Math 5230 - Algebraic Number Theory (Fall 2012) Due in MSB 318
Problem Set 6 11/16/12 at 4 PM

I [resolved to] study whatever [Hilbert] had written. At the end of my first year I went home with the "Zahlbericht" under my arm, and during the summer vacation I worked my way through it–without any previous knowledge of elementary number theory or Galois theory. These were the happiest months of my life, whose shine, across years burdened with our common share of doubt and failure, still comforts my soul. H. Weyl

1. Let $K = \mathbf{Q}(\alpha)$ where α is a root of $T^3 - T^2 - 34T - 24$.

   a) Show the polynomial is irreducible over $\mathbf{Q}$ with three real roots.

   b) Show $\mathrm{disc}(K) = 32009$.

   c) Find a $\mathbf{Z}$-basis for $\mathcal{O}_K$.

   d) On the previous problem set you met three cubic fields with discriminant 32009 that are not isomorphic to each other. Prove K is not isomorphic to any of them.

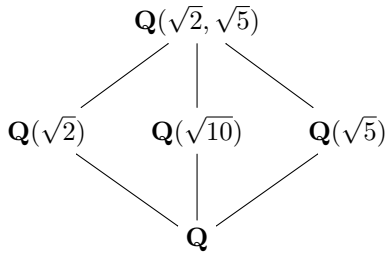
   e) Show $\mathcal{O}_K \neq \mathbf{Z}[\gamma]$ for any γ by the same method used with Dedekind's field on Set 4.

2. Let $K/\mathbf{Q}$ be a Galois extension and $K = \mathbf{Q}(\alpha)$ for an algebraic integer α having minimal polynomial $f(T) \in \mathbf{Z}[T]$.

   a) If $p \nmid \mathrm{disc}\, f$ then show the irreducible factors of $f(T)$ mod p all have the same degree. (Note: It is **not** assumed that $\mathcal{O}_K = \mathbf{Z}[\gamma]$ for any γ. You should make essential use of the fact that $p \nmid \mathrm{disc}\, f$.)

   b) Find an example of a Galois extension of $\mathbf{Q}$ where $p \mid \mathrm{disc}\, f$ and the irreducible factors of $f(T)$ mod p do *not* have the same degree.

3. Let $K = \mathbf{Q}(\sqrt{2}, \sqrt{5})$. Its lattice of subfields is given below, and $\mathrm{Gal}(K/\mathbf{Q}) = \{1, \sigma, \tau, \sigma\tau\}$, where $\sigma(\sqrt{2}) = -\sqrt{2}, \sigma(\sqrt{5}) = \sqrt{5}$, $\tau(\sqrt{2}) = \sqrt{2}$, and $\tau(\sqrt{5}) = -\sqrt{5}$.



   a) Show $\mathcal{O}_K = \mathbf{Z}[\sqrt{2}, \frac{1+\sqrt{5}}{2}]$ and compute $\mathrm{disc}(K)$. (Don't say "By PARI...")

   b) Since $\mathrm{Gal}(K/\mathbf{Q})$ is abelian, decomposition and inertia groups only depend on the prime downstairs. Compute $D_2(K/\mathbf{Q})$, $I_2(K/\mathbf{Q})$, $D_5(K/\mathbf{Q})$, and $I_5(K/\mathbf{Q})$.

   c) Compute $\mathrm{Fr}_p(K/\mathbf{Q})$ for $p = 3, 7, 11$, and 13. Then use your answers to conjecture and then prove a rule for determining $\mathrm{Fr}_p(K/\mathbf{Q})$ for $p \neq 2$ or 5 based on how $T^2 - 2$ mod p and $T^2 - 5$ mod p factor.

4. Let $K = \mathbf{Q}(r)$, where $r^3 - 3r - 1 = 0$. This is a cubic Galois extension of $\mathbf{Q}$, with r having $\mathbf{Q}$-conjugates $2 - r^2$ and $r^2 - r - 2$. Let $\sigma(r) = 2 - r^2$.

   a) Show $\mathcal{O}_K = \mathbf{Z}[r]$ and $\mathrm{disc}(K) = 81$.

   b) Compute $\mathrm{Fr}_p(K/\mathbf{Q})$ for all primes $p \leq 23$ except 3. Each Frobenius element will be 1, σ, or σ^2.

5. Let $K = \mathbf{Q}(\sqrt[4]{3}, i)$, so $\mathrm{Gal}(K/\mathbf{Q}) = \langle r, s \rangle \cong D_4$, where $r(\sqrt[4]{3}) = i\sqrt[4]{3}$, $r(i) = i$, and $s(\sqrt[4]{3}) = \sqrt[4]{3}$, $s(i) = -i$.

   a) Inside K is $\sqrt{-3} = i\sqrt{3}$. Look at the decomposition of 2 in the subfields $\mathbf{Q}(\sqrt{-3})$ and $\mathbf{Q}(\sqrt[4]{3})$ to determine the values of $e_2(K/\mathbf{Q})$, $f_2(K/\mathbf{Q})$, and $g_2(K/\mathbf{Q})$.

   b) Compute the decomposition and inertia groups at a prime over 2 in K.

   c) Compute a Frobenius element at some prime over 2 in $\mathrm{Gal}(K/\mathbf{Q})$. (Since 2 is ramified, it does not have a Frobenius conjugacy class.)

   d) Determine how 11 factors into prime ideals in K and find its Frobenius conjugacy class in $\mathrm{Gal}(K/\mathbf{Q})$.