Problems and Solutions

1. Determine all finitely generated abelian groups G whose automorphism group is finite.

   Solution: Let G be a finitely generated abelian group. By the classification of finitely generated abelian groups, we know that G is isomorphic to a direct product of finitely many cyclic groups. In particular, $G \cong \mathbf{Z}^r \times H$ where H is a finite group and $r \geq 0$. The subgroup H is precisely the torsion subgroup of $\mathbf{Z}^r \times H$. Any element of $\mathrm{Aut}(G)$ must preserve the torsion subgroup. It follows that $\mathrm{Aut}(G) \cong \mathrm{Aut}(\mathbf{Z}^r) \times \mathrm{Aut}(H)$. Since H is finite, it follows that $\mathrm{Aut}(H)$ is finite. Thus, it suffices to determine when $\mathrm{Aut}(\mathbf{Z}^r)$ is finite. We have $\mathrm{Aut}(\mathbf{Z}^0) = \mathrm{Aut}(1) = 1$ and $\mathrm{Aut}(\mathbf{Z}) \cong \mathbf{Z}/2\mathbf{Z}$, and so for $r = 0, 1$, we have that $\mathrm{Aut}(G)$ is finite. For $r \geq 2$, we have

   $$\mathrm{GL}(2, \mathbf{Z}) \cong \mathrm{Aut}(\mathbf{Z}^2) \leq \mathrm{Aut}(\mathbf{Z}^r) \leq \mathrm{Aut}(\mathbf{Z}^r) \times \mathrm{Aut}(H) \cong \mathrm{Aut}(G).$$

   Since $\mathrm{GL}(2, \mathbf{Z})$ is an infinite group, we see that $\mathrm{Aut}(G)$ is infinite. Thus $\mathrm{Aut}(G) \cong \mathrm{Aut}(\mathbf{Z}^r \times H)$ is finite if and only if $r \leq 1$.

2. Prove that if G is a finite group containing no subgroup of index 2, then any subgroup of index 3 is normal in G.

   Solution: Let $H < G$ be a subgroup of index 3. The group G acts on the set of left cosets of H by left multiplication. This action gives a homomorphism $\phi : G \to S_3$. Let $K = \ker(\phi)$. If $g \in K$, then in particular $gH = H$, and so we see that $K < H$. Let $k = [H : K]$. Since K is normal in G it suffices to show $H = K$, that is, $k = 1$.

   We know that $[G : K] = [G : H][H : K] = 3k$. By the first isomorphism theorem we also have

   $$3k = [G : K] = |G|/|K| = |\phi(G)|.$$

   Since $\phi(G)$ is a subgroup of S_3, it follows from Lagrange's theorem that $|\phi(G)|$ divides $|S_3| = 6$ and so $3k$ divides 6. Thus k is equal to either 1 or 2.

Suppose that $k = 2$. This means that $[G : K] = |\phi(G)| = 6$, which is to say that ϕ is surjective. It follows that $[G : \phi^{-1}(A_3)] = [S_3 : A_3] = 2$, contradicting the assumption that G does not contain any subgroup of index 2. Thus, it must be that $k = 1$, which is what we wanted to show.

3. Prove the following special case of Gauss' lemma: If $p(x) \in \mathbf{Z}[x]$ is reducible in $\mathbf{Q}[x]$, then $p(x)$ is reducible in $\mathbf{Z}[x]$.

   Solution: This is a special case of Gauss' lemma, which can be found in any textbook on abstract algebra.

4. Let R be a *local ring*, i.e., a commutative ring with identity having a unique maximal ideal $\mathfrak{m}$. Let A be a 2×2 matrix with coefficients in $\mathfrak{m}$. Show that the matrix $B = A + I$ is invertible over R, i.e., that there exists a 2×2 matrix B' with coefficients in R such that $BB' = B'B = I$.

   Solution: First note that an element $x \in R$ is invertible iff $x \notin \mathfrak{m}$. Indeed, if $x \in \mathfrak{m}$ then clearly x is not invertible; conversely, if $x \notin \mathfrak{m}$ then x is not contained in any maximal ideal of R so $(x) = R$. The determinant of B is

$$\det(B) = b_{11}b_{22} - b_{12}b_{21} = (a_{11} + 1)(a_{22} + 1) - a_{12}a_{21}$$

   with $a_{ij} \in \mathfrak{m}$. Thus $\det(B) = 1 + a$ with $a \in \mathfrak{m}$ which implies that $\det(B)$ is invertible in R. We can take B' to be the matrix

$$B' = \det(B)^{-1} \begin{pmatrix} b_{22} & -b_{12} \\ -b_{21} & b_{11} \end{pmatrix}.$$

5. Suppose L/K is an algebraic field extension, and that R is a subring of L containing K. Prove that R is a field.

   Solution: Let $r \in R$ be any nonzero element. Since L/K is algebraic and $r \in L$ is nonzero, r satisfies a polynomial equation

$$a_n r^n + a_{n-1} r^{n-1} + \cdots + a_1 r + a_0 = 0$$

   with $a_n \neq 0$ and $a_i \in K$ for all i. We may assume that n is minimal, and thus that $a_0 \neq 0$. We can rewrite the above equation as

$$r\left(-a_0^{-1}(a_n r^{n-1} + a_{n-1} r^{n-2} + \cdots + a_1)\right) = 1$$

   in which all terms belong to R, since K is a field contained in R. It follows that r is invertible in R as desired.

6. Prove that every element of finite order in the group $\mathrm{SL}(2, \mathbf{Z})$ of 2×2 integer matrices with determinant 1 has order dividing 12. [**Hint:** First show that the eigenvalues of any torsion element must be roots of unity.]

   Solution: Let A be an element of exact order m in $\mathrm{SL}(2, \mathbf{Z})$, so that the minimal polynomial of A over $\mathbf{Q}$ is $X^m - 1$. Since the minimal and characteristic polynomial of A have the same irreducible factors, it follows that the eigenvalues of A are m^{th} roots of unity. (Alternately, one can use the fact that the eigenvalues of A^m are the m^{th} powers of the eigenvalues of A.) Also, since the minimal polynomial of A is square-free (since there are m distinct m^{th} roots of unity in $\mathbf{C}$), it follows that A is diagonalizable. Thus the eigenvalues of A are *primitive* m^{th} roots of unity.

   On the other hand, the eigenvalues of A satisfy the characteristic polynomial of A, which is a monic polynomial of degree 2 with integer coefficients. In particular, the eigenvalues of A are defined over a quadratic extension of $\mathbf{Q}$. By the irreducibility of the m^{th} cyclotomic polynomial, we have $[\mathbf{Q}(\zeta_m) : \mathbf{Q}] = \varphi(m)$ (Euler's φ-function) if ζ_m is a primitive m^{th} root of unity. By the explicit formula for φ, it is easy to see that $\varphi(n) \leq 2$ iff $n \mid 4$ or $n \mid 6$. In particular, we must have $m \mid 12$.

7. Let V be a finite dimensional vector space over a field F, and let $T : V \to V$ be a linear endomorphism. Prove that there is a direct sum decomposition $V = V_1 \oplus V_2$ with the following properties:

   (1) $T(V_i) \subseteq V_i$ for $i = 1, 2$.

   (2) T is an isomorphism on V_1.

   (3) T is nilpotent on V_2.

   [**Hint:** Consider the subspaces $\mathrm{Im}(T) \supseteq \mathrm{Im}(T^2) \supseteq \cdots$ and $\mathrm{Ker}(T) \subseteq \mathrm{Ker}(T^2) \subseteq \cdots$]

   Solution: The chain $\mathrm{Im}(T) \supseteq \mathrm{Im}(T^2) \supseteq \cdots$ must stabilize to a T-invariant subspace V_1 and the chain $\mathrm{Ker}(T) \subseteq \mathrm{Ker}(T^2) \subseteq \cdots$ must stabilize to a T-invariant subspace V_2.

   We claim that T is an isomorphism on V_1 and T is nilpotent on V_2. Indeed, it is easy to see that $T(V_1) = V_1$, which implies that T is an isomorphism on V_1 by the rank-nullity theorem. Moreover, $V_2 = \mathrm{Ker}(T^m)$ for some positive integer m and thus $T^m|_{V_2} = 0$, so T is nilpotent on V_2.

Finally, we claim that $V = V_1 \oplus V_2$. It is clear from what we have already shown that $V_1 \cap V_2 = (0)$. So it suffices to show that every $v \in V$ can be written as $v_1 + v_2$ with $v_i \in V_i$. Without loss of generality (replacing m by a larger integer if necessary), we may assume that $V_1 = T^m(V)$ and $V_2 = \mathrm{Ker}(T^m)$ for the same m. Since $\mathrm{Im}(T^{2m}) = \mathrm{Im}(T^m)$, we have $T^m(v) = T^{2m}(w)$ for some $w \in V$. Then $T^m(v - T^m(w)) = T^m(v) - T^{2m}(w) = 0$, so $v_2 := v - T^m(w) \in V_2$. Setting $v_1 := T^m(w) \in V_1$ gives the desired decomposition of v.