rightarrow \mathbb{R}$ be $f(x) = x$ and let $g : \mathbb{R} \rightarrow \mathbb{R}$ be $g(x) = x^2$. Clearly, g is not one-to-one. For example $g(-1) = g(1)$. Now $g \circ f : \mathbb{R}^{\geq 0} \rightarrow \mathbb{R}$ is $g \circ f(x) = x^2$. This is one-to-one because if $x \neq y$ are nonnegative numbers then their squares are different.

6. (10 pts) Let G be an infinite cyclic group. Suppose that a and b are both generators of G .

- (a) Prove that either $a = b$ or $a = b^{-1}$.

Since a generates G , $b = a^k$ for some $k \in \mathbb{Z}$. But b also generates G , so $a = b^n$ for some $n \in \mathbb{Z}$. Hence

$$a = b^n = (a^k)^n = a^{kn}.$$

This implies $e = aa^{-1} = a^{kn}a^{-1} = a^{kn-1}$. Since $k, n \in \mathbb{Z}$, $kn - 1 \in \mathbb{Z}$. If $kn - 1 > 0$ then $|a| \leq kn - 1$. This cannot be as a is the generator of an infinite cyclic group, hence $|a| = \infty$. If $kn - 1 < 0$, take inverses of both sides of the equation. We can do this because inverses in a group are unique. So $e = a^{1-kn}$. But $1 - kn > 0$, so this again says that a has finite order, which is a contradiction. Therefore the only possibility is that $kn - 1 = 0$. Hence $kn = 1$. Since $k, n \in \mathbb{Z}$, this can happen only if $k = n = \pm 1$. That is $a = b^{\pm 1}$.

- (b) What does the result in (a) tell you about the number of generators in an infinite cyclic group?

It suggests that an infinite cyclic group has exactly two generators. If a is a generator, so is a^{-1} , as the set of powers of a and the set of powers of a^{-1} are the same. But $a \neq a^{-1}$, otherwise $a^2 = aa = aa^{-1} = e$, which contradicts the infinity of the group. Any other generator must be equal to a or a^{-1} . Hence there are no other generators, but a and a^{-1} .

7. (10 pts each) **Extra credit problem.**

- (a) Let G be a group in which $x^2 = e$ for all $x \in G$. Prove that G is abelian.

Let $x, y \in G$. Then $e = (xy)^2 = xyxy$. Multiply on the left by x and on the right by y to get

$$xey = x(xyxy)y = x^2yxy^2 = yx.$$

So $xy = yx$ for any $x, y \in G$, hence G is abelian.

- (b) Let $*$ be an associative operation on a nonempty set S . Suppose that

$$x * x * y = y = y * x * x \quad \forall x, y \in S.$$

Prove that S is a group under $*$. Is this group abelian?

Fix $x \in S$ and let y run through all the elements of S . Since $(x * x) * y = y = y * (x * x)$ for all $y \in S$, $x * x$ acts as an identity. So S has an identity e . In fact, for any $x \in S$, $x * x = e$, so x is its own inverse. We already know $*$ is an operation on S and it is associative, so S is a group under $*$.

Notice that $x^2 = e$ for any $x \in S$, so by the previous problem, S is abelian.