Homework #8

Problems to hand in on Thursday, March 28, in the beginning of class. Write your answers out carefully, staple pages, and write your name and section number on each page.

1) Let S^1 be the subset of $\mathbb{C}$ consisting of complex numbers of absolute value 1; that is

$$S^1 := \{z \in \mathbb{C} \mid |z| = 1\}.$$

(a) Prove that S^1 is a subgroup of $\mathbb{C}^\times$.

(b) Prove that the map

$$S^1 \to \mathrm{SL}_2(\mathbb{R}) \qquad x + iy \mapsto \begin{bmatrix} x & -y \\ y & x \end{bmatrix}$$

is an injective group homomorphism.

(c) Prove that S^1 is isomorphic to $\mathrm{SO}_2(\mathbb{R})$, the group of 2×2 orthogonal matrices of determinant 1. Use this to give a geometric interpretation of the group S^1 that explains why some call it the "continuous rotation group."

(d) For every positive integer n, find an element of order n in S^1.

(e) Find an element of infinite order in S^1.

Solution.

(a) Given $x, y \in S^1$, $|xy| = |x||y| = 1$, so S^1 is closed for the product. Moreover, $1 \in S^1$, and $|x^{-1}| = |x|^{-1} = 1$, so S^1 is also closed for inverses. We conclude that S^1 is a subgroup of $\mathbb{C}$.

(b) It is clear this map is injective, and it lands inside SL_2 since

$$\det \begin{pmatrix} x & -y \\ y & x \end{pmatrix} = x^2 + y^2 = |x + iy| = 1.$$

To see that this is a group homomorphism, just notice that

$$\begin{bmatrix} x & -y \\ y & x \end{bmatrix} \begin{bmatrix} z & -w \\ w & z \end{bmatrix} = \begin{bmatrix} xz - yw & -(xw + yz) \\ yz + xw & xz - yw \end{bmatrix},$$

and

$$(x + iy)(z + iw) = (xz - yw) + i(xw + yz).$$

(c) By 217, the set of orthogonal 2×2 matrices is precisely the set of all matrices of the form

$$\begin{bmatrix} x & -y \\ y & x \end{bmatrix}.$$

Therefore, image of the injective group homomorphism in (b) is precisely $\mathrm{SO}_2(\mathbb{R})$, and this is the isomorphism we are looking for.

(d) The matrix

$$\begin{bmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{bmatrix}$$

corresponds to the rotation by $\frac{2\pi}{n}$ around the origin in $\mathbb{R}^2$, so this is an element of order n in $\mathrm{O}_2(\mathbb{R})$. Its preimage is the element $z = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right) \in S^1$, and z is an element of S^1 of order n.

Another way to think about z is to rewrite it as $z = e^{\frac{2\pi}{n}i}$, which is a primitive n-th root of unity, so an element of S^1 of order n.

(e) Consider a rotation centered at the origin of $\mathbb{R}^2$ by any irrational multiple of 2π; for example, the rotation by 2 radians. This gives an element of $\mathrm{O}_2(\mathbb{R})$ or infinite order, corresponding to $z = e^{2i} \in S^1$.

2) Towards the end of the worksheet on group homomorphisms, we encountered the following:

THEOREM: If $\mathbb{F}$ is a finite field, then $\mathbb{F}^\times$ is cyclic.

(a) Check that 2 is not a generator for $\mathbb{Z}_{17}^\times$ but 3 is a generator for $\mathbb{Z}_{17}^\times$.
(b) Verify that $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+x+2)$ is a field, and find a generator for $\mathbb{F}_9^\times$.
(c) Read Corollary 7.10 on page 200, and use this corollary to prove the THEOREM above.[1]
(d) The THEOREM above only applies to finite fields, but we can sometimes describe multiplicative groups of infinite fields in terms of other groups. Show that $\mathbb{R}^\times \cong \mathbb{R} \times \mathbb{Z}_2$.
(e) Show that $\mathbb{C}^\times \cong \mathbb{R} \times S^1$.

Solution.

(a) $\langle 2 \rangle = \{2, 4, 8, 16, 15, 13, 9, 1\}$ – so 2 only has order 8. On the other hand, $\langle 3 \rangle = \{3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1\}$.

(b) $p(x) = x^2 + x + 2$ is irreducible, since it is a polynomial of degree 2 with no roots: $p(0) = 0^2 + 0 + 2 = 2 \neq 0$, $p(1) = 1^2 + 1 + 2 = 1 \neq 0$, and $p(2) = 2^2 + 2 + 2 = 2 \neq 0$. $\mathbb{F}_9^\times$ is generated by

(c) The solutions are written up in the adventure sheet on group homomorphisms.

(d) We will think of $\mathbb{Z}_2$ as the set $\{1, -1\}$ with the operation $\times$. Consider the map $f : \mathbb{R} \times \mathbb{Z}_2 \longrightarrow \mathbb{R}^\times$ given by

$$f(x, y) = ye^x.$$

This is a group homomorphism:

$$f(x,y)f(z,w) = (ye^x)(we^z) = (yw)e^{x+z} = f(x+z, yz).$$

Moreover, the map $g : \mathbb{R}^\times \longrightarrow \mathbb{R} \times \mathbb{Z}_2$ given by $g(z) = (\log(|z|), \frac{z}{|z|})$ is the inverse of f:

$$fg(z) = f\left(\log(|z|), \frac{z}{|z|}\right) = \frac{z}{|z|}e^{|z|} = z \text{ and } gf(x,y) = g(ye^x) = \left(\log(e^x), \frac{ye^x}{e^x}\right) = (x, y).$$

This shows that f is bijective, and thus an isomorphism.

[1] For a hint, look at the worksheet on group homomorphisms.

(e) Consider the map $f : \mathbb{C}^\times \longrightarrow \mathbb{R} \times S^1$ given by $f(z) = \left(\log(|z|), \frac{z}{|z|}\right)$. Again, this is a group homomorphism, with inverse $f : \mathbb{R} \times S^1 \longrightarrow \mathbb{C}^\times$ given by $f(x, y) = e^x y$.

3) Consider the following elements in $GL_2(\mathbb{C})$:

$$\mathbf{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{i} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad \mathbf{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix},$$

Let Q be the subgroup of $GL_2(\mathbb{C})$ generated by the matrices $\mathbf{i}, \mathbf{j}, \mathbf{k}$. You should verify (but not necessarily turn in a proof) that Q contains the 8 elements $\{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$, You may wish to make a multiplication table for Q to answer the following questions. (You do not need to turn in the multiplication table – although notice you have already written in down in last week's webwork!)

(a) Find the complete list of all cyclic subgroups of Q of order 4.
(b) Find the complete list of all cyclic subgroups of Q of order 2.
(c) Find the complete list of all noncyclic subgroups of Q of order 4.
(d) Can Q be generated by two elements? Prove it.
(e) Is Q_8 isomorphic to D_4? Prove or disprove.

Solution.

(a) $\langle i \rangle$, $\langle j \rangle$, $\langle k \rangle$. Notice $ij = k$, $jk = i$, $ki = j$.
(b) $\left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$.
(c) There aren't any!
(d) Yes! Since $ij = k$, $\langle i \rangle = Q$.
(e) No, since D_8 has a noncyclic subgroup of order 4.

4) Consider the symmetric group $\mathbb{S}_n$.

(a) Show that every element of $\mathbb{S}_n$ is a product of transpositions.[2]
(b) Let $\tau \in \mathbb{S}_n$ be a permutation, and $(\,a\,b\,)$ be a transposition. Show that $\tau(\,a\,b\,)\tau^{-1} = (\,\tau(a)\,\tau(b)\,)$, the transposition changing $\tau(a)$ and $\tau(b)$.
(c) Show that $(\,i\,j\,) = (\,1\,i\,)(\,1\,j\,)(\,1\,i\,)$. Conclude that every element of $\mathcal{S}_n$ is the product of transpositions of the form $(\,1\,i\,)$.
(d) Let σ be the n-cycle $(2 \cdots n\,)$. Show that $(\,1\,i\,) = \sigma^{i-2}(\,1\,2\,)(\sigma^{-1})^{i-2}$. Conclude that $\mathcal{S}_n = \langle (\,1\,2\,), (2 \cdots n\,) \rangle$.

[2] Hint: One possibility for a quick solution is induction on n. Can you multiply any permutation by a transposition to obtain a permutation that fixes one element?

Solution. Important note: a permutation is a FUNCTION $\{1,\ldots,n\} \longrightarrow \{1,\ldots,n\}$.

(a) First, we observe that every element in $\mathbb{S}_2$ is a product of transpositions, since the only element besides the identity is the transposition $(1\,2)$. Now suppose that every element in $\mathbb{S}_n$ is indeed a product of transpositions. Consider any element $\sigma \in \mathbb{S}_{n+1}$. Suppose that $\sigma(n+1) = i$. Then $\tau = (n+1\,i)\sigma$ fixes $n+1$, so we can think about it as an element of $\mathbb{S}_n$. Then by assumption τ can be written as a product of transpositions. Finally, $\sigma = (n+1\,i)\tau$ is a product of transpositions.

(b) Write $\sigma = \tau(\,a\,b\,)\tau^{-1}$. Then

$$\sigma(\tau(a)) = \left(\tau(a\,b)\tau^{-1}\right)(\tau(a)) = (\tau(a\,b))\,(a) = \tau(b).$$

Similarly, we can show that $\sigma(\tau(b)) = \tau(a)$. Moreover, given $k \neq \tau(a), \tau(b)$, we have $\tau^{-1}(k) \neq a, b$. Therefore,

$$\sigma(k) = \left(\tau(a\,b)\tau^{-1}\right)(k) = (\tau(a\,b))\left(\tau^{-1}(k)\right) = \tau(\tau^{-1}(k)) = k.$$

We conclude that σ switches $\tau(a), \tau(b)$ and fixes all other elements.

(c) Apply the previous formula with $\tau = (1\,i)$, $a = 1$, and $b = j$; then $(\,1\,i\,)(\,1\,j\,)(\,1\,i\,) = (\,i\,j\,)$ follows immediately. Since every element in $\mathbb{S}_n$ is a product of transpositions and any transposition is a product of elements of the form $(1\,i)$, we conclude that every element is a product of transpositions of the form $(1\,i)$.

(d) First, note that $(\sigma^{-1})^{i-1} = \left(\sigma^{i-1}\right)^{-1}$. Therefore,

$$\sigma^{i-1}(\,1\,2\,)(\sigma^{-1})^{i-1} = \left(\sigma^{i-2}(1)\ \sigma^{i-2}(2)\right) = (1\ \ i).$$

In particular, $\langle(\,1\,2\,), (2\,\cdots\,n\,)\rangle$ contains all the cycles of the form $(1\,i)$, and thus all elements of $\mathbb{S}_n$.