

NUMBER FIELDS HW 3

(1) This exercise shows that there are finitely many number fields K whose discriminant is bounded above by a given constant C . Let K be a number field of degree $n = r_1 + 2r_2$. Let the embeddings of K into \mathbb{C} be $\sigma_1, \dots, \sigma_n$ with $\sigma_1, \dots, \sigma_{r_1}$ the real embeddings.

(i) Suppose that $r_1 > 0$ and $\alpha \in \mathcal{O}_K$ is such that $|\sigma_i(\alpha)| < 1$ for all $i > 1$. Show that $K = \mathbb{Q}(\alpha)$.

(ii) With $r_1 > 0$, show that there is an $\alpha \in \mathcal{O}_K$ with $|\sigma_i(\alpha)| < 1$ for $i > 1$, and

$$|\sigma_1(\alpha)| \leq \left(\frac{2}{\pi}\right)^{r_2} \cdot (1 + \sqrt{|disc(K)|}).$$

Deduce that there are finitely many number fields with $r_1 > 0$ and discriminant $< C$.

(iii) By adapting the argument above, remove the condition that $r_1 > 0$ from (ii).

(2) This exercise applies Minkowski's geometry of numbers arguments to show that every positive integer is the sum of 4 squares.

(a) Suppose that m and n are both the sum of 4 squares, show that mn is also the sum of 4 squares. (Hint: think about norms of quaternions). This reduces one to showing that any prime number is the sum of 4 squares.

(b) Suppose that p is an odd prime (How about the prime 2?). Show that one can find integers m and n so that $m^2 + n^2 + 1 \equiv 0 \pmod{p}$.

(c) Consider the lattice in \mathbb{R}^4 defined by

$$L = \{(a, b, c, d) \in \mathbb{Z}^4 : c \equiv ma + nb \pmod{p} \text{ and } d \equiv mb - na \pmod{p}\}.$$

Find $Vol(\mathbb{R}^4/L)$.

(d) Let X_r be the sphere in \mathbb{R}^4 centered at the origin and of radius r , so that $Vol(X_r) = \pi^2 r^4/2$. Suppose that

$$2p > r^2 > \frac{4p}{\pi} \cdot \sqrt{2}.$$

Applying Minkowski's results to such an X_r and the lattice L , show that p is the sum of 4 squares.

(3) Recall that if $\mathcal{O}_K = \oplus_i \mathbb{Z}\alpha_i$, then $disc(K) = |\det(A)|$, where A is the matrix such that $A_{ij} = \sigma_i(\alpha_j)$, where the σ_i 's are the embeddings of K into \mathbb{C} . Suppose now that $\mathcal{O}_K = \mathbb{Z}[\beta]$ and the minimal polynomial of β over \mathbb{Z}

is $f(x)$. Show that

$$\text{disc}(K) = \prod_{i < j} (\beta_i - \beta_j)^2 = N_{K/\mathbb{Q}}(f'(\beta)),$$

where the β_i 's are the roots of $f(x)$.

(4) This exercise gives the definition of the relative norm map on ideals.

(a) Suppose first that L/K is a Galois extension of number fields with $G = \text{Gal}(L/K)$. For an ideal I of \mathcal{O}_L , set

$$N_{L/K}(I) = \left(\prod_{\sigma \in G} \sigma(I) \right) \cap \mathcal{O}_K.$$

Convince yourself that $N_{L/K}(I)$ is an ideal of \mathcal{O}_K . Show that for a prime ideal \mathfrak{q} of \mathcal{O}_L lying over \mathfrak{p} , one has

$$N_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f(\mathfrak{q}|\mathfrak{p})}.$$

(b) For any I , show that

$$\prod_{\sigma \in G} \sigma(I) = (N_{L/K}(I))\mathcal{O}_L.$$

Then show that

$$N_{L/K}(IJ) = N_{L/K}(I) \cdot N_{L/K}(J).$$

(c) For a principal ideal $I = (\alpha)$, show that $N_{L/K}(I)$ is the principal ideal generated by $N_{L/K}(\alpha)$.

(d) Now suppose that L/K is not necessarily Galois. We define $N_{L/K}(I)$ by setting

$$N_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f(\mathfrak{q}|\mathfrak{p})}$$

for any prime ideal \mathfrak{q} and extending it multiplicatively to all ideals I using prime factorization. Show that if $K \subset L \subset M$ is a tower of number fields, then

$$N_{L/K} \circ N_{M/L} = N_{M/K}$$

on ideals of \mathcal{O}_M .

(e) Show that the result of (c) remains true for general L/K . Also show that if I is an ideal in \mathcal{O}_K , then $N_{K/\mathbb{Q}}(I)$ is the ideal generated by $\# \mathcal{O}/I$.

(5) Consider a degree n extension L/K of number fields. If \mathfrak{p} is a prime in K , say that \mathfrak{p} is totally ramified in L if $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}^n$.

(a) Show that if \mathfrak{p} is totally ramified in L , then it is totally ramified in every intermediate field M .

(b) Show that if \mathfrak{p} is totally ramified in L and unramified in another extension L' of K , then $L \cap L' = K$.

(7) This exercise proves that there are infinitely many prime numbers $p \equiv 1 \pmod{m}$, among other things.

(a) Let $f(x)$ be any non-constant polynomial over \mathbb{Z} . Prove that f has a root mod p for infinitely many primes p .

(b) Let K be a number field. Prove that there are infinitely many primes \mathfrak{p} in K such that $f(\mathfrak{p}|p) = 1$.

(c) Prove that there are infinitely many primes $p \equiv 1 \pmod{m}$.

(d) Let $K \subset L$ be number fields. Show that there are infinitely many primes of K which splits completely in L . (Recall that \mathfrak{p} splits completely if $\mathfrak{p}\mathcal{O}_L$ is the product of $[L : K]$ distinct primes in L).

(8) Suppose that $f(x)$ is a monic polynomial over \mathbb{Z} and $f(x)$ is reducible modulo p for every prime p . Is f necessarily reducible over \mathbb{Z} ?

(9) This exercise introduces the notion of the different $Diff(L/K)$ of L/K . Let $A \subset L$ be an additive subgroup (eg. A is a fractional ideal or an order in L). Set

$$\begin{cases} A^{-1} = \{\alpha \in L : \alpha A \subset \mathcal{O}_L\} \\ A^* = \{\alpha \in L : Tr_{L/K}(\alpha \mathcal{O}_L) \subset \mathcal{O}_K\}. \end{cases}$$

(a) Convince yourself that $A^{-1} \subset A^*$, A^{-1} is an \mathcal{O}_L -module and A^* is an \mathcal{O}_K -module.

(b) Show that A is a fractional ideal of L iff A is an \mathcal{O}_L -submodule of L such that $A^{-1} \neq 0$.

(c) Show that if A is a fractional ideal in L , then A^* is also a fractional ideal of L . Show that if A is an order in L , then A^* is a fractional ideal.

One defines: $Diff(A) = (A^*)^{-1}$: by (c), it is a fractional ideal if A is a fractional ideal or an order. One sets: $Diff(L/K) := Diff(\mathcal{O}_L)$.

(10) This exercise computes $Diff(L/K)$ in a particular situation: suppose that

$$\mathcal{O}_L = \mathcal{O}_K[\alpha] = \mathcal{O}_K \oplus \mathcal{O}_K\alpha \oplus \dots \oplus \mathcal{O}_K\alpha^{n-1},$$

where α has minimal polynomial $f(x)$ over K . Write

$$f(x) = (x - \alpha)(b_0 + b_1x + \dots + b_{n-1}x^{n-1}).$$

To compute $Diff(\mathcal{O}_L)$, we first need to compute \mathcal{O}_L^* .

(a) Show that for $1 \leq r \leq n - 1$,

$$\sum_{i=1}^n \frac{f(x)}{x - \alpha_i} \cdot \frac{\alpha_i^r}{f'(\alpha_i)} = x^r,$$

where the α_i 's are the conjugates of α .

(b) Deduce from (a) that

$$\text{Tr}_{L/K} \left(\frac{f(x)}{x - \alpha} \cdot \frac{\alpha^r}{f'(\alpha)} \right) = x^r$$

where the trace of a polynomial is obtained by taking the trace of each coefficient.

(c) Deduce from (b) that

$$\text{Tr}_{L/K} \left(\alpha^i \cdot \frac{b_j}{f'(\alpha)} \right) = \delta_{ij}.$$

Thus, we have shown that \mathcal{O}_L^* has \mathcal{O}_K -basis

$$\frac{b_0}{f'(\alpha)}, \dots, \frac{b_{n-1}}{f'(\alpha)}.$$

(d) Deduce from (c) that $\mathcal{O}_L^* = \frac{1}{f'(\alpha)} \cdot \mathcal{O}_L$, so that $\text{Diff}(L/K)$ is the principal ideal generated by $f'(\alpha)$.

(e) Consider the situation K/\mathbb{Q} . Observe from (d) and Problems 3 and 4 above that

$$N_{K/\mathbb{Q}}(\text{Diff}(K/\mathbb{Q})) = (\text{Disc}(K/\mathbb{Q})).$$

(f) Show that a prime \mathfrak{q} of L is ramified in L/K iff \mathfrak{q} divides $\text{Diff}(L/K)$.