MATH1530, HOMEWORK 5

Showing that Two Given Groups are Isomorphic

There have been many exercises in which we were asked to show that two given groups A and B are isomorphic. In most cases, one of them (say A) is a known group, like S_3, D_8, Q_8, $\mathbb{Z}/n\mathbb{Z}$, etc, and B is a less-understood one. Exercise 14 of page 72, Exercise 26 of page 41, and Exercise 7 of page 65 are some problems of this type.

The following strategy is quite useful: First, pick your favorite presentation of the group A. For example,

$$D_{2n} =< r, s \,:\, r^n = s^2 = 1, rs = sr^{-1} >,$$

$$Q_8 =< i, j \,:\, i^4 = 1, i^2 = j^2, j^{-1}ij = i^{-1} >,$$

,

$$S_n =< \sigma_1, ..., \sigma_{n-1} \,:\, \sigma_i^2 = 1, \sigma_i\sigma_j = \sigma_j\sigma_i \text{ if } \; j \neq i \pm 1, \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} >,$$

and

$$\mathbb{Z}/n\mathbb{Z} =< x \,:\, x^n = 1 > .$$

You can look them up on the web page http://en.wikipedia.org/wiki/Presentation_of_a_group.

Next, find elements of the other group B that satisfy the corresponding relations as the generators for A do. That is, if you want to show B is isomorphic to D_{2n}, you need to find two elements $a, b \in B$ such that $a^n = b^2 = 1$ and $ab = ba^{-1}$.

Once you have found such elements, it directly implies that there is a surjective homomorphism $\phi : A \to B$. (Proof?) To finish the argument, you want to show ϕ is also injective. This can be usually done by showing that B has as many elements as A has. In particular, if B is a quotient group $B = G/H$, $|B| = |G|/|H|$ if G is finite. In addition, existence of such a homomorphism enables us to identify B as a subgroup of A and hence we can use Lagrange's theorem. For example, if $D_{2n} = A$ and once we have found ϕ, it is enough to "present" five distinct elements of B by Lagrange's theorem to show that they are isomorphic.

In this problem set, this strategy will be used in Exercise 18 and Exercise 34.

Section 3.1

1. Let $\phi : G \to H$ be a homomorphism and let E be a subgroup of H. Prove that $\phi^{-1}(E) \leq G$. If $E \trianglelefteq H$ prove that $\phi^{-1}(E) \trianglelefteq G$. Deduce that $\ker\phi \trianglelefteq G$.

Let $a, b \in \phi^{-1}(E)$. It means there exist elements $x, y \in E$ such that $\phi(a) = x$ and $\phi(b) = y$. Then $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = xy^{-1} \in E$ since E is a subgroup. This means $ab^{-1} \in \phi^{-1}(E)$, which shows that $\phi^{-1}(E)$ is a subgroup of G. If E is a normal subgroup, consider gag^{-1} where g is any element of G and $a \in \phi^{-1}(E)$. Then $\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g)^{-1} \in E$, since $\phi(a) \in E$ and E is a normal subgroup. That is, $gag^{-1} \in \phi^{-1}(E)$ and $\phi^{-1}(E)$ is a normal subgroup.

Finally, the single-element group $\{e\}$ is normal in any group, and hence $\ker\phi = \phi^{-1}(\{e\})$ is normal in G.

3. Let A be an abelian group and let B be a subgroup of A. Prove that A/B is abelian. Given an example of a non-abelian group G containing a proper normal subgroup N such that G/N is abelian.

Given two elements aB and bB of A/B, group operation $\circ$ on A/B is defined by $aB \circ bB := (ab)B$. However, $ab = ba$ so $(ab)B = (ba)B$ which means $aB \circ bB = bB \circ aB$.

For an example take $G = S_3$ which is the smallest non-abelian group. If we consider the subgroup generated by a 3-cycle, namely $K = \{1, (123), (132)\}$, it is normal, (since its index is 2) and G/K is abelian since it has only two elements.

Or you can show that K is normal directly, by computing $(12)K(12)^{-1}$, $(13)K(13)^{-1}$, and $(23)K(23)^{-1}$. (but by an apparent symmetry, it is enough to check one of these)

4. In G/N show that $(gN)^\alpha = g^\alpha N$ for all $\alpha \in \mathbb{Z}$.

When $\alpha = 0$, the left hand side is the identity of G/N which is $1N = N$, and the right hand side is $g^0 N = 1N = N$. This is clear when $\alpha = 1$, and $(gN) \circ (g^{-1}N) = (gg^{-1})N = 1N = N$, which means $(gN)^{-1} = g^{-1}N$. Therefore this statement is true for $\alpha = \pm 1$, and we can use induction in the positive direction and the negative direction.

Assume we know $(gN)^\alpha = g^\alpha N$ for $\alpha > 0$. Then $(gN)^{\alpha+1} = (gN)^\alpha (gN) = (g^\alpha N)(gN) = g^{\alpha+1}N$. When $\alpha < 0$, $(gN)^{\alpha-1} = (gN)^\alpha (gN)^{-1} = (g^\alpha N)(g^{-1}N) = g^{\alpha-1}N$.

9. Define $\phi : \mathbb{C}^\times \to \mathbb{R}^\times$ by $\phi(a + bi) = a^2 + b^2$. Prove that ϕ is a homomorphism and find the image of ϕ. Describe the kernel and the fibers of ϕ geometrically.

$\phi((a+bi)(c+di)) = \phi(ac-bd+(ad+bc)i) = (ac-bd)^2+(ad+bc)^2 = (ac)^2+(bd)^2+(ad)^2+(bc)^2 = (a^2+b^2)(c^2+d^2) = \phi(a+bi)\phi(c+di)$, so ϕ is a homomorphism. For any $a+bi$, $\phi(a+bi) = a^2+b^2 > 0$ (0 is not in the domain) and given any positive real r, $\phi(\sqrt{r}) = r$ so the image of ϕ is precisely the set of positive reals.

Identity of $\mathbb{R}^\times$ is 1, and hence the kernel is the set of complex numbers $a + bi$ satisfying $a^2 + b^2$. Given $r > 0$, we see that its fiber is a circle $\{(a + bi) : a^2 + b^2 = r\}$.

10. Let $\phi : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ by $\phi(\bar{a}) = \bar{a}$. Show that this is a well defined, surjective homomorphism and describe its fibers and kernel explicitly.

Why do we need to show this is well defined? It is because this map is defined in terms of $\bar{a}$, but this $\bar{a}$ in the domain means a modulo 8 while in the range means a modulo 4.

In the domain, we have $...\overline{a-8} = \overline{a} = \overline{a+8} = \overline{a+16}...$ so we must have $\phi(\overline{a-8}) = \phi(\overline{a}) = \phi(\overline{a+8}) = \phi(\overline{a+16})$ and so on, which is true since $8 = 0$ modulo 4.

Then $\phi(\bar{a} + \bar{b}) = \phi(\overline{a+b}) = \overline{a+b} = \bar{a} + \bar{b} = \phi(\bar{a}) + \phi(\bar{b})$ which shows it is a homomorphism. Surjectivity: $\bar{0} \mapsto \bar{0}$, $\bar{1} \mapsto \bar{1}$, $\bar{2} \mapsto \bar{2}$, and $\bar{3} \mapsto \bar{3}$. Kernel is $\{\bar{0}, \bar{4}\}$, which is also the fiber of $\bar{0} \in \mathbb{Z}/4\mathbb{Z}$. Likewise, $\{\bar{a}, \overline{a+4}\}$ is the fiber of $\bar{a} \in \mathbb{Z}/4\mathbb{Z}$.

18. Let G be the quasidihedral group of order 16:

$$G = <\sigma, \tau \,:\, \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3>$$

and let $\bar{G} = G/ <\sigma^4>$ be the quotient of G by the subgroup generated by σ^4.

(a) Show that the order of $\bar{G}$ is 8. We are quotienting out by the subgroup $<\sigma^4> = \{1, \sigma^4\}$. That is, the kernel of the projection $G \to \bar{G}$ has two elements $\{1, \sigma^4\}$, which is the fiber of $1 \in G/N$. Since each fiber has the same number of elements, $\bar{G}$ has order $16/2 = 8$.

(b) Exhibit each element of $\bar{G}$ in the form $\bar{\tau}^a\bar{\sigma}^b$, for some integers a and b. The claim is that every element has the form $\bar{\tau}^a\bar{\sigma}^b$ for $a \in \{0,1\}$ and $b \in \{0,1,2,3\}$. These 8 elements are certainly contained in $\bar{G}$, so it is enough to show that they are all distinct. If we set $\bar{\tau}^a\bar{\sigma}^b = \bar{\tau}^c\bar{\sigma}^d$, from cancellations we would get $\bar{\tau}^{a-c}\bar{\sigma}^{b-d} = 1$, where $|a-c| \le 1$, $|b-d| \le 3$. To argue that this cannot happen, we can use the fact that $\tau^{a-c}\sigma^{b-d} \neq 1$ in G. But $\bar{\tau}^{a-c}\bar{\sigma}^{b-d} = 1$ means $\tau^{a-c}\sigma^{b-d} \in \ker(G \to \bar{G}) = \{1, \sigma^4\}$ but $|b-d| \le 3$ forces $a = c$ and $b = d$.

Notice that here we are using a result that every element of G is uniquely represented by $\tau^a\sigma^b$ for $a \in \{0,1\}$ and $b \in \{0,1,2,3,4,5,6,7\}$.

(c) Find the order of each of the elements of $\bar{G}$. .

$\bar{\sigma}$: order 4, since $(\bar{\sigma})^4 = \bar{\sigma^4} = 1$, while $\bar{\sigma}, \bar{\sigma}^2, \bar{\sigma}^3$ are not equal to $1 \in \bar{G}$.

$\bar{\sigma}^2$: order 2

$\bar{\sigma}^3$: order 4

$\bar{\tau}$: order 2

$\bar{\tau}\bar{\sigma}$: order 2, $(\bar{\tau}\bar{\sigma})^2 = \bar{\tau}\bar{\sigma}\bar{\tau}\bar{\sigma} = \bar{\sigma}^3\bar{\sigma} = 1$ (the relation $\tau\sigma\tau = \sigma^3$ in G carries over to $\bar{G}$ give $\bar{\tau}\bar{\sigma}\bar{\tau} = 1$)

$\bar{\tau}\bar{\sigma}^2$: order 2, likewise

$\bar{\tau}\bar{\sigma}^3$: order 2, likewise

(d) Write each of the following elements in the form $\bar{\tau}^a\bar{\sigma}^b$.

. $\overline{\sigma\tau} = \overline{\tau\sigma^3} = \bar{\tau}\bar{\sigma}^3$

$\overline{\tau\sigma^{-2}\tau} = \overline{\tau\sigma^2\tau} = \overline{\tau\sigma\tau\sigma^3} = \overline{\tau^2\sigma^6} = \overline{\sigma^2} = \bar{\sigma}^2$

$\overline{\tau^{-1}\sigma^{-1}\tau\sigma} = \overline{\tau\sigma^3\tau\sigma} = \overline{(\tau\sigma\tau)^3\sigma} = \overline{\sigma^9\sigma} = \overline{\sigma^2} = \bar{\sigma}^2$

(e) Prove that $\bar{G} \simeq D_8$. Clearly $\bar{G}$ is generated by $\bar{\sigma}$ and $\bar{\tau}$, where $\bar{\sigma}^4 = \bar{\tau}^2 = 1$ and $\bar{\tau}\bar{\sigma}^3 = \bar{\sigma}\bar{\tau}$ reduces to $\bar{\tau}\bar{\sigma}^{-1} = \bar{\sigma}\bar{\tau}$. So by identifying these with the generators of D_8, we get a surjective homomorphism $D_8 \to \bar{G}$, but $\bar{G}$ also has 8 elements, so they are isomorphic.

22.

(a) Prove that if H and K are normal subgroups of a group G then their intersection $H \cap K$ is also a normal subgroup of G. To begin with, $H \cap K$ cannot be empty as it contains 1. Let $a, b \in H \cap K$. Then $ab^{-1} \in H$, and $ab^{-1} \in K$ so $ab^{-1} \in H \cap K$ which shows $H \cap K$ is a subgroup. Now let $x \in H \cap K$ and $g \in G$. Then consider gxg^{-1}, which is contained in H because $x \in H$ and H is normal. But for the same reason, this is also contained in K. Therefore gxg^{-1} is contained in $H \cap K$, which means $H \cap K$ is normal.

(b) Prove that the intersection of an arbitrary nonempty collection of normal subgroups of a group is a normal subgroup. Let $\{A_i\}_{i \in I}$ be a nonempty collection of normal subgroups of G. Here I is the set of indices which can be very big (for instance, I can be $\mathbb{R}$). Then consider $A := \cap_{i \in I} A_i$. It contains 1 so nonempty and if we assume $a, b \in A$ then in particular, $a, b \in A_i$ for any $i \in I$ which means $ab^{-1} \in A_i$ and $ab^{-1} \in A$.

Likewise, let $x \in A$ and $g \in G$. Then $gxg^{-1} \in A_i$ for any $i \in I$ because A_i is normal and $x \in A_i$. Therefore $gxg^{-1} \in A$, showing A is normal.

24. Prove that if $N \trianglelefteq G$ and H is any subgroup of G then $N \cap H \trianglelefteq H$.

First, $N \cap H$ is a group and $N \cap H \subseteq H$, so $N \cap H \le H$. Now let $x \in N \cap H$ and $h \in H$.

Then $hxh^{-1} \in N$ because $x \in N$ and N is a normal subgroup. But $h, x \in H$ so $hxh^{-1} \in H$ showing that $hxh^{-1} \in N \cap H$, and that $N \cap H$ is normal in H.

Let $z \in Z(G)$. Then $zg = gz$ for all $g \in G$. We want to show that $zAz^{-1} = A$ but all elements in zAz^{-1} has the form zaz^{-1} for some $a \in A$, while $zaz^{-1} = zz^{-1}a = a$ and hence $zAz^{-1} = A$. We get $Z(G) \subseteq N_G(A)$ and again, this directly implies $Z(G) \leq N_G(A)$.

36. Prove that $G/Z(G)$ is cyclic then G is abelian.

Let x be a generator of $G/Z(G)$. Then every element of $G/Z(G)$ has the form x^n for some $n \in \mathbb{Z}$. Equivalently, they have the form $x^n Z(G)$. But this means that every element g of G has the form $x^n z$ for some $z \in Z(G)$ simply because $g \mapsto \bar{g} = x^n Z(G)$. Hence for any two elements $g, h \in G$, $g = x^n z$ and $h = x^m z'$ where $z, z' \in Z(G)$ and

$gh = x^n z x^m z' = x^n x^m z z'$ (since z commutes with x^m) $= x^m x^n z' z$ (z' commutes with z) $= x^m z' x^n z$ (z' commutes with x^n)$= hg$, showing that G is abelian.

Section 3.1 Suggested Exercises

2. Let ϕ be a homomorphism $G \to H$ with kernel K and let $a, b \in \phi(G)$. Let $X \in G/K$ be the fiber above a and let Y be the fiber above b. Fix an element u of $X = \phi^{-1}(a)$. Prove that if $XY = Z$ in the quotient group G/K and w is any member of Z, there is some $v \in Y$ such that $uv = w$.

In the quotient group G/K, we have $X = uK$ and $Z = wK$. And $XY = Z$ means $Y = X^{-1}Z$, where $X^{-1} = u^{-1}K$ by our group operation in G/K. And $X^{-1}Z = u^{-1}wK$. That is, $Y = u^{-1}wK$, or $u^{-1}w$ is contained in Y. For some $v \in Y$ we have $v = u^{-1}w$, or $uv = w$.

5. Use the preceding exercise to prove that the order of the element gN in G/N is n, where n is the smallest positive integer such that $g^n \in N$. Given an example to show that the order of gN in G/N may be strictly smaller than the order of g in G.

The identity of G/N is $1N = N$, and hence $(gN)^n = g^n N = N$ if and only if g^n and 1 are in the same coset, or equivalently, $g^n \in N$. This proves the first statement.

Consider $G = \mathbb{Z}/4\mathbb{Z}$, and $N = \{\bar{0}, \bar{2}\} \leq G$. In G, $\bar{1}$ has order 4, while in G/N, $\bar{1} + N$ has order 2.

12. Let G be the additive group of real numbers, let H be the multiplicative group of complex numbers of absolute value 1 and let $\phi : G \to H$ be the homomorphism $\phi : r \mapsto e^{2\pi i r}$. Draw the points on a real line which lie in the kernel of ϕ. Describe similarly the elements in the fibers of ϕ above points -1, i, and $e^{4\pi i/3}$ of H.

Since the multiplicative identity of H is 1, the kernel is the set of real numbers r such that $e^{2\pi i r} = 1$, but $e^{2\pi i r} = \cos(2\pi r) + i \sin(2\pi r)$ which equals 1 if and only if $r \in \mathbb{Z}$. The fiber of -1 is the set of solutions for the equation $e^{2\pi i r} = -1$ and it corresponds to the set of half-integers, real numbers of the form $n + \frac{1}{2}$. You can likewise determine the fibers of i and $e^{4\pi i/3}$.

27. Let N be a finite subgroup of a group G. Show that $gNg^{-1} \subseteq N$ if and only if $gNg^{-1} = N$. Deduce that $N_G(N) = \{g \in G \mid gNg^{-1} \subseteq N\}$.

Since $N_G(N) = \{g \in G \mid gNg^{-1} = N\}$ by definition, if we show the first statement, the second one is obvious.

Indeed, at some point we have proved that gNg^{-1} has the same number of elements as N. An element $n \in N$ would bijectively correspond to the element $gng^{-1} \in N$. Therefore, $gNg^{-1} \subseteq N$ implies that they are the same.

31. Prove that if $H \leq G$ and N is a normal subgroup of H then $H \leq N_G(H)$. Deduce that $N_G(N)$ is the largest subgroup of G in which N is normal.

Assume that N is a normal subgroup of H. Then by definition, it means whenever $h \in H$, $hNh^{-1} = N$. This shows again by definition, $h \in N_G(H)$. Therefore $H \subseteq N_G(H)$, and since H is closed under group operation and inverses, $H \leq N_G(H)$.

For the same reason, we see that N is normal in $N_G(N)$. Second statement is now trivial.

34. Let $D_{2n} =< r, s : r^n = s^2 = 1, rs = sr^{-1} >$ be the usual presentation of the dihedral group of order $2n$ and let k be a positive integer dividing n.

(a) Prove that $< r^k >$ is a normal subgroup of D_{2n}.

By definition, we need to check $g < r^k > g^{-1} =< r^k >$ for all $g \in D_{2n}$. But from exercise 27, it is enough to check $g < r^k > g^{-1} \subseteq< r^k >$. In addition, it is enough to check $gr^kg^{-1} \in< r^k >$, because then while all elements in $< r^k >$ has the form r^{ik} (for some integer i), $gr^{ik}g^{-1} = (gr^kg^{-1})^i$.

Any $g \in D_{2n}$ is either in the form sr^j or r^j for some integer j. If $g = r^j$, $r^jr^kr^{-j} = r^k$. If $g = sr^j$, $sr^jr^k(sr^j)^{-1} = sr^jr^kr^{-j}s^{-1} = sr^ks^{-1} = sr^ks = sr^{k-1}rs = sr^{k-1}sr^{-1} = ... = s^2r^{-k} = r^{-k}$, which is contained in $< r^k >$. Therefore, we are done.

(b) Prove that $D_{2n}/ < r^k >\cong D_{2k}$.

Consider the natural projection $p : D_{2n} \to D_{2n}/ < r^k >$ and let $\bar{r} = p(r)$ and $\bar{s} = p(s)$. In this quotient group, we clearly have $(\bar{r})^k = 1$ since r^k is contained in the kernel of the projection, and we have "inherited" relations $\bar{s}^2 = 1$, $\bar{r}\bar{s} = \bar{s}\bar{r}^{-1}$. It is obvious that $\bar{r}$ and $\bar{s}$ generates the quotient group. (In general, images of the generators under a quotient map generates the quotient group)

Therefore, $\bar{r}$ and $\bar{s}$ satisfies the same relations with generators of D_{2k}, which means we have a well-defined surjective homomorphism $\phi : D_{2k} \to D_{2n}/ < r^k >$. We count how many elements are there in $< r^k >$. If $n = dk$, we have d elements in $< r^k >$, which shows that the kernel of the projection p has d elements and $|D_{2n}/ < r^k > | = 2n/d = 2k$. That is, D_{2k} and $D_{2n}/ < r^k >$ has the same number of elements, which forces ϕ to be an isomorphism.

41. Let G be a group. Prove that $N =< x^{-1}y^{-1}xy : x, y \in G >$ is a normal subgroup of G and G/N is abelian.

We show that $gNg^{-1} \subseteq N$ for any $g \in G$. This follows from a computation $gx^{-1}y^{-1}xyg^{-1} = (gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}) \in N$. Since g was arbitrary, we also have $gNg^{-1} \supseteq N$, showing that N is a normal subgroup.

Let aN and bN be two elements of G/N. We want to show $abN = baN$ or $ab(ba)^{-1} \in N$. But $ab(ba)^{-1} = aba^{-1}b^{-1} \in N$, where we put $x = a^{-1}$ and $y = b^{-1}$. So G/N is an abelian group, called the abelianization of G.