Dr. Martin Olbermann
September 25, 2007

Math 113, Section 4
Fall 2007

Midterm Exam 1 - Solutions

1. Give a (detailed) definition of a group. (8 points)

Solution: (This is the most important definition so far. You have to know it!)
A group $\langle G, * \rangle$ is a binary algebraic structure, i.e. a set G together with a map $* : G \times G \to G$, $(a, b) \mapsto a * b$, that has the following three properties:
G_1: Associativity of $*$: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
G_2: There is an identity element for $*$, i.e. an element $e \in G$ s.t. $e * x = x * e = x$ for all $x \in G$.
G_3: Each element has an inverse, i.e. for each $a \in G$ there is an element $a' \in G$ s.t. $a * a' = a' * a = e$.

2. For each of the following statements indicate whether it is true or false. (7 points)

If the binary operation $*$ on a set S is commutative, then
$a * (b * c) = (b * c) * a$ for all $a, b, c \in S$.

TRUE (since the commutative law allows to exchange $(b * c)$ and a)

If the binary operation $*$ on a set S is associative, then
$a * (b * c) = (b * c) * a$ for all $a, b, c \in S$.

FALSE (the associative law only allows to put brackets at other places, but here the order of the variables has changed)

There exists a group G and elements $a, b, c \in G$
such that $a \neq c$, but $ab = cb$.

FALSE (in a group one has cancellation laws, so one can cancel b on both sides in $ab = cb$)

If two groups have the same number of elements, they are isomorphic.

FALSE (you have seen examples of this: e.g. $\mathbb{Z}_4$ and the four-group V both have four elements, but they are not isomorphic since in V, each element is the inverse to itself, and in $\mathbb{Z}_4$ not)

In every group, the identity element is the only element of order 1.

TRUE (the subgroup contained by $a \in G$ contains always a and $a^0 = e$; if the subgroup contained by a has 1 element, then $a = e$; on the other hand e generates the subgroup $\{e\}$)

Every abelian group is cyclic.

FALSE (e.g. V is abelian but not cyclic. It is true that every cyclic group is abelian.)

If a is an element of a group of order 4, then a^2 has order 2.

TRUE or FALSE (oops - there were two interpretations of that statement, so no matter what you wrote, you got a point for that)
1) if $a \in G$ and a has order 4, then a^2 has order 2. This is TRUE since if a has order 4, then 4 is the smallest positive exponent m s.t. $a^m = e$. Then 2 is the smallest positive exponent s.t. $(a^2)^m = e$, so a^2 has order 2.
2) if $a \in G$ and G has order 4, then it is possible that $a = e$, so $a^2 = e$ has order 1, so the statement is FALSE.)

3. (4 + 4 points)

a) Let $U = \{z \in \mathbb{C} \mid |z| = 1\}$. Show that the relation $\sim$ on U, defined by

$$x \sim y \text{ if and only if } x^n = y^n$$

is an equivalence relation.

Solution: For all $x, y, z \in U$:
$x^n = x^n \Rightarrow x \sim x$ so the relation is reflexive.
if $x \sim y$, then $x^n = y^n$, so $y^n = x^n \Rightarrow y \sim x$, so the relation is symmetric,
if $x \sim y$ and if $y \sim z$, then $x^n = y^n = z^n$, so $x \sim z$, i.e. the relation is transitive. Thus it is an equivalence relation.

b) Show that each equivalence class (cell of the corresponding partition) of the equivalence relation in **a)** is a set of cardinality n.

Solution: Let $x \in U$. We show that the equivalence class which contains x has cardinality n, i.e. that the set $S = \{y \in U \mid y \sim x\}$ has exactly n elements.
$S = \{y \in U \mid y^n = x^n\}$. $x^n \in U$, so let $x^n = e^{i\phi}$, where $0 \le \phi < 2\pi$. We solve the equation $y^n = e^{i\phi}$ (say in $\mathbb{C}$): we must have $|y| = 1$ (thus all solutions in $\mathbb{C}$ are solutions in U), and if ψ is the polar angle of y, where $0 \le \psi < 2\pi$, we must have that $n\psi - \phi$ is a multiple of 2π. There are n possible values for ψ: $\phi/n, \phi/n + 2\pi/n, \ldots, \phi/n + (n-1) \cdot 2\pi/n$. Thus the equation $y^n = x^n$ has exactly n solutions in U, i.e. S has cardinality n.

4. (7 points)

Recall that $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ for $n \in \mathbb{Z}^+$ is a group under multiplication.
Find all subgroups of the group U_{70} and draw a subgroup diagram. (Lines of the diagram are allowed to cross each other.) Identify all subgroups that are equal to U_n for some n.

Solution: For $n \in \mathbb{Z}^+$, we have that U_n is a cyclic group of order n with generator $\zeta_n = e^{\frac{2\pi i}{n}}$. U_{70} is a cyclic group of order 70 with generator ζ_{70}. By the theorem about subgroups of finite cyclic groups we proved in class, the subgroups of U_{70} are the groups $\langle \zeta_{70}^d \rangle$, where d is a divisor of 70. The divisors of 70 are: $1, 2, 5, 7, 10, 14, 35, 70$. So we get subgroups $\langle \zeta_{70}^1 \rangle = U_{70}$, $\langle \zeta_{70}^2 \rangle = \langle \zeta_{35} \rangle = U_{35}$, since $\zeta_{70}^2 = \zeta_{35}$, $\langle \zeta_{70}^5 \rangle = U_{14}$, since $\zeta_{70}^5 = \zeta_{14}$, $\langle \zeta_{70}^7 \rangle = U_{10}$, since $\zeta_{70}^7 = \zeta_{10}$, $\langle \zeta_{70}^{10} \rangle = U_7$, $\langle \zeta_{70}^{14} \rangle = U_5$, $\langle \zeta_{70}^{35} \rangle = U_2$, $\langle \zeta_{70}^{70} \rangle = U_1$. The subgroup diagram is:

$$\begin{tikzcd}
& U_{70} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
U_{35} \arrow[d, dash] \arrow[dr, dash] & U_{14} \arrow[dl, dash] \arrow[dr, dash] & U_{10} \arrow[dl, dash] \arrow[d, dash] \\
U_7 \arrow[dr, dash] & U_5 \arrow[d, dash] & U_2 \arrow[dl, dash] \\
& U_1 &
\end{tikzcd}$$

5. (4 + 4 points)

a) Show that $\mathbb{Z}[\frac{1}{2}] = \{\frac{p}{q} \mid p \in \mathbb{Z}, q = 2^n \text{ for some } n \in \mathbb{Z}^+\}$ is a subgroup of $\mathbb{Q}$ under addition.

Solution: $\mathbb{Z}[\frac{1}{2}]$ is closed under addition since for all $p_1, p_2 \in \mathbb{Z}$, $n_1, n_2 \in \mathbb{Z}^+$, we have

$$\frac{p_1}{2^{n_1}} + \frac{p_1}{2^{n_1}} = \frac{p_1 \cdot 2^{n_2} + p_2 \cdot 2^{n_1}}{2^{n_1+n_2}} \in \mathbb{Z}\left[\frac{1}{2}\right].$$

The identity element of $\mathbb{Q}$ is $0 = \frac{0}{2} \in H$. If $\frac{p}{2^n} \in \mathbb{Z}[\frac{1}{2}]$, where $p \in \mathbb{Z}$, $n \in \mathbb{Z}^+$, then its inverse in $\mathbb{Q}$ is $\frac{-p}{2^n} \in \mathbb{Z}[\frac{1}{2}]$. By the theorem about characterizing properties of subgroups we proved in class, $\mathbb{Z}[\frac{1}{2}]$ is a subgroup of $\mathbb{Q}$ under addition.

b) Show that $\mathbb{Z}[\frac{1}{2}]$ is not a finitely generated abelian group.

Solution: Let $S = \{a_1 = \frac{p_1}{2^{n_1}}, \ldots a_m = \frac{p_m}{2^{n_m}}\}$ be a finite subset of $\mathbb{Z}[\frac{1}{2}]$. The subgroup H generated by S consists (by transferring the theorem in class into the additive notation that we use here) of all finite sums of integer multiples of elements of S, that is $H = \{\lambda_1 a_1 + \ldots + \lambda_m a_m \mid \lambda_i \in \mathbb{Z}\}$. But all elements in this set are integer multiples of $q = \frac{1}{2^{n_1 + \cdots + n_m}}$. This implies that $\frac{q}{2} = \frac{1}{2^{n_1 + \cdots + n_m + 1}}$ is contained in $\mathbb{Z}[\frac{1}{2}]$, but not in H. It follows that no finite set S generates $\mathbb{Z}[\frac{1}{2}]$.

6. (4 + 4 + 4 points)

Let G be a group. An isomorphism $f : G \to G$ is called an **automorphism** of G. The set of all automorphisms of G is denoted by $Aut(G)$. It is a group under composition of functions (you do not have to prove this).

a) Show that there is an element $f \in Aut(\mathbb{Z}_8)$ (i.e. an isomorphism $f : \mathbb{Z}_8 \to \mathbb{Z}_8$) such that $f(1) = 5$.

Solution: (If such an isomorphism f exists, it must be bijective, and we must have $f(m +_8 n) = f(m) +_8 f(n)$ for all $m, n \in \mathbb{Z}_8$. So for example one must have $f(2) = f(1 +_8 1) = f(1) +_8 f(1) = 5 +_8 5 = 2$, and $f(3) = f(2 +_8 1) = \dots$ and so on. One may find the formula $f(n) = 5 +_8 \dots +_8 5$, with n summands, in that way. We also proved that an isomorphism sends identity element to identity element. So it must map 0 to 0.)

We have $gcd(5, 8) = 1$, so 5 is a generator for $\mathbb{Z}_8$, so $\mathbb{Z}_8$ consists of the elements $0, 5, 5 +_8 5, 5 +_8 5 +_8 5, \dots 5 +_8 5 +_8 5 +_8 5 +_8 5 +_8 5 +_8 5$. (The sum modulo 8 with 8 summands equal to 5 is 0.) The map $f : \mathbb{Z}_8 \to \mathbb{Z}_8$ defined by $f(n) = 5 +_8 \dots +_8 5$, with n summands, is an isomorphism. (It is obviously well-defined, surjective and injective. We have $f(m +_8 n) = f(m) +_8 f(n)$ for all $m, n \in \mathbb{Z}_8$ since the sum with 8 summands is 0, so the sum with $m +_8 n$ summands equals the sum with $m + n$ summands.)

One could also refer to the proof that every finite cyclic group $G = \langle a \rangle$ is isomorphic to $\mathbb{Z}_n$: the proof constructs an isomorphism $\mathbb{Z}_n \to G$ which sends $1 \in \mathbb{Z}_n$ to $a \in G$ (or the inverse isomorphism, to be exact). Now we put $G = \mathbb{Z}_8$, $a = 5$ and we are done.

b) What is the order of $Aut(\mathbb{Z}_8)$? (Justify your answer.)

Solution: As we have seen in part a) (or also in the last problem of homework 4:) For each $i \in \mathbb{Z}_8$, there exists at most one isomorphism f s.t. $f(1) = i$: because of the homomorphism property, one must have $f(n) = i +_8 \dots +_8 i$, with n summands.

Since $\mathbb{Z}_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$, we can do the same steps as in part **a)** to construct four isomorphisms f_1, f_3, f_5, f_7 such that $f_i(1) = i$, and they are given by $f_i(n) = i +_8 \dots +_8 i$, with n summands.

The candidates for an isomorphism $f_i(n) = i +_8 \dots +_8 i$, where $i = f_i(1)$ is even, do all send 0 to 0 and 4 to 0, so there are no isomorphisms where $f(1)$ is even. So $Aut(\mathbb{Z}_8) = \{f_1, f_3, f_5, f_7\}$, i.e. $Aut(\mathbb{Z}_8)$ has order 4.

c) Show that $Aut(\mathbb{Z}_8)$ is isomorphic to a group that you have seen in class.

Solution: We have seen in class that all groups of four elements are either isomorphic to $\mathbb{Z}_4$ or to the Klein 4-group V.

$f_1 = id$ is the identity function, i.e. the identity element of the group. But since $Aut(\mathbb{Z}_8)$ is a group, it is closed under composition, so we must have $f_3 \circ f_3 = f_i$ for some $i \in \{1, 3, 5, 7\}$. We compute $f_3(f_3(1)) = f_3(3) = 3 +_8 3 +_8 3 = 1$, so we must have $f_3 \circ f_3 = f_1$. But similarly, we compute that (we could compute the whole group table of $Aut(\mathbb{Z}_8)$) $f_1 \circ f_1 = f_3 \circ f_3 = f_5 \circ f_5 = f_7 \circ f_7 = f_1$, so each element of the group is its own inverse. Therefore the group $Aut(\mathbb{Z}_8)$ must be isomorphic to V (and not to $\mathbb{Z}_4$).