# Math 249B. Homework 2

1. This first exercise is some reading.

(*i*) Read the handout on Galois groups and abelianizations.

(*ii*) (optional) An application of Minkowski's Lemma which was omitted in Math 248A was to show Hermite's theorem that up to isomorphism there are only *finitely many* number fields with a given discriminant. This is proved at the end of §4.3 of Samuel's "Algebraic theory of numbers", and also in (2.16) of Ch. III in Neukirch's "Algebraic number theory". (A key ingredient in the proof is that bounding the discriminant of a number field actually bounds its degree.)

In another direction, related arguments show that if we fix not the discriminant but rather its set of prime factors and we also bound the degree of the number field then once again there are only *finitely many* such number fields up to isomorphism. More generally, for *any* number field $K$ (not just $\mathbf{Q}$), up to $K$-isomorphism there are only *finitely many* extensions $L/K$ with a specified degree and unramified away from a given finite set $S$ of places of $K$. This is Theorem 2.13 in Ch. III of Neukirch's book, for example. This latter finiteness result (in its relative formulation) is true with $K$ allowed to be a global function field provided that we require $L/K$ to have Galois closure with degree not divisible by the characteristic (it is false otherwise, as you will show in HW3). To prove it one of course has to replace Minkowski's Lemma with some other technique, and the only method I know requires some serious input from algebraic geometry (SGA1).

2. (*i*) Prove that the natural map $\mathbf{R}_{>0}^{\times} \times \widehat{\mathbf{Z}}^{\times} \rightarrow \mathbf{A}_{\mathbf{Q}}^{\times}$ is a homeomorphism onto an open subgroup.

(*ii*) Prove that the induced map $\mathbf{R}_{>0}^{\times} \times \widehat{\mathbf{Z}}^{\times} \rightarrow \mathbf{A}_{\mathbf{Q}}^{\times}/\mathbf{Q}^{\times}$ is an isomorphism of topological groups.

(*iii*) Let $K$ be a number field. Prove that the natural ring map $\widehat{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathscr{O}_K \rightarrow \prod_{v \nmid \infty} \mathscr{O}_v$ is a topological isomorphism, and relate $\mathrm{Cl}(K)$ (resp. $\mathscr{O}_K^{\times}$) to the cokernel (resp. kernel) of the map $(K \otimes_{\mathbf{Q}} \mathbf{R})^{\times} \times \prod_{v \nmid \infty} \mathscr{O}_v^{\times} \rightarrow \mathbf{A}_K^{\times}/K^{\times}$.

3. Let $K$ be a non-archimedean local field with residue field $k$ of characteristic $p > 0$. For $m > 0$ not divisible by $p$, prove that $K(\zeta_m)$ is the unramified extension of $K$ corresponding to the extension $k(\zeta_m)$ of $k$. Also prove that the resulting isomorphism $\mathrm{Gal}(K(\zeta_m)/K) \simeq \mathrm{Gal}(k(\zeta_m)/k)$ respects the natural identification of each group with a subgroup of $(\mathbf{Z}/m\mathbf{Z})^{\times}$.

4. Let $f = X^3 - X - 1$, $K = \mathbf{Q}(\sqrt{-23})$.

(*i*) Prove that $f$ is irreducible with discriminant $-23$, and that the resulting cubic extension $F = \mathbf{Q}(\alpha)$ (with $f(\alpha) = 0$) is ramified over $\mathbf{Q}$ at precisely two places: a 23-adic place of $F$ and a complex place of $F$. Show that the ramification index for the ramified 23-adic place is 2 (not 3).

(*ii*) Prove that the Galois closure $L$ of $F$ over $\mathbf{Q}$ contains $K$ and is identified with $K(\alpha)$. (In particular, $f$ is irreducible over $K$.) Show that $L/K$ is a cubic abelian extension that is unramified at all places.

**Remark**. One can check that $K$ has class number 3, so $L = K(\alpha)$ is the Hilbert class field of $K$. This underlies the "right" explanation of the classically-known (but mysterious) fact that for positive primes $p \neq 23$ the property that $p$ has the form $x^2 + 23y^2$ with $x, y \in \mathbf{Z}$ is governed by congruential conditions on $p \bmod 23$ *and* the number of roots of $f \bmod p$ in $\mathbf{F}_p$. (Contrast this with the classical fact that whether or not $p = x^2 + y^2$ amounts to a *purely* congruential condition on $p \bmod 4$ for odd $p$.) The intervention of counting solutions to $f(x) \equiv 0 \bmod p$ is best explained by using the main theorems of class field theory: it is due to $K = \mathbf{Q}(\sqrt{-23})$ having Hilbert class field $L \simeq K[X]/(f)$ (in contrast with $\mathbf{Q}(\sqrt{-1})$, whose Hilbert class field is trivial!).