Math 5230 - Algebraic Number Theory (Fall 2012) Due by email
Problem Set 7: **Work on your own!** 12/15/12 at 4 PM

If there is one thing in mathematics that fascinates me more than anything else (and doubtless always has), it is neither "number" nor "size", but always form. And among the thousand-and-one faces whereby form chooses to reveal itself to us, the one that fascinates me more than any other and continues to fascinate me, is the structure hidden in mathematical things. Grothendieck

1. (In this problem, you can use `nfbasis` and `nfdisc` in PARI to compute bases for the ring of integers and discriminants of number fields.)

   a) Use the Minkowski bound to prove $\mathbf{Q}(\sqrt{101})$, $\mathbf{Q}(\sqrt{-163})$, and $\mathbf{Q}(\zeta_5)$ have class number 1. (Be careful: for prime p, the degree of $\mathbf{Q}(\zeta_p)$ over $\mathbf{Q}$ is $p-1$, *not* p.)

   b) Use the Minkowski bound to prove $\mathbf{Q}(\sqrt{-31})$ has class number 3 and a prime ideal dividing (2) generates the ideal class group.

   c) The cubic field $\mathbf{Q}(\alpha)$, where $\alpha^3 - \alpha - 10 = 0$, has class number 4. Accepting this, use the Minkowski bound to determine whether the class group is cyclic or a direct product of two groups of order 2. (Bonus: prove the class number is 4 from scratch.)

2. Redo the proof of the Minkowski bound using the convex and centrally-symmetric region

$$X_t = \{(x_1, \ldots, z_1, \ldots) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} : |x_i| < t, |z_j| < t\}.$$

   This is a simpler type of region than the one in the proof from class: if an algebraic integer has Euclidean image in X_t, its norm has absolute value at most t^n, a bound that does not need anything like the arithmetic-geometric mean inequality.

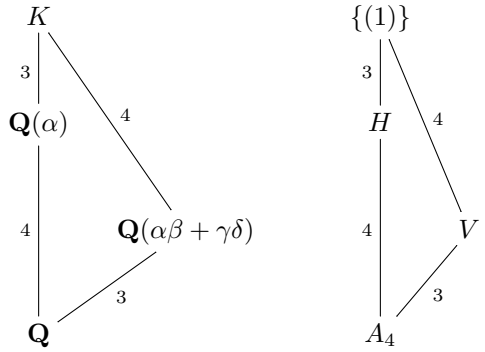
   Using X_t for suitable t, for what bound M can you conclude each nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ contains a nonzero element α such that $|\,\mathrm{N}_{K/\mathbf{Q}}(\alpha)| \leq M\,\mathrm{N}(\mathfrak{a})$? (Be sure you compute the volume of X_t correctly. It is generally *not* $(2t)^n$.) Show this bound is *always* weaker than the Minkowski bound when $n \geq 3$ (what if $n = 2$?). Does this alternate bound allow you to prove every number field $K \neq \mathbf{Q}$ has $|\,\mathrm{disc}(K)| > 1$?

3. Let $K = \mathbf{Q}(r)$, where $r^3 - 3r - 1 = 0$. You looked at this number field on Set 6.

   a) In PARI, the class group command `bnfclgp(x^3 - 3*x - 1)` tells you that $h(K) = 1$. Prove this using the Minkowski bound.

   b) By the unit theorem, $\mathcal{O}_K^\times$ has rank $3 + 0 - 1 = 2$. Show r, $r+1$, $r-2$, and $2r+3$ are all units; they have infinite order since they are not ± 1 (the only roots of unity in a field with a real embedding). Compute the log mapping $L\colon K^\times \to \mathbf{R}^3$ numerically at these four units and use PARI (*e.g.*, the `matker` command) to discover a $\mathbf{Z}$-linear multiplicative relation among $L(r)$, $L(r+1)$, and the log mapping at each of the other two units. Use that to discover a formula for $r-2$ and $2r+3$ as a product of powers of r and $r+1$, up to multiplication by a definite sign ± 1.

4. The polynomial $T^4 + 8T + 12$ is irreducible over $\mathbf{Q}$ and its splitting field $K/\mathbf{Q}$ has degree 12; the group $\mathrm{Gal}(K/\mathbf{Q})$ looks like A_4 as a permutation group on the four roots. Write the four roots of $T^4 + 8T + 12$ as $\alpha, \beta, \gamma, \delta$. Depending on the ordering of these roots, $\alpha\beta + \gamma\delta$ can take on three possible values and (by PARI, say) they share the same minimal polynomial $T^3 - 48T - 64$ in $\mathbf{Q}[T]$. Since $T^3 - 48T - 64 = 64((T/4)^3 - 3(T/4) - 1)$ in $\mathbf{Q}[T]$, $\mathbf{Q}(\alpha\beta + \gamma\delta)$ is the cubic Galois extension of $\mathbf{Q}$ in the previous exercise. Here is a field diagram, where V is the unique (normal) subgroup of index 3 in A_4. Explicitly, $V = \{(1), (12)(34), (14)(23), (13)(24)\}$.



a) Using the equation of principal ideals $(2)^2(3) = (\alpha)(\alpha^3 + 8)$ in $\mathbf{Q}(\alpha)$, show $(3) = \mathfrak{p}_3\mathfrak{p}_3'^3$ as ideals in the integers of $\mathbf{Q}(\alpha)$. (Hint: $\alpha^3 + 8$ can be factored a little further.)

b) Use PARI's `nfbasis` command to find a $\mathbf{Z}$-basis for the ring of integers of $\mathbf{Q}(\alpha)$; it is not $\mathbf{Z}[\alpha]$. Then use `algdep` to find the minimal polynomials of the members of that basis not in $\mathbf{Z}[\alpha]$ to prove that 2 is totally ramified in K, and thus $(2) = \mathfrak{p}_2^4$ in $\mathbf{Q}(\alpha)$.

c) By looking at the factorizations of 2 and 3 in $\mathbf{Q}(\alpha)$ and in $\mathbf{Q}(\alpha\beta+\gamma\delta)$, show the decomposition and inertia groups over 2 in $\mathrm{Gal}(K/\mathbf{Q})$ are A_4 and V respectively, while the decomposition and inertia groups over 3 in $\mathrm{Gal}(K/\mathbf{Q})$ are the subgroups conjugate to H. (Hint: there is no subgroup in A_4 of order 6, so no decomposition group in $\mathrm{Gal}(K/\mathbf{Q})$ can have order 6.)

d) Conjugacy classes in A_4 are $\{(1)\}$, $\{(12)(34), (13)(24), (14)(23)\}$, $\{(123), (134), (142), (243)\}$, and $\{(132), (143), (124), (234)\}$. The cycle types in the third and fourth conjugacy classes are the same, so only when $T^4 + 8T + 12 \bmod p$ decomposes as a linear times a cubic does that factorization not predict the Frobenius conjugacy class of p in $\mathrm{Gal}(K/\mathbf{Q})$.

The restriction homomorphism $\mathrm{Gal}(K/\mathbf{Q}) \to \mathrm{Gal}(\mathbf{Q}(\alpha\beta + \gamma\delta)/\mathbf{Q})$ corresponds to the natural reduction $A_4 \to A_4/V$ by Galois theory. Your task: show the two conjugacy classes of 3-cycles in A_4 are sent to different nontrivial cosets in $A_4/V \cong \mathbf{Z}/(3)$ and then explain why, if $T^4 + 8T + 12 \bmod p$ is a linear times a cubic irreducible, then the Frobenius conjugacy class of $p \neq 2, 3$ in $\mathrm{Gal}(K/\mathbf{Q})$ is determined by the Frobenius at p in $\mathrm{Gal}(\mathbf{Q}(\alpha\beta + \gamma\delta)/\mathbf{Q})$.

e) Use PARI to compute the Frobenius conjugacy class of p in $\mathrm{Gal}(K/\mathbf{Q})$ for $3 < p < 100$. List the primes with a common Frobenius conjugacy class, so there will be four lists. (Distinguish between the conjugacy classes of 3-cycles by declaring one to be the Frobenius conjugacy class of 5 and the other to be the Frobenius conjugacy class of 7, which are different by Set 6.)