COMPREHENSIVE EXAM IN ALGEBRAIC NUMBER THEORY (FALL 2014)

Recall that the **Minkowski bound** is

$$N(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s |\Delta_K|^{1/2}.$$

Please choose either the (E) (elementary) or (A) algebraic questions. You don't need to do both (although you can!)

1. Let K be the cubic field generated by a root of $x^3 + x^2 + 1$. Determine the following data associated to K:
   (a) its **discriminant**;
   (b) the **ring of integers**;
   (c) the number of **real and complex embeddings**;
   (d) the isomorphism class of its **unit group** (your answer should look like, e.g., $\mathbb{Z}^2 \times \mathbb{Z}/(6)$; you do not need to find the actual units);
   (e) the list of **ramified primes**;
   (f) the splitting types of the ideals $(2), (3), (5), (7)$;
   (g) whether or not K is **Galois** over $\mathbb{Q}$; and if not, the Galois group of its Galois closure (i.e., the splitting field of $x^3 + 2x - 1$);
   (h) (bonus: if you can) the **the class group**;
   (i) (bonus: if you can) the **proportion of primes** which have the splitting types you found above.

2. Let K be the quartic field generated by a root of $f(x) := x^4 - x^3 - 2x^2 - 3x - 2$, and let L be its Galois closure. The aim of this exercise is to give a (partial) proof that its Galois group is S_4.
   (a) The discriminant of the ring generated by a root α of $f(x)$ is -3751. Give a sketch of how you would prove this.
   (b) What are the possible values for $\mathrm{Disc}(K)$? (Bonus: actually determine $\mathrm{Disc}(K)$.)
   (c) State an appropriate theorem which identifies an element of $\mathrm{Gal}(L/\mathbb{Q})$ in terms of the splitting of a prime p in $\mathcal{O}_K$.
   (d) By proving that $\mathrm{Gal}(L/\mathbb{Q})$ contains 'enough' elements, prove that it is all of S_4. If this becomes tedious, begin a proof and explain in detail how you would finish.
   Be sure not to assume that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ unless you proved it previously.
   (e) If $f(x)$ instead generated a D_4 extension, it would be much more difficult to prove this. Explain why.

3. (a) Define the p-adic integers $\mathbb{Z}_p$ (in any way you choose). Determine, with proof, the maximal ideal $\mathfrak{m}$ and the residue class field $\mathbb{Z}_p/\mathfrak{m}$.
   (b) Write out 5-adic expansions for $\frac{1}{4}$, 7, and $\sqrt{6}$ in $\mathbb{Q}_5$. (First three digits for $\sqrt{6}$.)

(c) (E) It is known that any element of $\mathbb{Q}$ has a repeating decimal expansion when written in $\mathbb{R}$. Determine, with a proof or counterexamples, whether this result extends in a natural way to the p-adics.

(d) Suppose you defined the 10-adic integers in an analogous way to the p-adics. State your definition precisely, and then prove that you don't obtain an integral domain.

(e) (A) Like Z, $\mathbb{C}[x]$ is also a principal ideal domain. Define what should be the analogue of $\mathbb{Z}_p$ for $\mathbb{C}[x]$, and describe the rings you obtain by your construction.

4. Compute the ring of integers and class group of $\mathbb{Q}(\sqrt{39})$.

5. (E) Let K be the number field generated by a root of $x^5 + 2x + 10$. It turns out that its ring of integers is generated by a root of this polynomial. Given this, compute $\mathrm{Disc}(K)$.

6. (A) Let L/K be an extension of number fields, let $\mathcal{O}_L$ and $\mathcal{O}_K$ be their rings of integers, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. We are interested in proving that $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is an $\mathcal{O}_K/\mathfrak{p}$-vector space of dimension $n := [L : K]$. (This is an important step in the efg theorem.)

(a) Can we write the following, for some $\alpha_i \in \mathcal{O}_K$?

$$\mathcal{O}_L = \mathcal{O}_K\alpha_1 \oplus \cdots \oplus \mathcal{O}_K\alpha_n \tag{1}$$

If not in general, by quoting a relevant theorem give an example of a K for which we can do this.

(b) Assume that (1) holds. Prove that the images of the α_i under the natural reduction map modulo $\mathfrak{p}$ form a basis for $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ as an $\mathcal{O}_K/\mathfrak{p}$-vector space, thereby obtaining the result. You may (and almost certainly will) give a proof that requires an condition on $\mathcal{O}_K$. This is allowed, if you state your condition explicitly and if it does not restrict your proof to only $K = \mathbb{Q}$.