Sample Questions from Past Qualifying Exams

This list may give the impression that the exams consist of a series of questions fired at the student one after another. In fact most exams have more the character of a conversation with considerable give and take. Hence this list cannot be expected to indicate accurately the difficulties involved.

The list indicates the professor associated to each question where available. Some have been in the MGSA files for a while, and this information has been lost (if it was ever there).

The listing by section is approximate, since some questions may fit under more than one heading.

Number Theory

- Prove that the class group of a number field is finite. [**Ribet**]
- What is your favorite proof of quadratic reciprocity? [**Ribet**]
- Prove that there exists a field of order p^n for every prime p and positive integer n. [**Peres** (Stat)]
- Prove that $\mathbb{Q}[\sqrt{3}]$ has no unramified extensions. [**Ribet**]
- Describe the ring of integers in $\mathbb{Q}(\zeta_{p^\infty})$. [**Coleman**]
- Tell me about integral extensions. [**Hartshorne**] item• What is a Dedekind domain? [**Hartshorne**]
  - An example of a domain which is noetherian, integrally closed, and not one-dimensional.
  - An example of a domain which is integrally closed, one-dimensional, and not noetherian.
- State Leopoldt's conjecture. [**Coleman**]
- State the main theorem of Class Field Theory in terms of idèles. [**Coleman**]
  - Define idèles.
  - Give the Class Field Theory correspondence.
  - What subgroup corresponds to the kernel of the Artin map for unramified extensions?
  - Describe the maximal abelian extension L of $\mathbb{Q}$ unramified outside p explicitly, using the idèlic formulation of Class Field Theory.
  - Show that $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}^\times$ directly, from the Artin map on idèles.
- Why are elliptic curves important in number theory?
- Say everything you can about $\mathbb{Q}(\sqrt{-5})$: ring of integers, discriminant, which primes ramify, split or remain inert, and whether $\mathbb{Z}[\sqrt{-5}]$ is a PID. What is the class number?
- Let $K = \mathbb{Q}(\alpha)$, where $\mathrm{Irr}_{\alpha,\mathbb{Q}}(x) = x^3 + 2x + 1$. What is D_K (the discriminant)? Which primes ramify in K? What is the splitting behavior of 2 and of 3?
- Let $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ be the splitting field of $x^3 + 2x + 1$ over $\mathbb{Q}$. (i.e., α_i are the roots). What is $\mathrm{Gal}(L/\mathbb{Q})$? How does 59 ramify in $K = \mathbb{Q}(\alpha_1)$? In L?

- Is 79 a square mod 445?
- What is the product formula for $\mathbb{Q}$? For a number field K? Prove them.
- Which primes ramify, split or stay inert in $\mathbb{Q}(\sqrt{3})$?
- In $\mathbb{Z}[\sqrt{-3}]$ let $\mathbf{a} = (2, 1+\sqrt{-3})$. Show that $\mathbf{a} \not= (2)$, but $\mathbf{a}^2 = 2\mathbf{a}$. Conclude that ideals in $\mathbb{Z}[\sqrt{-3}]$ do not factor uniquely into prime ideals.
- Prove that $x^8 + 1$ is irreducible over $\mathbb{Q}$.
- What is the splitting field of $x^8 + 1$ over $\mathbb{Q}$. Call it K.
  - What is $\mathrm{Gal}(K/\mathbb{Q})$?
  - Which primes ramify in K?
  - Using only the preceding two questions, what are the quadratic extensions of $\mathbb{Q}$ lying inside of K?
  - For which primes p is $x^8 + 1$ irreducible mod p over $\mathbb{F}_p$?
  - What is the rank of the unit group in K?
- Which integers are sums of two squares?
- Show that 2 splits completely in $\mathbb{Q}(\sqrt{17})$ but remains inert in $\mathbb{Q}(\sqrt{13})$.
- Write down a polynomial f over $\mathbb{Q}_3$ such that $\mathbb{Q}_3[x]/(f)$ is a totally ramified quartic extension of $\mathbb{Q}_3$.
- What are the main statements of class field theory?
- Say all you can about cyclotomic extensions and cyclotomic polynomials.
- For any d squarefree integer, find the units in the ring of integers of $\mathbb{Q}(\sqrt{d})$.
- Does 5 have a square root in $\mathbb{Q}_3$.
- Let K be obtained from $\mathbb{Q}$ by adjoining a root of $x^3 + x + 1$. What are the possible ways a prime can ramify in K? [**Poonen**]
- Suppose -31 is not a square mod p where p is a prime. What can you say about $K \otimes \mathbb{Q}_p$? [**Poonen**]
- Let L be the Galois closure of K. Prove that L is the Hilbert Class field of $\mathbb{Q}(\sqrt{-31})$. [**Poonen**]
- What are the possible extensions of degree 3 of $\mathbb{Q}_2$? [**Poonen**]
- State the Kronecker-Weber theorem. Sketch a proof if possible. [**Lenstra**]
- Prove that the Galois group of the maximal cyclotomic extension of $\mathbb{Q}$ is the product of the groups of p-adic units. [**Lenstra**]
- Give a canonical decomposition of the ideles of $\mathbb{Q}$. [**Lenstra**]
- Give a natural generalization of this product for a general number field K. Show that there is always a map from the product to the ideles of K. What is its kernel? What is its cokernel? [**Lenstra**]
- Let $f = X^3 - X^2 - 2X + 1$. Show that f is irreducible over $\mathbb{Q}$. [**Lenstra**]

- Let $K = Q[X]/f$. Show that K is abelian. You can use the fact that the discriminant of f is 49. [**Lenstra**]
- Find the discriminant of K and its ring of integers. Which non-archimedean primes ramify in K? [**Lenstra**]
- Does the infinite prime ramify in K? [**Ribet**]
- If a prime p is unramified in K, what does this mean about the Artin map corresponding to K? [**Lenstra**]
- Using class field theory, find a cyclotomic extension of $\mathbb{Q}$ which contains K. [**Lenstra**]
- Why is the Mordell-Weil theorem not effective? [**Ribet**]
- Prove the Mordell-Weil theorem. [**Ribet**]
- Let $P \in E(K)$, and let $\{Q\}$ be the set of points such that $nQ = P$. Describe the Galois theory of $\mathbb{Q}(\{Q\})$. [**Ribet**]
- What is the endomorphism ring of $y^2 + y = x^3$ over $\mathbb{F}_2$? What about $\mathrm{End}_{\mathbb{F}_2}(E)$? [**Poonen**]
- Show that the endomorphism ring of an elliptic curve of characteristic p is ramified over at most p and ∞. [**Poonen**]
- Is the (geometric) Frobenius always defined over $\mathbb{F}_p$? [**Poonen**]