Algebra questions

1. Let n be a positive integer. If $\gcd(n, \phi(n)) > 1$, prove that there exists a non-cyclic group of order n. (Here $\phi(n)$ denotes Euler's ϕ-function.)

   Solution: By the formula for Euler's ϕ-function, either $p^2 \mid n$ for some prime p, or $pq \mid n$ with p, q primes for which $p \mid q - 1$. In the first case, take the direct product of $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ with any group of order n/p^2; this contains a non-cyclic subgroup so is non-cyclic. In the second case, by taking direct products as before, it suffices to prove that there is a non-abelian (and hence non-cyclic) group G of order pq. One can take for G the semidirect product of $\mathbf{Z}/p\mathbf{Z}$ and $\mathbf{Z}/q\mathbf{Z}$ with respect to any homomorphism $\mathbf{Z}/p\mathbf{Z} \to \mathrm{Aut}(\mathbf{Z}/q\mathbf{Z})^*$ which takes a generator of $\mathbf{Z}/p\mathbf{Z}$ to any element of order p in $\mathrm{Aut}(\mathbf{Z}/q\mathbf{Z})^* \cong \mathbf{Z}/(q-1)\mathbf{Z}$.

2. If $p < q$ are primes and $q \not\equiv \pm 1 \pmod{p}$, prove that there are exactly two groups of order pq^2, up to isomorphism. (You may assume as known the fact that every group of order q^2 is abelian.)

   Solution: Let P be a Sylow p-subgroup and Q a Sylow q-subgroup of G. Since p is the smallest prime dividing $|G|$ and Q has index p, Q is normal in G. Let n_p be the number of p-Sylow subgroups of G. Then $n_p \equiv 1 \pmod{p}$ and $n_p \mid |G|$. Since $q^2 \equiv 1 \pmod{p}$ iff $q \equiv \pm 1 \pmod{p}$, it follows that $n_p = 1$. Thus P is normal in G. By the recognition theorem for direct products, G is isomorphic to $P \times Q$, and therefore G is abelian. By the structure theorem for finite abelian groups, it follows that $G \cong \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q^2\mathbf{Z}$ or $G \cong \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z}$.

3. Let n be a positive integer, and let A be an $n \times n$ integer matrix. Define an equivalence relation on $\mathbf{Z}^n$ by setting $x \sim y$ if and only if $x - y = Az$ for some $z \in \mathbf{Z}^n$. Find an explicit formula for the number of equivalence classes.

   Solution: The answer is $|\det(A)|$ if $\det(A) \neq 0$, and ∞ if $\det(A) = 0$. To see this, note that the problem is just asking for the size of the quotient group $G = \mathbf{Z}^n/H$, where H is the subgroup of $\mathbf{Z}^n$ spanned by the columns of A. The group G is isomorphic to $\prod \mathbf{Z}/m_i\mathbf{Z}$, where $m_1, \ldots, m_n$ are the diagonal entries in the Smith Normal Form of the matrix A. If some $m_i = 0$ then G is infinite. Otherwise $|G| = |\prod m_i|$. The result now follows from the fact that the Smith Normal Form is obtained by elementary row and column operations which do not change $|\det(A)|$, and thus $|\det(A)| = |\prod m_i|$.

4. Prove that the ring $\mathbf{Z}[i]$ of Gaussian integers (where $i = \sqrt{-1}$) is a Euclidean domain.

   Solution: This is a standard result which can be found in most textbooks.

5. Find a splitting field for $x^{15} + 2$ over $\mathbf{Q}$, and determine its degree.

   Proof: A splitting field is obtained by adjoining one complex root α of $x^{15} + 2$ (which is irreducible since it's Eisenstein at 2) to $\mathbf{Q}$, and then adjoining a 15th root of unity ζ. As $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 15$ and $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \phi(15) = 8$ are relatively prime, it follows from the multiplicativity of the degree of field extensions in towers that $[\mathbf{Q}(\alpha, \zeta) : \mathbf{Q}] = 120$.

6. Let n be a positive integer, and let $G = \mathrm{GL}(n, \mathbf{C})$ be the group of invertible $n \times n$ matrices with complex coefficients. Prove that there is a proper subgroup H of G such that

$$\bigcup_{g \in G} g^{-1} H g = G.$$

   Proof: [We tacitly assumed $n \geq 2$.] Let H be the subgroup of upper triangular matrices. By a well-known result in linear algebra, every $n \times n$ matrix A is similar to an upper triangular matrix, i.e., there exists $C \in G$ such that $CAC^{-1} \in H$. But then $A \in C^{-1}HC$, and we're done.

7. Let n be a positive integer, and let $v_1, \ldots, v_{n+2}$ be any $n+2$ vectors in $\mathbf{R}^n$. Prove that $v_i \cdot v_j \geq 0$ for some $i \neq j$. [**Hint:** Use orthogonal projection to induct on n.]

   Solution: The case $n = 1$ is obvious. Assume the result is true for $n-1$. Let w_i for $i = 2, \ldots, n+2$ be the orthogonal projection of v_i onto the $(n-1)$-dimensional subspace $W = v_1^{\perp}$ of $\mathbf{R}^n$ orthogonal to v_1. Thus $w_i = v_i - \frac{v_i \cdot v_1}{v_1 \cdot v_1} v_1$. Assume for the sake of contradiction that $v_i \cdot v_j < 0$ for all $1 \leq i < j \leq n+2$. By induction, there exist indices $2 \leq i \neq j \leq n+2$ such that $w_i \cdot w_j \geq 0$. But by direct calculation,

$$w_i \cdot w_j = v_i \cdot v_j - \frac{(v_i \cdot v_1)(v_j \cdot v_1)}{v_1 \cdot v_1} < 0,$$

a contradiction.