Assignment 3

Due on June 5, 2009

For a finite set S, write $\#S =$ the cardinality of S. Let $\mathcal{O} =$ the ring of algebraic integers of $\mathbb{C}$. For a number field $K \subset \mathbb{C}$, write $\mathcal{O}_K = \mathcal{O} \cap K$; $[K : \mathbb{Q}] = r + 2s$, where $r = \#$ of real embeddings of K.

1. ([1, Ex 5.43]) Let K be a normal extension of $\mathbb{Q}$ with Galois group G.
   (a) Prove that K has degree 1 or 2 over $K \cap \mathbb{R}$.
   (b) Prove that $K \cap \mathbb{R}$ is a normal extension of $\mathbb{Q}$ iff $K \cap \mathbb{R}$ has no non-real embeddings in $\mathbb{C}$.
   (c) Let U be the group of units in $\mathcal{O} \cap K$. Prove that $U/(U \cap \mathbb{R})$ is finite iff complex conjugation is in the center of G.

2. ([1, Ex 5.48]) For $m \geq 3$, set $\omega = \exp(\frac{2\pi i}{m}), \alpha = \exp(\frac{\pi i}{m})$.
   (a) Show that
   $$1 - \omega^k = -2i\alpha^k \cdot \sin\left(\frac{k\pi}{m}\right)$$
   for all $k \in \mathbb{Z}$; conclude that
   $$\frac{1-\omega^k}{1-\omega} = \alpha^{k-1} \cdot \frac{\sin(k\pi/m)}{\sin(\pi/m)}.$$
   (b) Show that if k and m are not both even, then $\alpha^{k-1} = \pm\omega^h$ for some $h \in \mathbb{Z}$.
   (c) Show that if k is relatively prime to m then
   $$u_k = \frac{\sin(k\pi/m)}{\sin(\pi/m)}$$
   is a unit in $\mathbb{Z}[\omega]$.

3. ([1, Ex 6.4]) Let K be a number field. An element $\alpha \in \mathcal{O}_K$ is called *totally positive* iff $\sigma(\alpha) > 0$ for every real embedding $\sigma : K \to \mathbb{R}$. Let $\mathcal{O}_K^+$ denote the set of all totally positive numbers of $\mathcal{O}_K$. Define a relation $\overset{\circ}{\sim}$ on the nonzero ideals of $\mathcal{O}_K$ as follows:
   $$I \overset{\circ}{\sim} J \text{ iff } \alpha I = \beta J \text{ for some } \alpha, \beta \in \mathcal{O}_K^+.$$
   (a) Prove that this is an equivalent relation.
   (b) Prove that the equivalent classes under this relation form a group G^+ in which the identity element is the class consisting of all principal ideals $(\alpha), \alpha \in \mathcal{O}_K^+$. (Use the fact that the ordinary ideal classes from a group. Notice that $\alpha^2 \in \mathcal{O}_K^+$ for every nonzero $\alpha \in \mathcal{O}_K$.)
   (c) Show that there is a group-homomorphism $f : G^+ \to G$, where G is the ideal class group of $\mathcal{O}_K$.

(d) Prove that the kernel of f has at most 2^r elements, where r is the number of embeddings $K \to \mathbb{R}$. Conclude that G^+ is finite.

4. ([1, Ex 6.5]) Continuing the notation of exercise 3, assume that K has at least one real embedding $\sigma : K \to \mathbb{R}$. Fix this σ and let U be the group of units in $\mathcal{O}_K$.

   (a) What can you say about the roots of 1 in $\mathcal{O}_K$?

   (b) Show that $U = \{\pm 1\} \times V$, where V consists of those $u \in U$ such that $\sigma(u) > 0$. Using [1, Thm 38], prove that V is a free abelian group of rank $r + s - 1$.

   (c) Let $U^+ = U \cap \mathcal{O}_K^+$. Then $U^+ \subset V$, and clearly U^+ contains $V^2 = \{v^2 : v \in V\}$. Use this to prove that U^+ is a free abelian group of rank $r + s - 1$. (See [1, Ex 2.24].)

5. ([1, Ex 6.10]) Fix a nonzero ideal M in $\mathcal{O}_K$ and define a relation $\overset{\circ}{\sim}_M$ on the set of ideals of $\mathcal{O}_K$ which are relative prime to M, as follows:

$$I \overset{\circ}{\sim}_M J \text{ iff } \alpha I = \beta J \text{ for some } \alpha, \beta \in \mathcal{O}_K^+, \alpha \equiv \beta \equiv 1 \pmod{M}.$$

   (a) Prove that this is an equivalent relation.

   (b) Prove that the equivalent classes from a group G_M^+ in which the identity element is the class consisting of all principal ideals $(\alpha), \alpha \in \mathcal{O}_K^+, \alpha \equiv 1 \pmod{M}$. (Hint: To show that a given class has an inverse, fix I in the class and use the Chinese Remainder Theorem to obtain $\alpha \in I, \alpha \equiv 1 \pmod{M}$.) The equivalence classes are called *ray classes* and G_M^+ is called a *ray class group*.

   (c) Show that there is a group-homomorphism $f : G_M^+ \to G^+$, where G^+ is as in Ex 3.

   (d) Prove that the kernel of f has at most $\#(\mathcal{O}_K/M)^\times$ elements, where $(\mathcal{O}_K/M)^\times$ is the multiplicative group of the finite ring $\mathcal{O}_K/M$. Conclude that G_M^+ is finite.

6. ([1, Ex 7.8]) Use [1, Cor 2 of Thm 43] to determine the density of the set of primes $p \in \mathbb{Z}$ such that

   (a) 2 is a square mod p;

   (b) 2 is a cube mod p;

   (c) 2 is a fourth power mod p.

   (Note: If $p \not\equiv 1 \pmod 3$ then everything is a cube mod p; however $x^3 - 2$ does not split completely mod p unless $p \equiv 1 \pmod 3$ and 2 is a cube mod p. Similar remarks hold for fourth powers.)

7. ([1, Ex 7.11]) Let L be a normal extension of K with cyclic Galois group. Prove that infinitely many primes of K remain prime in L. What is the density of the set of primes of K which split into a given number of primes in L?

References

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