UMASS AMHERST MATH 411 SECTION 2, FALL 2009, F. HAJIR

HOMEWORK 2: DUE TH. OCT. 1

READINGS: These notes are intended as a SUPPLEMENT TO THE TEXTBOOK, NOT A REPLACEMENT FOR IT.

1. Elements of a group, their powers and their orders

Let $(G, *, e)$ be a group. For convenience, we will often write write ab instead of $a * b$. We will write a^{-1} for the inverse of a, which is okay because we have proved that the inverse is unique. Note that when the binary operation $*$ is addition $(+)$, the usual notation for the inverse of a is $-a$, not a^{-1}. Also, in that case, the identity element is usually 0.

Suppose $a, b \in G$. You should prove for yourself that: $(ab)^{-1} = b^{-1}a^{-1}$ and more generally, if $a_1, \ldots, a_n \in G$, $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$. We also recall that Generaralized Associativity follows from associativity, i.e. $a_1 \cdots a_n$ does not depend on how we parenthesize the product.

From now on, let G be a group and $a \in G$ an element of G.

For $a \in G$ and $n \in \mathbb{Z}$ we define a^n to be $aa \cdots a$ (product of n a's), if $n > 0$, e if $n = 0$, and $a^{-1} \cdots a^{-1}$ (product of $|n|$ a^{-1}s) if $n < 0$.

PROBLEM 1. For $a \in G$ and $m, n \in \mathbb{Z}$, prove that $a^n a^m = a^{n+m}$ and $(a^n)^m = a^{nm}$.

Hint: first do the case where either m or n is 0. Next do $m > 0, n > 0$. Now do the other cases.

Recall that the order of a in G is defined by

$$\mathrm{ord}_G(a) = \min\{m \geq 1 | a^m = e\}.$$

If $a^m \neq e$ for all $m \geq 1$, then we say that $\mathrm{ord}_G(a) = \infty$. In other words, $\mathrm{ord}_G(a)$ is the smallest positive exponent which "kills" a. [Note: you should think of the identity element as "dead", so a "killer" of x is something that renders x into the identity]. Note that a has order 1 if and only if $a = e$.

PROBLEM 2. List the elements of S_4 (as permutations) and find the order of each one in S_4. Note: S_4 has 24 elements.

Lemma 1.1. *If $(G, *, e)$ is a finite group (i.e. G is a finite set, i.e. it has only finitely many elements), and $a \in G$, then $\mathrm{ord}_G(a) < \infty$.*

Proof. Consider the set $\{a^m | m \geq 1\}$. This is a subset of G (why?), hence must be finite. Thus, $a, a^2, a^3, \ldots$ cannot all be pairwise distinct. Thus, there exist integers $1 \leq i < j$ such that $a^i = a^j$. Let us write $j = i + r$ with $r \geq 1$. Then $a^i = a^{i+r} = a^i a^r$. Therefore $e = a^r$ (why?). Thus, $\mathrm{ord}_G(a) \leq r < \infty$. $\square$

PROBLEM 3. Prove: If $a \in G$ has finite order $k = \mathrm{ord}_G(a)$, then $a, a^2, a^3, \ldots, a^{k-1}, a^k$ are all distinct.

Hint: suppose not; then $a^i = a^{i+r}$ for some $i, r \geq 1$ (why?). Now derive an upper bound for r and obtain a contradiction to the minimality of k as "killer exponent" of a. If you have trouble, see Lemma 3.2 of these notes, but try it yourself first.

Recall some notation from number theory. If k, n are integers and $k \neq 0$, then we write $k|n$ (read: k divides n, or n is a multiple of k) if and only if $kt = n$ for some integer t. For example $1|n$ for all integers n, but $n|1$ implies that $n = \pm 1$. We have $n|0$ for every integer n because $n \cdot 0 = 0$.

NOTE: THE FOLLOWING RESULT IS VERY USEFUL AND IMPORTANT.

Lemma 1.2. *Suppose $a \in G$ has finite order $k = \mathrm{ord}_G(a)$. If $a^n = e$ for some $n \in \mathbb{Z}$, then $k|n$. In fact, for $n \in \mathbb{Z}$, $a^n = e$ if and only $k|n$. In other words,*

the killer exponents of a are exactly the integer multiples of $\mathrm{ord}_G(a)$.

Proof. By the Euclidean (or division) algorithm, there exist integers q, r such that

$$n = qk + r, \qquad 0 \leq r \leq k - 1.$$

In fact, a pair of integers (n, k) with $k \neq 0$, uniquely determines integers (q, r) with $0 \leq r \leq |k| - 1$ such that $n = qk + r$. Here is one way to see this. Let's assume $n, k > 0$ for convenience. The other cases easily follow from this anyway. For every real number x, we can write $x = [x] + \langle x \rangle$ where $[x]$ is the largest integer not greater than x and $0 \leq \langle x \rangle < 1$. Sometimes $[x]$ is called the integral part (or *floor*) of x and $\langle x \rangle$ is its fractional part. Returning to $n = kq + r$, we simply take $x = n/k \in \mathbb{R}$ and write $q = [n/k]$; then $\langle n/k \rangle = n/k - q = r/k$ for a unique integer r in the range $0 \leq r \leq k-1$. For more details, you may consult Theorem 1.26 in the book, for example.

Now, recall $k = \mathrm{ord}_G(a) \geq 1$ and suppose $n \in \mathbb{Z}$. Writing $n = kq + r$, with $0 \leq r \leq k - 1$, we have $a^n = a^{kq+r} = a^{kq}a^r$ by PROBLEM 1. Thus $a^n = (a^k)^q a^r = e^q a^r = a^r$. If we assume $a^n = e$, then $a^r = e$; but $0 \leq r \leq k - 1 < \mathrm{ord}_G(a)$. By the definition of $\mathrm{ord}_G(a)$, $a, a^2, \cdots, a^{k-1}$ are all distinct from e. Hence, we must have $r = 0$. Thus, $a^n = e$ implies that $n = kq$ i.e. $k|n$. On the other hand, if $k|n$, i.e. $kq = n$, then $a^n = (a^k)^q = e^q = e$. □

PROBLEM 4. a) What is the order of 5 in $(\mathbb{Z}, +)$?

b) The group of non-zero real numbers under multiplication is denoted by $\mathbb{R}^\times$. What are the elements of order 2 in $\mathbb{R}^\times$? [First make sure you understand who the identity of this group is].

c) Are there any elements of order 3 in $\mathbb{R}^\times$?

PROBLEM 5. Prove that if G is a group and $a \in G$, then $\mathrm{ord}_G(a) = \mathrm{ord}_G(a^{-1})$. Be sure to include the case where $\mathrm{ord}_G(a)$ is infinite.

PROBLEM 6. Suppose G is a group and $g \in G$ has order $m = pn$ where p is a prime number and n is a positive integer. Let $h = g^n$. Show that h has order p in G.

2. Homomorphisms, Isomorphisms, and Subgroups

Definition 2.1. Suppose $(G_1, *_1, e_1)$ and $(G_2, *_2, e_2)$ are groups, and $f : G_1 \to G_2$ is a map. We say that f is a *group homomorphism* (usually *homomorphism* for short) if

$$f(a *_1 b) = f(a) *_2 f(b) \qquad \text{for all } a, b \in G_1.$$

In other words, f carries the product of two elments in G_1 to the product of their images in G_2; we say that f *respects* the groups laws of G_1 and G_2.

Example 2.2. We will define a group $V = \{e, a, b, c\}$ as follows. Let S be a square whose sides (edges) are labelled $\{1, 2, 3, 4\}$ with $1, 2$ forming one pair of opposite edges and $3, 4$ forming the other pair. Let a be the reflection of the square across the line that bisects edges $3, 4$. Let b be the reflection of the square across the line that bisets $1, 2$. And let c be the rotation by 180 degrees of the square about is center (where the diagonals meet). Together with the identity symmetry (do nothing!), these 4 symmetries of the square form a group, under composition of functions (which is always associative as we saw last time). Spend a moment to verify that this is the case. Now we will define a map $\sigma : V \to S_4$ which is a group homomorphism, namely each element of V permutes the edges thus gives rise to an element of S_4 since we have labelled the edges with the integers $1, 2, 3, 4$. Thus,

$$e \mapsto \sigma(e) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, a \mapsto \sigma(a) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix},$$

$$b \mapsto \sigma(b) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, c \mapsto \sigma(c) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

In order to check that this is indeed a homomorphism, we would have to verify $\sigma(xy) = \sigma(x)\sigma(y)$ for all pairs $(x, y) \in V \times V$. Note that there are 16 such pairs. In general, if G_1 is a finite group of order N, then to say that $f : G_1 \to G_2$ is a homomorphism is to summarize in one breath N^2 different equalities! Thus, being a homomorphism is a *strong* condition.

A homomorphism $f : G_1 \to G_2$ is called *trivial* if $f(g_1) = e_2$ for all $g_1 \in G_1$. You should check that this is indeed a homomorphism. Philosophically speaking, whenever there is a non-trival homomorphism from a group G_1 to a group G_2, then in some sense "a piece" of G_1 (called a *quotient* of G_1) is "identical" to "a piece" of G_2 (called a *subgroup* of G_2). This will be made precise later in the form of several "Isomorphism Theorems."

Lemma 2.3. *If $f : G_1 \to G_2$ is a homomorphism, then $f(e_1) = e_2$, and $f(g^n) = f(g)^n$ for all $g \in G$, and all $n \in \mathbb{Z}$. In particular, $f(g^{-1}) = f(g)^{-1}$.*

Proof. For example, $f(e_1 *_1 e_1) = f(e_1) *_2 f(e_1) = f(e_1)$. Now use the cancellation law (or multiply by $f(e_1)^{-1}$) to get $f(e_1) = e_2$. Now $f(g) *_2 f(g^{-1}) = f(g *_1 g^{-1}) = f(e_1) = e_2$ and similarly for $f(g^{-1})f(g)$. Hence, $f(g^{-1})$ fulfills the role of inverse for $f(g)$ in G_2. By the uniqueness of inverses, $f(g^{-1}) = f(g)^{-1}$. The other cases left to reader, or look in book, Lemma 2.36. $\square$

Recall the group V from the example above. Under the map σ, it maps to the following group $W = \{E, A, B, C\}$ where

$$E = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, C = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

If you write the group tables for V and W, you will have a *dejà vu* feeling. You'll see that you're just writing the same group twice, the only difference being that the group elements have slightly different names. We say that the groups are *isomorphic*, the exact definition is to follow.

Definition 2.4. Suppose G_1, G_2 are groups. A map $f : G_1 \to G_2$ is called a *group isomorphism* (isomorphism for short) if 1) f is a homomorphism , and 2) f is bijective.

When we study sets, we feel that two sets "have the same structure" if we can set up a one-to-one-correspondence between them (i.e. a bijection). Now a group is a set carrying the additional structure of a composition law (verifying certain special properties). We feel that two groups "have the same structure" if we can set up a one-to-one-correspondence between the underlying sets (i.e. a bijection) which, additionally, "respects" the law of composition (i.e. is a homomorphism).

Definition 2.5. An *automorphism* of a group G is an isomrphism $f : G \to G$. The identity map from a group to itself is the trivial automorphism. The set of all automorphisms from G to itself is called $\mathrm{Aut}_{\mathrm{gp}}(G)$.

PROBLEM 7. Suppose G is a group. Consider the map $\iota : G \to G$ which sends $a \mapsto a^{-1}$. Prove or disprove: ι is always an automorphism of G. If this is false, can you think of a general condition on G under which it becomes true?

PROBLEM 8. Suppose $(G_1, *_1, e_1)$ and $(G_2, *_2, e_2)$ are groups, and $f : G_1 \to G_2$ is an isomorphism. Since f is a bijection, an inverse function $f^{-1} : G_2 \to G_1$ exists and is unique. Prove that f^{-1} is an isomorphism.

Definition 2.6. Suppose $(G, *, e)$ is a group and $H \subseteq G$ is a subset of G. We say that H is a *subgroup of* G if

i) $h_1, h_2 \in H$ implies that $h_1 * h_2 \in H$ ("closure")
ii) $e \in H$ ("identity")
iii) for all $h \in H$, $h^{-1} \in H$ ("inverse").

Let us interpret this definition in the following way: i) says that when we restrict the binary operation from G to H, we obtain not just a map $H \times H \to G$ but $H \times H \to H$. In other words, restricting the operation to elements of H yields a binary operation on H! Properties ii) and iii) then simply say that this binary operation of H obtained by restricting the law of composition of G to H makes H into a group. We often write $H \leq G$ as shorthand notation for H is a subgroup of G. Every group G has two God-given subgroups, namely, $\{e\}$ the subgroup consisting of the identity alone, and G itself. A subgroup $H \leq G$ is called *non-trivial* if $H \neq \{e\}$, and it is *proper* if $H \neq G$.

Example. The group $GL_2(\mathbb{Q})$ consists of two-by-two matrices with rational entries having non-zero determinant, under matrix multiplication. It is a subgroup of $GL_2(\mathbb{R})$. [check that this is so].

Definition 2.7. If $f : G_1 \to G_2$ is a homomorphism, then

$$\ker(f) = \{g_1 \in G_1 | f(g_1) = e_2\}, \qquad \mathrm{Im}(f) = \{g_2 \in G_2 | g_2 = f(g_1) \text{ for some } g_1 \in G_1\}.$$

Lemma 2.8. *If $f : G_1 \to G_2$ is a homomorphism, then* $\ker(f)$ *is a subgroup of G_1 and* $\mathrm{Im}(f)$ *is a subgroup of G_2.*

Proof. This is very easy if you keep in mind that $f(g^{-1}) = f(g)^{-1}$ and $f(e_1) = e_2$. □

PROBLEM 9. i) Verify that The set $SL_2(\mathbb{R})$ consisting of two-by-two real-entry matrices having determinant 1 is a subgroup of $GL_2(\mathbb{R})$.

ii) Recall the group $\mathbb{R}^\times$ consisting of non-zero numbers under multiplication. Now the determinant gives us a map

$$\det : GL_2(\mathbb{R}) \longrightarrow \mathbb{R}^\times,$$

sending a matrix A to $\det A$. Is this a group homomorphism? Prove your answer is correct.

iii) Is $\det : GL_2(\mathbb{R}) \longrightarrow \mathbb{R}^\times$ surjective? Is it injective? Justify your answers.

iv) What is $\ker(\det)$?

v) Now reprove i) in an easy way using iv).

PROBLEM 10. Prove that a homomorphism is injective if and only if its kernel is trivial.

3. Subgroup generated by an element

Definition 3.1. If $a \in G$, $< a >= \{a^n | n \in \mathbb{Z}\}$ is called the subgroup generated by a.

To check that it is indeed a subgroup, all we need, really, is apply PROBLEM 1: $a^{m+n} = a^m a^n$.

Lemma 3.2. *For $a \in G$, $| < a > | = \mathrm{ord}_G(a)$, i.e. the cardinality of the subgroup generated by a coincides with the order of a in G.*

Proof. If a has infinite order, then by definition, $a^m \neq e$ for all $m \geq 1$. I claim that $a, a^2, a^3, \cdots$ are all pairwise distinct. Otherwise, $a^i = a^{i+r}$ for some integers $i, r \geq 1$. By the cancellation law, we then would have $e = a^r$ and recall that $r \geq 1$. Thus, a has finite order, a contradiction. Thus, $a, a^2, a^3, \ldots$ are all distinct, thus, $| < a > | = \infty$. If a has finite order, then this lemma is proved in the proof of Prop 2.28 in the book, but here is the argument again. Say $\mathrm{ord}_G(a) = k < \infty$. Then $a^i \neq a^j$ for $1 \leq i < j \leq k$. Otherwise, $a^i = a^j = a^{i+r}$ with $j = i + r$ and $i, r \geq 1$. Since $j = i + r \leq k$ and $i \geq 1$, we have $1 \leq r \leq k - 1$. But $a^r = 1$ and $1 \leq r \leq k - 1$ contradict the fact that $k = \mathrm{ord}_G(a)$ is the minimal exponent "killing" a. Thus, $a, a^2, \cdots, a_k$ are all distinct. Note tat there are k of them. On the other hand, $a^{k+1} = a$ and in general, $a^t = a^i$ where i is the remainder when t is divided by k. We have shown that $| < a > | = k$. □

PROBLEM 11. [**EXTRA CREDIT**] Show that a finite group of even order must contain an element of order 2. [Hint: one way to proceed (there are many) would be to show that there is an element of even order; why would that practically clinch it?]

4. Tune in next week for ...

If G is a finite group and H is a subgroup of G, we know that $|H| \leq |G|$ just because H is a subset of G. But it turns out that: `DRUMROLL PLEASE`

Our TARGET THEOREM for the near future: If G is a finite group and H is a subgroup of it, then $|H|$ divides $|G|$. (Lagrange's Theorem).

In order to do this, we will introduce *cosets*, and review *equivalence classes*.