McGill University
Math 371B: Algebra IV
Term Test 2: due May 1, 1999

1. (a) Given any monic polynomial $f(X) \in \mathbb{Z}[X]$ of degree ≥ 1, show that there are an infinite number of primes dividing the integers $f(1), f(2), \ldots, f(n), \ldots$. **Hint**: Suppose that the only primes dividing the integers $f(n)$ $(n \geq 1)$ are the primes $p_1, \ldots, p_k$. Let N be a positive integer with $a = f(N) > 0$. If $m = p_1 \cdots p_k$, show that $g(X) = a^{-1} f(N + amX) \in \mathbb{Z}[X]$ and that $g(n) \equiv 1 \mod m$ for $n \geq 1$. Now show that there is some integer $M > 0$ such that $g(M)$ has a prime factor $p \not| m$ and hence $p \mid f(N + amM)$.

   (b) Let p be an odd prime not dividing n and let $\Phi_n(X)$ be the n-th cyclotomic polynomial. If $a \in \mathbb{Z}$ with $\Phi_n(a) \equiv 0 \mod p$, prove that $p \not| a$ and that the order of a in $(\mathbb{Z}/p\mathbb{Z})$ is n. **Hint**: Use the fact that

$$X^n - 1 = \prod_{d|n} \Phi_d(X) = \Phi_n(X) \prod_{\substack{d|n \\ d<n}} \Phi_d(X)$$

   and that $X^n - 1$ has no multiple root mod p.

   (c) Prove that, given $n \geq 2$, there are infinitely many primes p with $p \equiv 1 \mod n$. This is a special case of Dirichlet's Theorem on Primes in Arithmetic Progressions which states more generally that there are infinitely many primes $p \equiv a \mod n$ for any a relatively prime to n.

   (d) For any integer $n \geq 1$, show that there is a cyclic extension of $\mathbb{Q}$ of degree n. **Hint**: If ζ_p is a primitive p-th root of unity, $\mathbb{Q}(\zeta_p)$ is a cyclic extension of $\mathbb{Q}$ of degree $p - 1$.

2. Let $\alpha = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$ and Let $E = \mathbb{Q}(\alpha)$.

   (a) Show that $F = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq E$ and $a = (2+\sqrt{2})(3+\sqrt{3})$ is not a square in F. **Hint**: If $a = c^2$, $c \in F$ and $\phi \in \mathrm{Gal}(F/\mathbb{Q})$ with $\phi(\sqrt{2}) = \sqrt{2}$, $\phi(\sqrt{3}) = -\sqrt{3}$, then $a\phi(a) = (c\phi(c))^2 = 6(2+\sqrt{2})^2$. Now show that $c\phi(c) \in \mathbb{Q}(\sqrt{2})$ and $\sqrt{6} \notin \mathbb{Q}(\sqrt{2})$ to get a contradiction.

   (b) Show that $[E : \mathbb{Q}] = 8$ and that the conjugates of α over $\mathbb{Q}$ are the 8 elements $\pm\sqrt{(2\pm\sqrt{2})(3\pm\sqrt{3})}$ and that they are all in E. **Hint**: If $\beta = \sqrt{(2-\sqrt{2})(3+\sqrt{3})}$, then $\alpha\beta = \sqrt{2}(3+\sqrt{3})$.

   (c) Let $\sigma \in G = \mathrm{Gal}(E/Q)$ be the automorphism which maps α to $\beta = \sqrt{(2-\sqrt{2})(3+\sqrt{3})}$. Show that since $\sigma(\alpha^2) = \sigma(\beta^2)$, we have $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma(\sqrt{3}) = \sqrt{3}$. From $\alpha\beta = \sqrt{2}(3+\sqrt{3})$ conclude that $\sigma(\alpha\beta) = -\alpha\beta$ and hence that $\sigma(\beta) = -\alpha$. Show that σ is of order 4.

   (d) Show similarly that the automorphism τ of E defined by $\tau(\alpha) = \sqrt{(2+\sqrt{2})(3-\sqrt{3})}$ is of order 4. Show that σ, τ generate G and that $\sigma^2 = \tau^2$, $\sigma\tau = \tau\sigma^3$. Show that $G \cong Q_8$, the quaternion group of order 8.

   (e) Find all subfields of E and their corresponding subgroups in $\mathrm{Gal}(E/Q)$.

3. (a) Show that the Galois group of $X^6 - 12x^4 + 15x^3 - 6x^2 + 15x + 12$ over $\mathbb{Q}$ is isomorphic to S_6. **Hint**: Show that the only transitive subgroup of S_n which contains a 2-cycle and an $(n-1)$-cycle is S_n.

   (b) Show that the Galois group of $f(X) = X^5 + 20X + 16$ is isomorphic to A_5. **Hint**: Show that the discriminant of $f(X)$ is a square and that any transitive subgroup of A_5 is isomorphic to one of C_5, D_5, A_5.

4. **(Bonus Question)** Text: p. 469 (2nd ed. p. 536), # 13.