Problem set 10 – Math 699 – Algebraic number theory

(1) Show that the unit group $\mathcal{O}_K^\times$ has rank 1 if and only if K is real quadratic, complex cubic (i.e. not a totally real cubic), or totally imaginary quartic.

(2) Let K be a complex cubic, thought of as a subfield of $\mathbf{R}$. From Question (1), we know that the unit group has rank one, so, like in class, we can search for a fundamental unit $u > 1$; again, it will be the least unit > 1. Let $u > 1$ be a fundamental unit of K and write $\rho e^{i\theta}$ and $\rho e^{-i\theta}$ for its two Galois conjugates. Finding u is a bit more tedious than in the quadratic case.

  (a) Show that $u = \rho^{-2}$.

  (b) Show that the discriminant of u is $\Delta(u) = -4\sin^2(\theta)(\rho^3 + \rho^{-3} - 2\cos(\theta))^2$

  (c) Conclude that $|\Delta(u)| < 4(u^3 + u^{-3} + 6)$ and hence that $u^3 > \dfrac{|\Delta(K)|}{4} - 7$.

  (d) Here's how you can apply this to find the fundamental unit of a complex cubic. Let $K = \mathbf{Q}(\alpha)$ where $\alpha = \sqrt[3]{2}$. Let u denote the fundamental unit of K that is > 1. Show that $u^2 > 20^{2/3}$. Let $\eta = 1 + \alpha + \alpha^2$. Show that η is a unit. Show that $1 < \eta < u^2$ and conclude that $u = \eta$.

(3) Let K be a number field and suppose $\gamma \in K$ is a root of the monic polynomial $g(x) \in \mathbf{Z}[x]$. Suppose $a \in \mathbf{Z}$ is such that $g(a) = \pm 1$. Show that $\gamma - r \in \mathcal{O}_K^\times$. (Hint: consider $\widetilde{g}(x) = g(x + a)$, and use it to show that $N_{K/\mathbf{Q}}(\gamma - a) = \pm 1$.)

(4) Use Questions (2) and (3) to find fundamental units in the following complex cubic fields.

  (a) $K = \mathbf{Q}(\sqrt[3]{7})$

  (b) $K = \mathbf{Q}(\sqrt[3]{3})$ (Hint: show that $(3^{2/3} - 2)^{-1}$ is the fundamental unit.)

(5) Let's now look at totally imaginary quartic fields. Particularly, let's focus on V_4-quartics. Here is a bit of terminology: a number field K is called a *CM field* if it is a totally imaginary quadratic extension of a totally real field. It can be shown that a number field has a uniquely-defined complex conjugation if and only if it is totally real or CM. A CM field K is therefore uniquely a quadratic extension of a totally real field. This maximal totally real subfield will be denoted K^+.

  (a) Let K be an imaginary V_4 quartic field. Show that K is CM.

  (b) Show that if K is CM, then $\mathcal{O}_K^\times$ and $\mathcal{O}_{K^+}^\times$ have the same rank.

(c) Here are some facts that will help in finding units in imaginary V_4 quartics; you don't need to prove them. For details, see §V.2 of Fröhlich and Taylor's book. First off, suppose K is a CM field. Then, $[\mathcal{O}_K^\times : \mu(K)\mathcal{O}_{K^+}^\times] \leq 2$. Second, if K is a totally imaginary V_4 quartic field and the fundamental unit of K^+ has norm -1, then this index is 1, i.e. the fundamental unit of K is that of K^+. Finally, if $p \equiv 1 \pmod 4$, then $\mathbf{Q}(\sqrt{p})$ has fundamental unit of norm -1 (this is Theorem 11.5.4 of Alaca and Williams' book; they gave two proofs, one due to Hilbert, the other to Dirichlet).

(d) Find the fundamental unit of $K = \mathbf{Q}(\sqrt{-1}, \sqrt{-2})$.

(e) Find the fundamental unit of $K = \mathbf{Q}(\sqrt{-2}, \sqrt{-10})$.

(f) Find the fundamental unit of $K = \mathbf{Q}(\sqrt{-1}, \sqrt{-5})$.

(6) Let us turn to cyclotomic fields. Let $K_m = \mathbf{Q}(\zeta_m)$ where ζ_m is a primitive mth root of unity.

(a) Show that $\dfrac{1-\zeta_m^a}{1-\zeta_m}$ is a unit whenever $\gcd(a, m) = 1$. (Hint: what is $(1 - x^a)/(1 - x)$?)

(b) Show that if m has at least two distinct prime factors, then $1 - \zeta_m^a$ is a unit ($\gcd(a, m) = 1$). (Hint: show that the norm of $1 - \zeta_m^a$ is $\Phi_m(1)$, where Φ_m is the mth cyclotomic polynomial.)

(c) Show that if $m = p^r$ is a prime power, then $1 - \zeta_m$ is not a unit (in fact, $(1 - \zeta_m)\mathcal{O}_K$ is the unique prime dividing p).

(d) Units as above are called *cyclotomic units*. Not all units in K_m need be of this form. But here are some very intriguing statements that you need not prove (see §8.1 of Washington's book *Introduction to cyclotomic fields* for details). Let V_m denote the multiplicative group generated by $\pm\zeta_m$ and $1 - \zeta_m^a$ for $1 \leq a \leq m - 1$, then the group of *cyclotomic units* of K_m is $C_m := V_m \cap \mathcal{O}_{K_m}^\times$. The group of cyclotomic units of K_m^+ is similarly $C_m^+ := V_m \cap \mathcal{O}_{K_m^+}^\times$. Then $[\mathcal{O}_{K_m}^\times : C_m] < \infty$ and $[\mathcal{O}_{K_m^+}^\times : C_m^+] < \infty$. In fact, if $m = p^r$ is a prime power, then

$$[\mathcal{O}_{K_m^+}^\times : C_m^+] = h_{K_m^+},$$

the class number of K_m^+! It is a result of Sinnott that, for general m,

$$[\mathcal{O}_{K_m^+}^\times : C_m^+] = 2^b h_{K_m^+},$$

where $b = 0$ if m is a prime power, and $b = 2^{g-2} + 1 - g$ if the number of distinct prime factors g of m is at least 2.