Math 5863 homework solutions

31. (3/22) Denote the automorphism group of a group G by $\mathrm{Aut}(G)$. Determine the following automorphism groups:

1. $\mathrm{Aut}(\mathbb{Z})$. (Consider $\phi(1)$.)

   The homomorphism property tells us that $\phi(n) = \phi(1 + \cdots + 1) = n(\phi(1))$, so every value of ϕ is a mulitple of $\phi(1)$. In particular, 1 can be a value of ϕ only when $\phi(1) = \pm 1$. The choice $\phi(1) = 1$ gives $\phi(n) = n$ for all n, that is, ϕ is the identity function. The choice $\phi(1) = -1$ gives $\phi(n) = -n$ for all n, that is, ϕ is multiplication by -1. So $\mathrm{Aut}(\mathbb{Z})$ is a group with exactly two elements, hence $\mathrm{Aut}(\mathbb{Z}) \cong C_2$.

2. C_n. (Write C_n as $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. Observe that a homomorphism $\phi\colon C_n \to C_n$ is completely determined by $\phi(\alpha) = \alpha^m$. Show that ϕ is injective– hence bijective, since C_n is finite— if and only if m and n are relatively prime. Deduce that $\mathrm{Aut}(C_n) \cong \{1 \leq m < n \mid \gcd(m, n) = 1\}$ with the operation of multiplication modulo n.)

   From the homomorphism property, we have $\phi(\alpha^k) = \phi(\alpha)^k$, so ϕ is completely determined by $\phi(\alpha)$. Write $\phi(\alpha) = \alpha^m$. Suppose that the greatest common divisor $\gcd(m, n) = d > 1$. Then $m \cdot \frac{n}{d} = \frac{m}{d} \cdot n$, so $\phi(\alpha^{n/d}) = \alpha^{m(n/d)} = (\alpha^n)^{(m/d)} = 1$, that is, ϕ has nontrivial kernel and hence is not an automorphism. On the other hand, if $\gcd(m, n) = 1$, then $\phi(\alpha^k) = \alpha^{mk} = 1$ only when n divides mk, which is only when k is a multiple of n, so ϕ is injective. Since C_n is finite, any injective function is surjective, so all m relatively prime to n give automorphisms. Notice that if $\phi(\alpha) = \alpha^m$ and $\psi(\alpha) = \alpha^\ell$, then $\phi \circ \psi(\alpha) = \alpha^{m\ell}$, so composition of these automorphisms corresponds to multiplication of the powers of α that define them. That is, $\mathrm{Aut}(C_n)$ can be described as the group of numbers $1 \leq m < m$ with $\gcd(m, n) = 1$, with the operation of multiplication modulo n.

3. Verify that $\mathrm{Aut}(C_{12}) \cong C_2 \times C_2$.

   By the previous observations, $\mathrm{Aut}(C_{12})$ can be regarded as the set $\{1, 5, 7, 11\}$ with the operation of multiplication modulo 12. Since $5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \mod 12$, this is a group of order 4 with three elements of order 2, so must be $C_2 \times C_2$ (any bijection of $\{1, 5, 7, 11\}$ to $C_2 \times C_2$ that sends $(1, 1)$ to 1 defines an isomorphism).

4. $\mathrm{Aut}(\mathbb{Z} \times \mathbb{Z})$ (Regard elements of $\mathbb{Z} \times \mathbb{Z}$ as column vectors $\begin{bmatrix} a \\ b \end{bmatrix}$. Write $\phi\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) = \left(\begin{bmatrix} a \\ c \end{bmatrix}\right)$ and $\phi\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right) = \left(\begin{bmatrix} b \\ d \end{bmatrix}\right)$, and observe that ϕ equals left multiplication by the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Verify that $\mathrm{Aut}(\mathbb{Z} \times \mathbb{Z})$ is isomorphic to the group $\mathrm{GL}(2, \mathbb{Z})$ of 2×2 matrices with integer entries and determinant ± 1. This generalizes to direct products of any number of copies of $\mathbb{Z}$, that is, $\mathrm{Aut}(\mathbb{Z}^n) \cong \mathrm{GL}(n, \mathbb{Z})$, but you do not need to work out the details of this.)

Any homomorphism ϕ of $\mathbb{Z}\times\mathbb{Z}$ can be regarded as multiplication by $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, as indicated above. If ϕ is an automorphism, then it has an inverse automorphism which is multiplication by an integer matrix $N = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$. Since $MN = I$, the determinants are integers satisfying $(ad - bc)\det(M^{-1}) = 1$, so $ad - bc = \pm 1$. On the other hand, if $\det(M) = \pm 1$, then the inverse matrix $M^{-1} = \dfrac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ has integer entries, and multiplication by M^{-1} is an inverse of multiplication by M, so M is an automorphism. Thus there is a bijection from $\mathrm{Aut}(\mathbb{Z}\times\mathbb{Z})$ to $\mathrm{GL}(2,\mathbb{Z})$. Composition of the automorphisms corresponds to multiplication of the matrices, so it is an isomorphism.

32. (3/8) Recall that two elements g_1 and g_2 of a group G are said to be *conjugate* if there exists an element $g \in G$ such that $gg_1g^{-1} = g_2$. The *conjugacy class* of g_1 is the set of all elements of G that are conjugate to g_1.

    1. Verify that the relation of being conjugate is an equivalence relation.
    2. Verify that the conjugacy class of the identity element is the identity element.

33. (3/22) For $n \geq 2$, the *dihedral group of order* $2n$ is the group D_n consisting of all pairs $\alpha^i\beta^j$ where i is an integer modulo n and j is an integer modulo 2, with the multiplication rule that $\alpha^i\beta^j\alpha^k\beta^\ell = \alpha^{i+(-1)^jk}\beta^{j+\ell}$ (that is, $\beta\alpha^i\beta^{-1} = \alpha^{-i}$). Verify the following:

    1. Check that the condition $\alpha^i\beta^j\alpha^k\beta^\ell = \alpha^{i+(-1)^jk}\beta^{j+\ell}$ implies that $\beta\alpha\beta^{-1} = \alpha^{-1}$, and that the condition that $\beta\alpha\beta^{-1} = \alpha^{-1}$ implies that $\alpha^i\beta^j\alpha^k\beta^\ell = \alpha^{i+(-1)^jk}\beta^{j+\ell}$. Thus, people write $D_n = \langle \alpha, \beta \mid \alpha^n = \beta^2 = 1, \beta\alpha\beta^{-1} = \alpha^{-1}\rangle$.

       Taking $i = 0$, $j = k = 1$, and $\ell = -1$ in the first relation gives $\beta\alpha\beta^{-1} = \alpha^{-1}$. On the other hand, since $\beta^2 = 1$, the equation $\beta\alpha\beta^{-1} = \alpha^{-1}$ implies that $\beta^j\alpha\beta^{-j} = \alpha^{(-1)^j}$, so we have

       $$\begin{aligned} \alpha^i\beta^j\alpha^k\beta^\ell &= \alpha^i(\beta^j\alpha^k\beta^{-j})\beta^{j+\ell} = \alpha^i(\beta^j\alpha\beta^{-j})^k\beta^{j+\ell} \\ &= \alpha^i(\beta^j\alpha\beta^{-j})^k\beta^{j+\ell} = \alpha^i(\alpha^{(-1)^j})^k\beta^{j+\ell} = \alpha^{i+(-1)^jk}\beta^{j+\ell} \end{aligned}$$

    2. D_n has $2n$ elements.

       There are n integers modulo n, and two modulo 2, so there are $2n$ pairs $\alpha^i\beta^j$ where i is an integer modulo n and j is an integer modulo 2.

    3. D_1 is isomorphic to C_2.

       $D_1 = \{1, \beta\}$, with $\beta^2 = 1$.

    4. D_2 is isomorphic to $C_2 \times C_2$.

       Since $\alpha\beta\cdot\alpha\beta = \alpha\beta\cdot\alpha\beta^{-1} = \alpha\,\alpha^{-1} = 1$, $D_2 = \{1, \alpha, \beta, \alpha\beta\}$ is a group of four elements, three of which have order 2, so is isomorphic to $C_2 \times C_2$.

5. D_n is nonabelian for $n \geq 3$.

   If $\beta\alpha = \alpha\beta$, then $\alpha^{-1} = \beta\alpha\beta^{-1} = \alpha$, so $\alpha^2 = 1$ and therefore $n \leq 2$.

6. The powers of α form a subgroup isomorphic to C_n.
7. The powers of β form a subgroup isomorphic to C_2.
8. Find the conjugacy class of each element of D_n.

   For α^k, we have $\alpha^i\beta^j\alpha^k\beta^{-j}\alpha^{-i} = \alpha^i\alpha^{(-1)^j k}\alpha^{-i} = \alpha^{(-1)^j k}$, so the conjugacy class of α^k is $\{\alpha^k, \alpha^{-k}\}$. This has two elements except when n is even and $2k = n$, in which case $\alpha^k = \alpha^{-k}$. For $\alpha^k\beta$, we have $\alpha^i\beta^j\alpha^k\beta\beta^{-j}\alpha^{-i} = \alpha^i\alpha^{(-1)^j k}\beta\alpha^{-i} = \alpha^i\alpha^{(-1)^j k}\beta\alpha^{-i}\beta^{-1}\beta = \alpha^i\alpha^{(-1)^j k}\alpha^i\beta = \alpha^{2i+(-1)^j k}\beta$. If n is odd, then different possibilities for i yield every possible power of α, so the conjugacy class is $\{\alpha^\ell\beta\}$, where ℓ takes on all possible values, that is, $D_n - C_n$. If n is even, then the conjugation can change the exponent of α by any even number, and the conjugacy classes are $\{\alpha^{2\ell}\beta\}$ if k is even and are $\{\alpha^{2\ell+1}\beta\}$ if k is odd. In either case, it has $n/2$ elements.

   In summary, for n odd we have one conjugacy class with one element, $\{1\}$, $(n-1)/2$ conjugacy classes consisting of two elements $\{\alpha^k, \alpha^{-k}\}$, and one conjugacy class $D_n - C_n$ of n elements. When n is even, there are two conjugacy classes $\{1\}$ and $\{\alpha^{n/2}\}$ consisting of one element (note that this corresponds to the fact that $\alpha^{n/2}$ is a central element), $(n-2)/2$ conjugacy classes consisting of two elements $\{\alpha^k, \alpha^{-k}\}$, and two conjugacy classes each having $n/2$ elements, $\{\alpha^{2\ell}\beta\}$ and $\{\alpha^{2\ell+1}\beta\}$.

34. (3/22) Recall that the group $\mathrm{Isom}_+(\mathbb{R}^2)$ of orientation-preserving isometries consists of all compositions T_vR_α, for $v \in \mathbb{R}^2$ and $\alpha \in S^1$ (where we regard S^1 as the additive group of real numbers modulo 2π), with multiplication given by $T_vR_\alpha T_wR_\beta = T_{v+R_\alpha(w)}R_{\alpha+\beta}$. Note that the inverse of T_vR_α is $R_{-\alpha}T_{-v}$, which is also equal to $T_{R_{-\alpha}(-v)}R_{-\alpha}$.

    1. Verify that the conjugacy class of T_v ($v \neq 0$) is $\{T_w \mid \| w \| = \| v \|\}$. Describe these elements geometrically.

       We calculate that $T_wR_\alpha \cdot T_v \cdot R_{-\alpha}T_{-w} = T_wT_{R_\alpha(v)}R_\alpha R_{-\alpha}T_{-w} = T_{w+R_\alpha(v)-w} = T_{R_\alpha(v)}$. The possible vectors $R_\alpha(v)$ are exactly the vectors of length equal to the length of v. Geometrically, the conjugacy class of T_v consists of all the translations that move points the same distance as T_v does.

    2. Verify that the conjugacy class of R_α ($\alpha \neq 0$) is $\{T_vR_\alpha \mid v \in \mathbb{R}^2\}$. Show that these elements are exactly the isometries that rotate the plane through an angle α about some fixed point. (Observe that each conjugate can be written in the form $T_wR_\alpha T_{-w}$, and think about its geometric effect on the plane.)

       We calculate that $T_wR_\beta \cdot R_\alpha \cdot R_{-\beta}T_{-w} = T_wR_\alpha T_{-w} = T_wT_{R_\alpha(-w)}R_\alpha = T_{w+R_\alpha(-w)}R_\alpha$. Now, every vector v can be written in the form $w + R_\alpha(-w)$ for some w; w and $R_\alpha(-w)$ are vectors of equal length meeting at an angle $\pi + \alpha \neq \pi$, so we may select w so that v bisects the angle between w and $R_\alpha(-w)$, then adjust the length of w until $w + R_\alpha(-w)$ exactly v. So the conjugacy class is all elements of the form T_vR_α.

We calculated that each conjugate $T_w R_\beta \cdot R_\alpha \cdot R_{-\beta} T_{-w}$ equals $T_w R_\alpha T_{-w}$. Consider the effect of $T_w R_\alpha T_{-w}$ on the point w. First it is translated to the origin, then R_α rotates everything about the origin, then the origin is translated back to w. The composite effect is to rotate through an angle α, but with w in the role of the origin. Conversely, any rotation through an angle α about a fixed point w can be regarded as this conjugate $T_w R_\alpha T_{-w}$.

35. (3/22) Recall that if H is a subgroup of a group G, then gHg^{-1} is the subgroup consisting of all elements ghg^{-1} for $h \in H$, and recall that H is called a *normal* subgroup if $gHg^{-1} = H$ for all $g \in G$.

    1. Verify that every subgroup of an abelian group is normal.
    2. Verify that the subgroup consisting of the powers of α is a normal subgroup of D_n.
    3. Verify that the subgroup consisting of the powers of β is a normal subgroup of D_n if and only if $n \leq 2$.

       For $n \leq 2$, D_n is abelian so every subgroup is normal. If $n \geq 3$, then $\alpha^2 \neq 1$, so $\alpha \neq \alpha^{-1}$, so $\beta\alpha\beta^{-1} \neq \alpha$, so $\alpha^{-1}\beta\alpha \neq \beta$. Therefore $\alpha^{-1}\beta\alpha \notin \{1, \beta\}$, showing that $\{1, \beta\}$ is not normal.

    4. Let T be the subgroup of $\mathrm{Isom}_+(\mathbb{R}^2)$ consisting of all translations, that is, all elements of the form T_v. Verify that T is isomorphic to $\mathbb{R}^2$, and is a normal subgroup of $\mathrm{Isom}_+(\mathbb{R}^2)$.
    5. Let R be the subgroup of $\mathrm{Isom}_+(\mathbb{R}^2)$ consisting of all rotations, that is all elements of the form R_α. Verify that R is isomorphic to S^1, and is not a normal subgroup of $\mathrm{Isom}(\mathbb{R}^2)$.
    6. Find a subgroup of $\mathrm{Isom}(\mathbb{R}^2)$ (not $\mathrm{Isom}_+(\mathbb{R}^2)$, as you will want to use the isometry $\tau(x, y) = (x, -y)$) that is isomorphic to D_n.

       Put $\alpha = R_{2\pi/n}$ and $\beta = \tau$. Then α has order n, β has order 2, and $\beta\alpha\beta^{-1} = \tau R_{2\pi/n}\tau = R_{-2\pi/n} = \alpha^{-1}$. One can check that the elements $\alpha^i\beta^j$ for $0 \leq i \leq n-1$ and $0 \leq j \leq 1$ are distinct, so α and β produce a subgroup isomorphic to D_n.

36. (3/22) Consider the quotient space of the standard 2-sphere S^2 in $\mathbb{R}^3$, obtained by identifying each x with $-x$.

    1. Show that the quotient space is homeomorphic to the real projective plane $P = \mathbb{RP}^2$, obtained from a Möbius band and a 2-disk by identifying their boundary circles.

       Perhaps the easiest way is to think of first identifying each point below the equator with its corresponding point above the equator, giving just the upper hemipshere which is a disk D^2, and then making the remaining identifications on the equator, which amounts to identifying the opposite points on ∂D^2; thus the quotient is one of our standard descriptions of $\mathbb{RP}^2$.

2. Let $p\colon S^2 \to P$ be this quotient map. Show (a good picture should be enough) that each $x \in P$ has an open neighborhood U for which $p^{-1}(U)$ consists of two copies of U, each mapped homeomorphically to U by the restriction of p.

   For $x \in P$, the preimage is two points $\widetilde{x}$ and $-\widetilde{x}$ in S^2. Take D to be a small open disk in S^2 centered at $\widetilde{x}$, and let $-D$ be the disk consisting of all $-z$ for $z \in D$. Then the quotient map identifies each point in D with a unique point in $-D$, producing an open disk neighborhood U of x with the desired property. Note that this also verifies that P is a manifold.

3. The previous condition implies that $p\colon S^2 \to P$ satisfies the unique path lifting and unique homotopy lifting theorems, just as with the map $\mathbb{R} \to S^1$ (no need to prove this, the argument is exactly the same). Use these to prove that $\pi_1(P) \cong C_2$ (the fact that S^2 is simply-connected, which we proved in class since we proved that $\pi_1(S^2) = \{1\}$, is needed in the argument).

   Choose as basepoint the equivalence class $x_0 = \{N, S\}$ of the north and south poles. Any loop α in $\mathbb{RP}^2$ based at x_0 has a unique lift $\widetilde{\alpha}$ starting at N. Define $\Phi\colon \pi_1(\mathbb{RP}^2, x_0) \to C_2 = \{1, \sigma\}$ by $\Phi(\langle\alpha\rangle) = 1$ if $\widetilde{\alpha}(1) = N$ (that is, if α lifts to a loop at N) and $\Phi(\langle\alpha\rangle) = \sigma$ if $\widetilde{\alpha}(1) = S$.

   We note first that Φ is well-defined, for a path homotopy between α and α' lifts to a path homotopy between their lifts, so $\alpha(1) = \alpha'(1)$.

   To see that Φ is injective, suppose that $\Phi(\widetilde{\alpha} \simeq_p \widetilde{\alpha'}$. Then $\widetilde{\alpha}$ and $\widetilde{\alpha'}$ have the same starting point, N, and the same ending point. Since S^2 is simply-connected, there exists a path homotopy $F\colon \widetilde{\alpha} \simeq_p \widetilde{\alpha'}$. Then, $p \circ F\colon \alpha \simeq_p \alpha'$, so $\langle\alpha\rangle = \langle\alpha'\rangle$.

   Finally, to see that Φ is surjective, $\widetilde{c_{x_0}} = c_N$, and $c_N(1) = N$, so $\Phi(\langle c_{x_0}\rangle) = 1 \in C_2$. Now, let γ be any path in S^2 from N to S, and define $\alpha = p \circ \gamma$. Then, $\widetilde{\alpha}(1) = \gamma(1) = S$, so $\Phi(\langle\alpha\rangle) = \sigma$.