Math 5230 - Algebraic Number Theory (Fall 2012) Due in MSB 318
Problem Set 4 10/22/12 at 4 PM

*The further elaboration and development of systematic arithmetic, like nearly everything else which the mathematics of our [nineteenth] century has produced in the way of original scientific ideas, is knit to Gauss.* Kronecker

1. a) In the ring $\mathbf{Z}[\sqrt{-5}]$, find an element of the ideal $(6, 2+7\sqrt{-5})$ that is not in the $\mathbf{Z}$-span of 6 and $2+7\sqrt{-5}$. Thus $(6, 2+7\sqrt{-5}) \neq \mathbf{Z}6 + \mathbf{Z}(2+7\sqrt{-5})$.

   b) Let $d$ be a nonsquare integer. In $\mathbf{Z}[\sqrt{d}]$, let $\mathfrak{a}$ be the ideal $(a, b+c\sqrt{d})$, where $a$, $b$, and $c$ are integers and $a$ and $c$ are not 0. So as a $\mathbf{Z}[\sqrt{d}]$-module,

$$\mathfrak{a} = \mathbf{Z}[\sqrt{d}]a + \mathbf{Z}[\sqrt{d}](b+c\sqrt{d}),$$

   while as a $\mathbf{Z}$-module

$$\mathfrak{a} = \mathbf{Z}a + \mathbf{Z}a\sqrt{d} + \mathbf{Z}(b+c\sqrt{d}) + \mathbf{Z}(cd+b\sqrt{d}).$$

   It is natural to ask: does $\mathfrak{a} = \mathbf{Z}a + \mathbf{Z}(b+c\sqrt{d})$?

   Show $\mathfrak{a} = \mathbf{Z}a + \mathbf{Z}(b+c\sqrt{d})$ if and only if the following three conditions are all satisfied: $c \mid a$, $c \mid b$, and $d \equiv (b/c)^2 \bmod a/c$. (In particular, when $\mathfrak{a} = (a, b\pm\sqrt{d})$, we have $\mathfrak{a} = \mathbf{Z}a+\mathbf{Z}(b\pm\sqrt{d})$ if and only if $d \equiv b^2 \bmod a$.)

   c) In $\mathbf{Z}[\sqrt{-5}]$, part b implies that none of the ideals $(6, 2+7\sqrt{-5})$, $(3, 1+2\sqrt{-5})$, or $(7, 2+3\sqrt{-5})$ have the given ideal generators as a $\mathbf{Z}$-basis. Compute a $\mathbf{Z}$-basis for each ideal and use that $\mathbf{Z}$-basis to compute the norm of each ideal.

2. Describe the prime ideal factorization in $\mathbf{Z}[\sqrt{-6}]$ of all prime numbers less than 20, not just in terms of the shape of the factorization but also giving explicit generators for each prime ideal that appears.

3. (Dedekind's field, continued) Let $K = \mathbf{Q}(\alpha)$, where $\alpha^3 - \alpha^2 - 2\alpha - 8 = 0$.

   a) For any nonzero prime $\mathfrak{p}$ in $\mathcal{O}_K$ with $\mathfrak{p}|(2)$, prove $\mathfrak{p}|(\alpha)$ or $\mathfrak{p}|(\alpha-1)$, but not both.

   b) Compute $\mathrm{N}_{K/\mathbf{Q}}(\alpha+c)$ for $c \in \mathbf{Z}$ and use this to factor $(\alpha-1)$ into prime ideals. (Specify the norm of each prime.)

   c) Use parts a and b to show the ideal (2) must have at least two prime factors which do not divide $(\alpha-1)$, and therefore $(2) = \mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_2''$ with the prime factors all distinct. (Hint: Think about prime ideal factors of $(\alpha)$, $(\alpha-1)$, and $(\alpha-2)$.)

   d) Use part c to show $\mathcal{O}_K/(2) \cong \mathbf{F}_2 \times \mathbf{F}_2 \times \mathbf{F}_2$ as a ring, and explain from this why $\mathcal{O}_K \neq \mathbf{Z}[\gamma]$ for any $\gamma \in \mathcal{O}_K$. Thus, Dedekind's field does not admit a power basis for its ring of integers. (This was the first known example of a ring of integers without a power basis.)

   e) Factor the ideals $(\alpha)$, $(\alpha+1)$, $(\alpha+2)$, $(\alpha-2)$, $(\alpha+3)$, and $(\alpha-3)$ into primes, specifying the norm of each prime that appears. Continue the notation for ideals used in parts b and c.

4. For $i = 1, 2, 3$, define four cubic fields $K_i = \mathbf{Q}(\alpha_i)$ where $\alpha_i$ is the root of $f_i(T)$:

$$\begin{aligned} f_1(T) &= T^3 - T^2 - 20T - 1, \\ f_2(T) &= T^3 - T^2 - 52T + 159, \\ f_3(T) &= T^3 - 41T - 95. \end{aligned}$$

a) Show all three polynomials are irreducible over $\mathbf{Q}$ with three real roots.

b) Show all three number fields have prime discriminant 32009.

c) Find a basis for the ring of integers of each field.

d) Although these three number fields have the same degree and discriminant, prove they are nonisomorphic by finding prime numbers that factor in different ways in each pair of fields.

5. Let $K/F$ and $L/F$ be finite extensions in a common larger field, with $m = [K : F]$ and $n = [L : F]$. Suppose $[KL : F] = mn$.

Let $e_1, \dots, e_m$ be an $F$-basis of $K$ and $f_1, \dots, f_n$ be an $F$-basis of $L$.

a) Prove $\{e_i f_j\}$ is an $F$-basis of $KL$.

b) Use part a to prove for $\alpha \in K$ that $\chi_{KL/L,\alpha}(T) = \chi_{K/F,\alpha}(T)$. In particular, for $\alpha \in K$, $\mathrm{Tr}_{KL/L}(\alpha) = \mathrm{Tr}_{K/F}(\alpha)$.

c) Use parts a and b and transitivity of the trace map ($\mathrm{Tr}_{KL/F} = \mathrm{Tr}_{L/F} \circ \mathrm{Tr}_{KL/L}$) to show

$$\mathrm{disc}_{KL/F}(\{e_i f_j\}) = \mathrm{disc}_{K/F}(\{e_i\})^n \, \mathrm{disc}_{L/F}(\{f_j\})^m.$$

(Hint: The right side of this equation resembles the formula for the determinant of a tensor product of linear transformations: $\det(\varphi \otimes \psi) = (\det \varphi)^n (\det \psi)^m$ where $\varphi$ acts on an $m$-dimensional $F$-vector space and $\psi$ acts on an $n$-dimensional $F$-vector space. Review the matrix representation of a tensor product of linear maps.)

d) Now we give an application to number fields. Let $K$ and $L$ be number fields of respective degrees $m$ and $n$ over $\mathbf{Q}$ and assume $[KL : \mathbf{Q}] = mn$. Set

$$d = (\mathrm{disc}(\mathcal{O}_K), \mathrm{disc}(\mathcal{O}_L)) \quad \text{and} \quad \mathcal{O}_K\mathcal{O}_L = \left\{ \sum_{k=1}^{r} x_k y_k : r \geq 1, x_k \in \mathcal{O}_K, y_k \in \mathcal{O}_L \right\},$$

so trivially $\mathcal{O}_K\mathcal{O}_L \subset \mathcal{O}_{KL}$. Show $\mathcal{O}_{KL} \subset \frac{1}{d}\mathcal{O}_K\mathcal{O}_L$ and $\mathrm{disc}_{\mathbf{Z}}(\mathcal{O}_K\mathcal{O}_L) = \mathrm{disc}(\mathcal{O}_K)^n \, \mathrm{disc}(\mathcal{O}_L)^m$. (In particular, if $[KL : \mathbf{Q}] = [K : \mathbf{Q}][L : \mathbf{Q}]$ and $K$ and $L$ have relatively prime discriminants, then $\mathcal{O}_{KL} = \mathcal{O}_K\mathcal{O}_L$ and $\mathrm{disc}(\mathcal{O}_{KL}) = \mathrm{disc}(\mathcal{O}_K)^n \, \mathrm{disc}(\mathcal{O}_L)^m$.)

(Hint: First show $\mathcal{O}_{KL} \subset \frac{1}{\mathrm{disc}(\mathcal{O}_K)}\mathcal{O}_K\mathcal{O}_L$. Then switch the roles of $K$ and $L$.)

6. Let $F$ be a field not of characteristic 2 and $f(X)$ be a nonconstant squarefree[1] polynomial in $F[X]$. The polynomial $Y^2 - f(X) \in F(X)[Y]$ is irreducible (Eisenstein at any irreducible

[1] Squarefree means each irreducible factor of $f(X)$ has multiplicity 1; $f(X)$ need not be monic.

factor of $f(X)$), so we have a quadratic extension $F(X, \sqrt{f(X)})/F(X)$. From Set 2, the integral closure of $F[X]$ in $F(X, \sqrt{f(X)})$ is $F[X, \sqrt{f(X)}]$. This is analogous to knowing the ring of integers in a quadratic field, as in the diagram below.

$$\begin{tikzcd}
 & K \arrow[dd, dash, "2"] \\
\mathcal{O}_K \arrow[ur, dash] \arrow[dd, dash] & \\
 & F \\
\mathbf{Z} \arrow[ur, dash] &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & F(X, \sqrt{f(X)}) \arrow[dd, dash, "2"] \\
F[X, \sqrt{f(X)}] \arrow[ur, dash] \arrow[dd, dash] & \\
 & F(X) \\
F[X] \arrow[ur, dash] &
\end{tikzcd}$$

a) Prove $F[X, \sqrt{f(X)}]^\times = F^\times$ when $\deg f(X)$ is *odd*. (The situation when $\deg f(X)$ is even is more subtle.)

b) Let $\pi(X)$ be a monic irreducible factor of $f(X)$ in $F[X]$. (There are such irreducibles since $f(X)$ is nonconstant.) In $F[X, \sqrt{f(X)}]$, set $\mathfrak{p}_\pi = (\pi(X), \sqrt{f(X)})$. Prove $\mathfrak{p}_\pi^2 = (\pi(X))$, $\mathfrak{p}_\pi$ is a maximal ideal, and

$$(\sqrt{f(X)}) = \prod_{\pi | f} \mathfrak{p}_\pi,$$

where the product runs over monic irreducible factors $\pi(X)$ of $f(X)$ in $F[X]$.

c) Let $\overline{F}$ be an algebraic closure of $F$. For any $\alpha, \beta \in \overline{F}$ such that $\beta^2 = f(\alpha)$ (that is, the point $(\alpha, \beta)$ lies on the curve $y^2 = f(x)$ and has coordinates algebraic over $F$), set

$$\mathfrak{p}_{(\alpha,\beta)} = \left\{ a(X) + b(X)\sqrt{f(X)} : a(X), b(X) \in F[X] \text{ and } a(\alpha) + b(\alpha)\beta = 0 \right\}.$$

Show $\mathfrak{p}_{(\alpha,\beta)}$ is a maximal ideal in $F[X, \sqrt{f(X)}]$ and the ideal $\mathfrak{p}_\pi$ in part b has the form $\mathfrak{p}_{(\alpha,\beta)}$ for some $\overline{F}$-point $(\alpha, \beta)$ on $y^2 = f(x)$.

(Hint: Regard $F[X, \sqrt{f(X)}]$ as $F[X, Y]/(Y^2 - f(X))$, with $\sqrt{f(X)} \leftrightarrow Y \bmod (Y^2 - f(X))$ to streamline the construction of homomorphisms out of this ring.)