ALGEBRAIC NUMBER THEORY W4043

1. Homework, week 7, due March 24

If K is a number field, the letters r_1 and r_2 designate respectively the number of real embeddings and pairs of complex conjugate embeddings of K.

1. (a) Let $L \supset K$ be finite extensions of $\mathbb{Q}$. Show that if the prime p ramifies in $K/\mathbb{Q}$ then it ramifies in $L/\mathbb{Q}$. Give an example to show that the converse doesn't hold.

Let K be the splitting field over $\mathbb{Q}$ of the polynomial $X^13 - 1$.

(b) List the intermediate fields K_i between K and $\mathbb{Q}$ and for each i, use Galois theory to find $\alpha_i \in K$ such that $K_i = \mathbb{Q}(\alpha_i)$.

(c) Find a cyclic generator of the multiplicative group of the $\mathbb{Z}/13\mathbb{Z}$. Find elements in $(\mathbb{Z}/13\mathbb{Z})^\times$ of order 2, 3, 4, and 6. (Hint: $26 = 2 \times 13$.)

(d) Use the results of (c) to find the order of every number between 1 and 12 in $(\mathbb{Z}/13\mathbb{Z})^\times$.

(e) Use cyclotomic reciprocity to determine the factorization of the prime ideals (17), (29), (31) in the integer rings of each of the fields K_i listed in part (b).

2. The function $D(x_1, x_2, \ldots, x_n)$ in Hindry's exercise 6.15 of Hindry's book, p. 120, is called the *discriminant* of the basis $(x_1, \ldots, x_n)$. Compute discriminants of several bases of of the ring of integers in $\mathbb{Q}(\sqrt{d})$, where d is a square-free integer.

3. In the notation of Hindry's exercise, we let p be a prime number, r a positive integer, and let $F(X) = (X^{p^r} - 1)/(X^{p^{r-1}} - 1)$, a polynomial of degree $\phi(p^r)$ where ϕ denotes the Euler function. Let $K = \mathbb{Q}(\zeta_r)$ be the splitting field of F where ζ is a root of F, and therefore a primitive p^rth root of unity.

(a) Suppose $r = 1$. Show that the discriminant of the basis $\{1, \zeta_1, \zeta_1^2, \ldots, \zeta_1^{p-2}\}$ is equal to $\pm p^{p-2}$.

(b) Determine the sign in (a).

(c) Now for any r, show that $F(X)$ (denoted Φ_{p^r} in class) is irreducible in $\mathbb{Q}[X]$ by using Eisenstein's criterion.

(d) Show that the discriminant of the basis $\{1, \zeta_r, \zeta_r^2, \ldots, \zeta_r^{\phi(p^r)-1}\}$ is equal to $\pm p^{p^{r-1}(pr-r-1)}$. (You will find it convenient to use the result of (a).)

(e) Without using the fact that the ring of integers of $\mathbb{Q}(\zeta_r)$ is generated over $\mathbb{Z}$ by ζ_r, prove that p is the only prime that ramifies in $\mathbb{Q}(\zeta_r)$ by using the calculation in (d) and general properties of discriminants.