Homework 4 solutions.

Problem 7.4. Produce a specific isomorphism between S_3 and D_3. How many different isomorphisms are there from S_3 to D_3?

Answer. $S_3 = \{e, (12), (13), (23), (123), (132)\}$ and $D_3 = \{e, r, r^2, s, sr, sr^2\}$. The group D_3 is the group of symmetries of a triangle T. Label the corners of T with numbers 1,2,3 as in the picture. Let s be the reflection fixing 1 and exchanging 2 and 3 and let r be the clockwise rotation sending 1 to 2, 2 to 3 and 3 to 1. We see

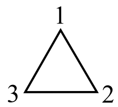

FIGURE 1. One way to number corners of a triangle.

that all elements of D_3 permute these labels, so they correspond to permutations of the set $\{1, 2, 3\}$. Let $f : D_3 \to S_3$ be the map sending each element of D_3 to the corresponding permutation of the set $\{1, 2, 3\}$. The position of the triangle is completely determined by where the labels are. So if A, B are two distinct elements of D_3, they do different things to the labels. Thus this map is one to one. There are six elements of D_3 and six of S_3. Since each element of D_3 does something different to the labels of T, every element of S_3 must have some element of D_3 mapped to it. So f is onto.

Finally, f is a homomorphism. To see this, suppose A, B are two elements of D_3. Then doing A followed by B to the triangle T first permutes the corners by the permutation $f(A)$ and then by permutation $f(B)$. In total the corners are permuted by permutation $f(B)f(A)$. The element BA in D_3 gives the permutation $f(BA)$. So we must have $f(BA) = f(B)f(A)$. Since this is true for any A, B in D_3, we must have that f is a homomorphism.

Therefore the map f defined in this way is an isomorphism. In fact, given any labeling of T we get a homomorphism in this way.

Note that two different labelings of T give two different isomorphisms. There are 6 possible labelings of T. (They correspond to the six elements of S_3, actually, because each element of S_3 tells you how to change the labels.) Therefore there are 6 isomorphisms between D_3 and S_3. $\square$

Problem 7.5. Let G be a group. Show that the correspondence $x \leftrightarrow x^{-1}$ is an isomorphism from G to G iff G is *abelian.*

Proof. Let G be a group, and define $f : G \to G$ by $f(x) = x^{-1}$.

Suppose G is abelian. We need to show that f is an isomorphism. That is, we need to show that f is one to one, onto, and a homomorphism.

To show that f is one to one, we need to show that if $x \neq y$ then $x^{-1} \neq y^{-1}$. Suppose for contradiction that $x \neq y$ but $x^{-1} = y^{-1}$. Then consider the quantity $xx^{-1}y$. Since $xx^{-1} = e$, $xx^{-1}y = y$. But since $x^{-1} = y^{-1}$, we have $x^{-1}y = e$ so $xx^{-1}y = x$ as well. That means $x = y$, so we arrive at a contradiction. Therefore f is one to one.

To show that f is onto, we need to show that for every $y \in G$ there is an $x \in G$ s.t. $f(x) = y$. So let $x = y^{-1}$. Then $f(x) = f(y^{-1}) = (y^{-1})^{-1} = y$. Therefore f is onto.

To show that f is a homomorphism, we need to show that for every $x, y \in G$ we have $f(xy) = f(x)f(y)$. We have that $f(xy) = (xy)^{-1} = y^{-1}x^{-1}$. (Recall that $(xy)^{-1} = y^{-1}x^{-1}$ from several problem sets ago.) And we know that $f(x)f(y) = x^{-1}y^{-1}$. Since G is abelian, $x^{-1}y^{-1} = y^{-1}x^{-1}$ so indeed $f(xy) = f(x)f(y)$. Therefore f is an homomorphism.

Since f is one to one, onto, and a homomorphism, f is an isomorphism.

Now suppose f is an isomorphism. We need to show that G is abelian. We use that since f is an isomorphism, $f(xy) = f(x)f(y)$. Plugging x^{-1} in for x and y^{-1} in for y, the homomorphism equality tells us that $f(x^{-1}y^{-1}) = f(x^{-1})f(y^{-1})$. Working this out we get that $(x^{-1}y^{-1})^{-1} = (x^{-1})^{-1}(y^{-1})^{-1}$. But this just means that $yx = xy$. Since we can do this for any x and y, this means that G is abelian.

Therefore f is an isomorphism iff G is abelian. $\square$

Problem 7.6. Prove that $\mathbb{Q}^{\text{pos}}$ is not isomorphic to $\mathbb{Z}$.

Proof. Suppose for contradiction that $\mathbb{Q}^{\text{pos}}$ is isomorphic to $\mathbb{Z}$ where $\mathbb{Q}^{\text{pos}}$ is a group under multiplication and $\mathbb{Z}$ is a group under addition. That means there exists an isomorphism $f : \mathbb{Q}^{\text{pos}} \to \mathbb{Z}$. Since f is an isomorphism, f is onto. That means for every $y \in \mathbb{Z}$ there is an $x \in \mathbb{Q}^{\text{pos}}$ s.t. $f(x) = y$. In particular, we can choose $y = 1 \in \mathbb{Z}$, so there must be some $\frac{p}{q} \in \mathbb{Q}^{\text{pos}}$ s.t. $f(\frac{p}{q}) = 1$. (When we write $\frac{p}{q} \in \mathbb{Q}^{\text{pos}}$ we mean that p, q are integers with no common factors.) Note that since -1 is the additive inverse of 1 in $\mathbb{Z}$, and $\frac{q}{p}$ is the multiplicative inverse of $\frac{p}{q}$ in $\mathbb{Q}^{\text{pos}}$ the fact that f is a isomorphism means that $f(\frac{q}{p}) = -1$.

Suppose $x \in \mathbb{N}$ is a prime number. Then $x \in \mathbb{Q}^{\text{pos}}$. Suppose $f(x) = n \in \mathbb{Z}$. Then either n is positive and $n = 1 + 1 + \cdots + 1$ (i.e. 1 added to itself n times), or n is negative so $n = -1 - 1 - \cdots - 1$ (i.e. -1 added to itself n times). Using the facts that $1 = f(\frac{p}{q})$ and $-1 = f(\frac{q}{p})$ we get either $f(x) = f(\frac{p}{q}) + f(\frac{p}{q}) + \cdots + f(\frac{p}{q})$ (that is, $f(\frac{p}{q})$ added to itself n times) or $f(x) = f(\frac{q}{p}) + f(\frac{q}{p}) + \cdots + f(\frac{q}{p})$ (that is, $f(\frac{q}{p})$ added to itself n times). By the homomorphism condition, this means that either $f(x) = f(\frac{p}{q} \cdot \frac{p}{q} \cdots \frac{p}{q}) = f(\frac{p^n}{q^n})$ or $f(x) = f(\frac{q^n}{p^n})$.

But f is one to one. So if $f(x) = f(\frac{p^n}{q^n},)$ then $x = \frac{p^n}{q^n}$ and if $f(x) = f(\frac{q^n}{p^n})$ then $x = \frac{q^n}{p^n}$. Either of these equalities would imply that x has an n^{th} root that is a rational number. But all the roots of any prime number are irrational. So we must have $n = 1$. Thus for any prime number x, either $x = \frac{p}{q}$ or $x = \frac{q}{p}$. But this would mean that the only primes are the numbers $\frac{p}{q}$ and $\frac{q}{p}$ which is impossible not least because there are infinitely many primes. So we have arrived at a contradiction. Therefore $\mathbb{Q}^{\text{pos}}$ is not isomorphic to $\mathbb{Z}$. $\square$

Problem 7.7. If G is a group, and if g is an element of G, show that the function $\phi : G \to G$ defined by $\phi(x) = gxg^{-1}$ is an isomorphism. Work out this isomorphism when G is A_4 and g is the permutation (123).

Proof. Let $\phi : G \to G$ be defined by $\phi(x) = gxg^{-1}$. We need to show the following things:

One to one: Suppose $\phi(x) = \phi(x')$. Then $gxg^{-1} = gx'g^{-1}$. Multiplying both sides by g on the right and by g^{-1} on the left we get that $x = x'$. So $\phi(x) = \phi(x')$ only if $x = x'$. Therefore the contrapositive is true: if $x \neq x'$ we have $\phi(x) \neq \phi(x')$. So ϕ is one to one.

Onto: Let $y \in G$. Let $x = g^{-1}yg$. Because G is a group, $x \in G$. We have that $\phi(x) = g(g^{-1}yg)g^{-1} = y$. So ϕ is onto.

Homomorhism: Let $x, y \in G$. Then $\phi(xy) = gxyg^{-1} = gxgg^{-1}yg^{-1} = \phi(x)\phi(y)$. So ϕ is a homomorphism.

Therefore, ϕ is an isomorphism.

We have that $A_4 = \{e, (123), (132),\ (124),\ (142),\ (134),\ (143),\ (234),\ (243),$ $(12)(34),\ (13)(24),\ (14)(23)\}$. Note that if α, β are in S_4 and β sends i to $\beta(i)$ then $\alpha\beta\alpha^{-1}$ sends $\alpha(i)$ to $\alpha(\beta(i))$. So expressing β as a cycle, we can replace all the numbers in β by α of those numbers. If $g = (123)$, g sends 1 to 2, 2 to 3, 3 to 1, and 4 to 4. Thus

$$\begin{array}{ccc} \phi(e) = e & \phi(123) = (231) & \phi(132) = (213) \\ \phi(124) = (234) & \phi(142) = (243) & \phi(134) = (214) \\ \phi(143) = (241) & \phi(234) = (314) & \phi(243) = (341) \\ \phi(12)(34) = (23)(14) & \phi(13)(24) = (21)(34) & \phi(14)(23) = (24)(31) \end{array}$$

Note that the answers above may look unfamiliar because they aren't written with the smallest number first. □

Problem 7.9. Suppose G is a cyclic group. If x generates G, and if $\phi : G \to G$ is an isomorphism, prove that ϕ is completely determined by $\phi(x)$ and that $\phi(x)$ also generates G. Use these facts to find all isomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$, and all isomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{12}$.

Proof. We know that x generates G so any element y of G can be written as $y = x^n$ for some $n \in \mathbb{Z}$. Suppose $\phi : G \to G$ is an isomorphism with $\phi(x) = x'$. Since ϕ is a homomorphism, we have $\phi(y) = \phi(x^n) = \phi(x)^n = (x')^n$. So if we know $\phi(x)$ we know $\phi(y)$ for any y in G. Therefore ϕ is completely determined by $\phi(x)$.

Let $y \in G$. Then there is an z in G s.t. $\phi(z) = y$. But since x generates G, we can write $z = x^n$ for some $x \in \mathbb{Z}$. Thus $\phi(x^n) = y$. But if we still have $\phi(x) = x'$ then this means $(x')^n = y$. So any y in G can be written as a power of $\phi(x) = x'$. This is exactly what it means for $\phi(x)$ to generate G.

Suppose $\phi : \mathbb{Z} \to \mathbb{Z}$ is an isomorphism. The only generator of $\mathbb{Z}$ is 1. So ϕ can only send 1 to itself. This completely determines ϕ so there can only be one isomorphism from $\mathbb{Z}$ to $\mathbb{Z}$.

Suppose $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ is an isomorphism. The generators of Z_{12} are all numbers that are relatively prime to 12. That is, they are all numbers that don't share a common factor with 12. These numbers are 1, 5, 7 and 11. The generator 1 can be sent by ϕ to any of these four numbers. And as soon as we know what $\phi(1)$ is, we know all of ϕ. So there are 4 isomorphisms from $\mathbb{Z}_{12}$ to itself. □

Problem 7.12. Show that the subgroup of S_4 generated by (1234) and (24) is isomorphic to D_4.

Proof. To begin, set $\alpha = (1234)$ and $\beta = (24)$. Let's describe the subgroup generated by α and β. First, the powers of α are $\alpha^2 = (13)(24), \alpha^3 = \alpha^{-1} = (1432)$ and $\alpha^4 = e$. Since β has order 2, it's powers are e and itself. Then there are products between α and β. Note that $\alpha\beta = \beta\alpha^{-1}$ so the rest of the elements are $\alpha\beta$, $\alpha^2\beta$, and $\alpha^3\beta$.

The group D_4 is generated by the elements s and r where s has order 2 and r has order 4. If we had a isomorphism $f : S_4 \to D_4$, it would send an element $\alpha \in S_4$ of order n to an element $x \in D_4$ of the same order n.

Define f s.t. $f : \alpha \mapsto r$ and $f : \beta \mapsto s$. Then the homomorphism property would ensure that $f(\alpha^n\beta^m) = f(\alpha)^n f(\beta)^m$ (where n = 0, 1, 2, 3 and m = 0,1). Define f to send α^n to r^n and to send $\alpha^n\beta$ to $r^n s$ for $n = 1, 2, 3$. To see that f thus defined is a homomorphism, note that $rs = sr^{-1}$ and $\alpha\beta = \beta\alpha^{-1}$. Thus

$$\begin{aligned} f((\alpha^n\beta^m)(\alpha^{n'}\beta^{m'})) &= f(\alpha^{n-n'}\beta^{m+m'}) \\ &= r^{n-n'}s^{m-m'} \\ &= (r^n s^m)(r^{n'}s^{m'}) \\ &= f(\alpha^n\beta^m)f(\alpha^{n'}\beta^{m'}) \end{aligned}$$

for any n between 0 and 3 and for any $m = 0, 1$.

Therefore f is a homomorphism. From the definition, it's clear that any two distinct elements $\alpha^n\beta^m$ and $\alpha^{n'}\beta^{m'}$ get mapped to distinct elements of D_4 and that every element $r^n s^m$ of D_4 has some element $(\alpha^n\beta^m)$ mapping to it. So f is one to one and onto. Therefore f is an isomorphism and the two groups are isomorphic. $\square$