Assignment 2

Due on May 22, 2009

Let $\mathcal{O}$ = the ring of algebraic integers of $\mathbb{C}$. For a number field $K \subset \mathbb{C}$, write $\mathcal{O}_K = \mathcal{O} \cap K$; write Cl_K = the class group $\mathcal{O}_K$ and U_K = the group of units of $\mathcal{O}_K$. For a finite set S, write $\#S$ = the cardinality of S.

1. For a number field K, let $\operatorname{diff} K = \operatorname{diff}(\mathcal{O}_K/\mathbb{Z})$ = the different ideal of $\mathcal{O}_K$ over $\mathbb{Z}$ (see [1, Ex 3.33]). It is an ideal of $\mathcal{O}_K$.

   (a) Let $K = \mathbb{Q}(\sqrt{m})$. Show that $\operatorname{diff} K$ is the principal ideal generated by $\sqrt{\operatorname{disc} K}$.

   (b) Fix an odd prime $p \in \mathbb{Q}$; let $K = \mathbb{Q}(\omega)$, where $\omega = e^{2\pi i/p}$. show that $\operatorname{diff} K_p$ is the principal ideal generated by $p/(1-\omega)$.

   (c) Suppose $K/\mathbb{Q}$ is Galois with $[K : \mathbb{Q}] = n$. Show that $(\operatorname{diff} K)^n$ is the principal ideal generated by $\operatorname{disc} K$.

   (Hint: You may want to use [1, Ex 3.35(f), 3.37(d), 3.39(c)].)

2. Let $K = \mathbb{Q}(\sqrt{-m})$, where m is a positive square-free integer. Show that

$$\#U_K = \begin{cases} 4 & \text{if } m = 1 \\ 6 & \text{if } m = 3 \\ 2 & \text{otherwise.} \end{cases}$$

3. ([1, Ex 3.16]) Let K and L be number fields, $K \subset L$.

   (a) Show that there is a homomorphism $Cl_L \to Cl_K$ defined by taking any I in a given class C and sending C to the class containing $\operatorname{Nm}_K^L(I)$. (Why is this well-defined?)

   (b) Let Q be a prime of $\mathcal{O}_L$ lying over a prime P of $\mathcal{O}_K$. Let d_Q denote the order of the class containing Q in Cl_L, d_P the order of the class containing P in Cl_K. Prove that

$$d_P | d_Q f(Q/P).$$

4. ([1, Ex 3.30])

   (a) Let f be any nonconstant polynomial over $\mathbb{Z}$. Prove that f has a root mod p for infinitely many primes p. (Suggestion: Prove this first under the assumption $f(0) = 1$ by considering prime divisors of the number $f(n!)$. Then reduce to this case by setting $g(x) = f(xf(0))/f(0)$.)

   (b) Let K be any number field. Prove that there are infinitely many primes P in K such that $f(P/p) = 1$, where p is the prime of $\mathbb{Z}$ lying under P.

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

   (d) Let K and L be number fields, $K \subset L$. Prove that infinitely many primes of K split completely (split into $[L : K]$ distinct factors) in L. (Hint: Apply (b) to the normal closure of L over K.)

(e) Let f be a nonconstant monic irreducible polynomial over a number ring R. Prove that f splits into linear factors mod P for infinitely many primes P of R.

5. ([1, Ex 4.12])

   (a) Let K be a subfield of $\mathbb{Q}[\omega], \omega = e^{2\pi i/m}$. Identify $(\mathbb{Z}/m)^\times$ with the Galois group of $\mathbb{Q}[\omega]$ over $\mathbb{Q}$ in the usual way, and let H be the subgroup of $(\mathbb{Z}/m)^\times$ fixing K pointwise. For a prime $p \in \mathbb{Z}$ not dividing m, let f denote the least positive integer such that $\bar{p}^f \in H$, where the bar denotes the congruence class mod m. Show that f is the inertial degree $f(P/p)$ for any prime P of K lying over p. (Suggestion: $f(P/p)$ is the order of the Frobenius automorphism $\phi(P/p)$. Use [1, exercise 4.11(b)]. Alternatively, use [1, Theorem 33].)

   (b) Let p be a prime not dividing m. Determine how p splits in $\mathbb{Q}[\omega + \omega^{-1}]$. (What is H?)

   (c) Let p be a prime not dividing m, and let K be any quadratic subfield $\mathbb{Q}[\sqrt{d}] \subset \mathbb{Q}[\omega]$. With notations as in part (a), show that if p is odd then $\bar{p} \in H$ iff d is a square mod p; and if $p = 2$, then $\bar{p} \in H$ iff $d \equiv 1 \pmod 8$. (Use [1, Theorem 25]. Note that if $p \not| m$ then p is unramified in $\mathbb{Q}[\omega]$, hence also in $\mathbb{Q}[\sqrt{d}]$.)

6. ([1, Ex 4.14]) Let $\omega = e^{2\pi i/m}$, and fix a prime p in $\mathbb{Z}$. Write $m = p^k n$, where $p \not| n$. The Galois group of $\mathbb{Q}[\omega]$ over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/m)^\times$, which is isomorphic in a natural way to the direct product $(\mathbb{Z}/p^k)^\times \times (\mathbb{Z}/n)^\times$. Describe D and E (corresponding to p) in terms of this direct product.

7. ([1, Ex 5.10]) Let m be a squarefree negative integer, and suppose that $\mathcal{O} \cap \mathbb{Q}[\sqrt{m}]$ is a principal ideal domain.

   (a) Show that $m \equiv 5 \pmod 8$ except when $m = -1, -2$, or -7. (Consider a prime lying over 2.)

   (b) Suppose p is an odd prime such that $m < -4p$. Show that m is non-square mod p.

   (c) Prove that if $m < -19$, then m is congruent to one of these mod 840:

   $$-43, -67, -163, -403, -547, -667.$$

   (d) Prove that the values of m given in [1, Exercise 5.9] are the only ones with $0 > m > -2000$ for which $\mathcal{O} \cap \mathbb{Q}[\sqrt{m}]$ is a principal ideal domain. (Actually it is known that they are the only ones with $m < 0$. See H.M. Stark, *A complete determination of the complex quadratic fields of class-number one*, Mich. Math. (1967), 1-27.)

8. ([1, Ex 5.33])

   (a) Let m be a squarefree positive integer, and assume first that $m \equiv 2$ or $3 \pmod 4$. Consider the numbers $mb^2 \pm 1, b \in \mathbb{Z}$, and take the smallest positive b such that either mb^2+1 or mb^2-1 is a square, say $a^2, a > 0$. Then $a + b\sqrt{m}$ is a unit in $\mathbb{Z}[\sqrt{m}]$. Prove that it is the fundamental unit. (Hint: In any case it is a power of the fundamental unit (why?). What if the exponent is greater than 1?)

   (b) Establish a similar procedure for determining the fundamental unit in $\mathcal{O} \cap \mathbb{Q}[\sqrt{m}]$ for squarefree $m > 1, m \equiv 1 \pmod 4$. (Hint: $mb^2 \pm 4$.)

References

[1] D.A. Marcus, *Number fields*. Universitext. Springer-Verlag, New York-Heidelberg, 1977.