UMASS AMHERST MATH 411 SECTION 2, FALL 2004, F. HAJIR

HOMEWORK 2: SELECTED SOLUTIONS

These are sketches of solutions to some of the problems from HW 2, provided as a courtesy to help you with studying for Exam 1.

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

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

If either n or m is 0, it's cake. Now suppose $m > 0, n > 0$. Then $(a^n)^m = a^n \cdots a^n$ (m copies), hence by generalized associativity, this is just nm copies of a composed together, i.e. it is a^{nm}. Now we note that when either m or n is -1, we also win easily. Namely,

Claim. If $k \geq 0$, $(a^{-1})^k = (a^k)^{-1} = a^{-k}$. Proof of Claim: First note that by definition, $a^{-k} = (a^{-1})^k$. Now, recall that $(a_1 \cdots a_k)^{-1} = a_k^{-1} \cdots a_1^{-1}$, hence

$$(a^k)^{-1} = (a \cdots a)^{-1} = a^{-1} \cdots a^{-1} = (a^{-1})^k = a^{-k}.$$

Now suppose $n < 0, m > 0$. Write $n = -N$. Then, by the claim,

$$(a^n)^m = (a^{-1} \cdots a^{-1})^m = (a^{-1})^{Nm} = a^{-Nm} = a^{nm}.$$

If $m < 0, n < 0$, then we write $n = -N, m = -M$. Then by the argument we just gave,

$$(a^n)^m = (a^{-N})^{-M} = (a^{-(-N)})^M = a^{NM} = a^{nm}.$$

The proof for $a^m a^n = a^{m+n}$ is similar (and easier in a sense).

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.

Left to reader. You should be very good at composing permutations for the exam.

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.

Suppose not; then two distinct powers of a in the given range coincide, i.e. $a^i = a^j$ for some $1 \leq i < j \leq k$. Letting $j = i + r$ with $r \geq 1$, we have $a^i = a^{i+r}$ with $i, r \geq 1$. Now $r = j - i < k$ since $j \leq k$ and $i \geq 1$. Multiplying by a^{-i}, or using the cancellation law, we get $e = a^r$ with $1 \leq r < k$. This contradicts the fact that k is the order of a (the **least** killer exponent). We have arrived at the desired contradiction. Thus, $a, \cdots, a^k$ are all distinct elements of G.

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

Infinity, since a non-trivial sum of 5's is never 0 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].

Here $e = 1$, so we must solve $x^2 = 1$. We then have $x^2 - 1 = (x-1)(x+1) = 0$ giving us $x = \pm 1$. Since 1 has order 1, the only element of order 2 is -1.

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

No, because $x^3 = 1$ has only 1 solution namely $x = 1$ in $\mathbb{R}$. The graph of $f(x) = x^3 - 1$ hits the real line only once by calculus considerations.

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.

By Problem 1, for any integer $j \geq 1$, $(a^j)^{-1} = (a^{-1})^j$. Therefore, $a^j = e$ if and only if $(a^j)^{-1} = e^{-1}$ which is true if and only if $(a^{-1})^j = e$. In other words, the killer exponents of a are exactly the killer exponents of a^{-1}. Thus, the order of a is the order of a^{-1} whether a has finite order or not.

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.

First of all, $h^p = (g^n)^p = g^{np}$ by Problem 1. But $g^{np} = e$ since np is the order of g. Thus, $h^p = e$. Now by the Very Useful Lemma, the order of h divides p. But p is a prime, so its only positive divisors are 1 and p. Since $h^1 = h = g^n$ and $n < np$ (recall that $p > 1$), g^n cannot be e (since np is the least killer exponent of g). Thus $h = g^n \neq e$. Since h doesn't have order 1, it must have order p.

2. Homomorphisms, Isomorphisms, and Subgroups

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?

First of all, ι is always bijective because it is its own inverse: $\iota(\iota(g)) = (g^{-1})^{-1} = g$. To be a homomorphism, we have to check: is it true that $\iota(xy) = \iota(x)\iota(y)$ for all $x, y \in G$? On the left hand side, we have $(xy)^{-1}$ which is $y^{-1}x^{-1}$. On the right hand side, we have $\iota(x)\iota(y) = x^{-1}y^{-1}$ so we are asking if $y^{-1}x^{-1} = x^{-1}y^{-1}$? for all x, y. This is true if and only if $ab = ba$ for all $a, b \in G$. Thus, ι is a homomorphism if and only if G is a commutative group.

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.

By a previous hw problem (HW 1), f^{-1} is bijective. We just have to show that f^{-1} is a homomorphism. I gave one proof in class. Here is another. We must prove for $x_2, y_2, \in G$ that $f^{-1}(x_2y_2) = f^{-1}(x_2)f^{-1}(y_2)$. Well, let $a = f^{-1}(x_2y_2)$ and $b = f^{-1}(x_2)f^{-1}(y_2)$. Then, $a, b \in G_1$. Since f is injective, we have $a = b$ if and only if $f(a) = f(b)$. But $f(a) = f(f^{-1}(x_2y_2)) = x_2y_2$ and

$$f(b) = f(f^{-1}(x_2)f^{-1}(y_2)) = f(f^{-1}(x_2))f(f^{-1}(y_2)) = x_2y_2$$

since f is a homomorphism. Thus, $f(a) = f(b)$, and since f is injective it follows that $a = b$.

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).

We went over this in class.

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

Suppose $f : G_1 \to G_2$ is a group homorphism. First suppose $\ker(f) = \{e_1\}$. We must show that f is injective. Suppose $x, y \in G_1$ and $f(x) = f(y)$. Let's call this common value $z = f(x) = f(y)$. Then

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = zz^{-1} = e_2.$$

Thus, $xy^{-1} \in \ker(f)$. Hence $xy^{-1} = e$, i.e. $x = y$. We have shown that f is injective.

Now suppose f is injective. Then there is at most one element $x \in G_1$ such that $f(x) = e_2$. On the other hand, $f(e_1) = e_2$ since f is a homomorphism. Therefore $\ker(f) = \{e_1\}$.