Peter Stevenhagen

1. Let G be a finite abelian group. Show that there exists a number field L with $\mathrm{Gal}(L/\mathbf{Q}) \cong G$.

2. Let K be a number field, and μ_∞ the group of roots of unity in an algebraic closure $\overline{K} \subset \mathbf{C}$ of K.
   (a) Show that the map $x \mapsto \exp(2\pi x)$ defines an isomorphism $\mathbf{Q}/\mathbf{Z} \cong \mu_\infty$.
   (b) Show that the action of G_K of K on μ_∞ gives rise to a Galois representation

$$\rho_K : G_K \to \mathrm{Aut}(\mathbf{Q}/\mathbf{Z}) \cong \mathrm{GL}_1(\widehat{\mathbf{Z}}) = \widehat{\mathbf{Z}}^*,$$

   and that the image $\rho[G_K]$ is open in $\mathrm{GL}_1(\widehat{\mathbf{Z}})$.

3. Let n be a positive integer, and B the collection of monic polynomials of degree n in $\mathbf{Z}[X]$. For $t \in \mathbf{R}_{>0}$, define $B_t \subset B$ as the finite subset of polynomials in B for which all coefficients are bounded in absolute value by t. Show that the irreducible polynomials in B have density 1, i.e.,

$$\lim_{t\to\infty} \frac{\#\{f \in B_t : f \text{ is irreducible}\}}{\#B_t} = 1.$$

   [Hint: if f is reducible, then $f \bmod p$ is not an irreducible polynomial in $\mathbf{F}_p[X]$ for any prime p.]

4. Let L be the splitting field of the polynomial $f = X^2 - X + 1$.
   (a) Can you characterize the primes p that split completely in the ring of integers of L? Are there infinitely many of them?
   (b) Same questions for $f = X^2 - X + 2$.

For the following exercises, it may be profitable to use the (free) gp-online calculator `https://pari.math.u-bordeaux.fr/gp.html` or something equivalent.

5. Take $f_1 = X^3 - X^2 - 2X - 1 \in \mathbf{Z}[X]$ and $f_2 = X^3 - X^2 - 2X + 1 \in \mathbf{Z}[X]$, and let $K_i = \mathbf{Q}[X]/(f_i)$ for $i = 1, 2$ be the associated cubic number fields.
   (a) Show that from the 25 primes $p \le 100$, only the prime 31 is ramified in K_1, and that for the 24 other values of $p \le 100$ the number of p with 1, 2 and 3 extension primes in K_1 is 8, 14, and 2, respectively.

(b) Show that from the 25 primes $p \leq 100$, only the prime 7 is ramified in K_2, and that for the 24 other values of $p \leq 100$, the number of p with 1, 2 and 3 extension primes in K_1 is 17, 0, and 7, respectively.

(c) Explain the different behavior of f_1 and f_2.

(d) Can you characterize the primes that split completely in K_2, and quantify how many there are?

(e*) Can you characterize the primes that split completely in K_1, and quantify how many there are?

6. Define for $i = 1, 2$ the elliptic curves $E_i/\mathbf{Q}$ by the Weierstrass equation $y^2 + xy = f_i(x)$, with f_i as in the previous exercise.

   (a) Show that E_1 and E_2 have short Weierstrass models given by $y^2 = x^3 - 35x - 98$ and $y^2 = x^3 - 35x + 30$, respectively.

   (b) Show that $E_1(\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z}$ is generated by the torsion point $(2, -1)$, and that $E_2(\mathbf{Q}) \cong \mathbf{Z}$ is generated by the point $(0, 1)$ of infinite order.

   (c) Show that E_1 has CM by $\mathbf{Z}[\frac{1+\sqrt{-7}}{2}]$ defined over $\mathbf{Q}(\sqrt{-7})$, and that E_2 has no CM over $\overline{\mathbf{Q}}$.