**Fundamental Units in a Number Field**  
Mckenzie West  
Algebraic Number Theory  
10/30/2013

**Definition:** Given a field extension of $K$ of $\mathbb{Q}$, the ring of integers $\mathcal{O}_K$ is the set 

$$\mathcal{O}_K := \{ x \in K : f(x) = 0 \text{ for some monic } f(T) \in \mathbb{Z}[T] \}.$$ 

That is, $\mathcal{O}_K$ is the set of solutions to monic polynomials in $\mathbb{Z}[T]$ which lie in $K$.

As we have seen, this set is in fact a ring, and further, it has a basis as a $\mathbb{Z}$-module. Within any ring $R$, lies a multiplicative group $\mathcal{O}_R^\times$, made up of the units of the ring. Thus we can examine the structure of $\mathcal{O}_K^\times$ for number fields $K$.

**Theorem:** (Dirichlet’s Unit Theorem) If $K/\mathbb{Q}$ is a number field, $s$ is the number of field embeddings of $K$ into $\mathbb{Q} \cap \mathbb{R}$, and $2t$ is the number of imaginary embeddings of $K$ into $\mathbb{Q}$, then 

$$\mathcal{O}_K^\times \simeq W_K \times \mathbb{Z}^{s+t-1},$$ 

where $W_k$ is the set of roots of unity which lie in $K$.

**Definition:** A set $\{\epsilon_1, \ldots, \epsilon_{s+t-1}\}$ is a set of fundamental units for $K$ if the $\mathbb{Z}^{s+t-1}$ portion of $\mathcal{O}_K^\times$ is generated by these elements. That is $\mathcal{O}_K^\times = \{ w^{i_1 \epsilon_1} \ldots \epsilon_{s+t-1} : w \in W_K, \ i, e_1, \ldots, e_{s+t-1} \in \mathbb{Z} \}$.

**Example:** In the case where $K = \mathbb{Q}(\sqrt{5})$, we have that $\mathcal{O}_K = \mathbb{Z}\left[\frac{1 + \sqrt{5}}{2}\right]$, since $5 \equiv 1 \pmod{4}$. The embeddings of $K$ into $\mathbb{Q}$ are the identity, $\sigma_0$, and $\sigma_1 : \sqrt{5} \mapsto -\sqrt{5}$. Therefore, by Dirichlet’s Unit Theorem, we have $\mathcal{O}_K^\times \simeq W_k \times \mathbb{Z}^1$.

As $K$ is totally real, $W_k = \{\pm 1\}$. Now we wish to find the generator of $\mathbb{Z}^1$. Compute

$$\frac{1 + \sqrt{5}}{2} \left(1 - \frac{1 + \sqrt{5}}{2}\right) = 1,$$

so we have that $\epsilon := \frac{1 + \sqrt{5}}{2}$ is a unit. If $\epsilon$ were not a fundamental unit, then there would be a $\epsilon' \in \mathcal{O}_K^\times$ such that $\epsilon'^k = \epsilon$ for some $k$. Intuitively, there is no way this could happen because $\epsilon$ is “small”.

**Goal:** Examine Dirichlet’s Unit Theorem through an example where $s, t > 0$.

In order to have both real and imaginary embeddings, we need an extension of $\mathbb{Q}$ which is not Galois. By the primitive root theorem, we can always write $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$. Thus, we require a $\alpha$ which has both real an imaginary conjugates, which will produce the real and imaginary embeddings, respectively.

**Example:** Consider $K = \mathbb{Q}(\sqrt[4]{2})$. We will fix some notation, $\alpha = \sqrt[4]{2}$ and $\zeta = e^{2\pi i/5}$. The conjugates of $\alpha$ then are $\alpha, \zeta\alpha, \zeta^2\alpha, \zeta^3\alpha$, and $\zeta^4\alpha$. Then we can write the embeddings of $K$ as $\sigma_i : \alpha \mapsto \zeta^i\alpha$ for $0 \leq i \leq 4$. Note that $\sigma_0$ is the only real embedding of $K$ into $\mathbb{Q}$,
and \( \sigma_1 = \bar{\sigma}_1 \) and \( \sigma_2 = \bar{\sigma}_3 \) are the imaginary embeddings. Therefore, as in Dirichlet’s Unit Theorem, \( s = 1, t = 2, \) and
\[ \mathcal{O}_K^\times \simeq W_k \times \mathbb{Z}^2. \]

As in the previous example, \( W_k = \{ \pm 1 \} \). To determine the exact structure of \( \mathcal{O}_K^\times \) we must begin by looking at \( \mathcal{O}_K \).

Certainly \( \mathbb{Z}[\alpha] \subseteq \mathcal{O}_K \). In fact, we will see that \( \mathbb{Z}[\alpha] = \mathcal{O}_K \). Set \( F(T) = T^5 - 2 \), the minimal polynomial of \( \alpha \) over \( \mathbb{Q} \). Then we can compute
\[ \Delta_K(1, \alpha, \alpha^2, \alpha^3, \alpha^4) = (-1)^{(5-1)/2}N_{K/\mathbb{Q}}(F'(\alpha)) = 5^5 \cdot 2^4. \]

As this is not prime, we must verify that for every \( x \in \mathbb{Z}[\alpha] \) with \( \frac{1}{5}x \) \( \notin \mathbb{Z}[\alpha] \), \( \frac{1}{5}x \notin \mathcal{O}_K \). For each such element, \( y \), compute \( F_K^y(T) := \prod_{i=0}^4(T - \sigma_i(y)) \). As \( F_K^y(T) \notin \mathbb{Z}[T] \), we can conclude that \( y \notin \mathcal{O}_K \). (See code below.) Therefore
\[ \mathcal{O}_K = \mathbb{Z}[\sqrt{2}]. \]

Now set \( \epsilon_1 = 1 - \alpha \) and \( \epsilon_2 = 1 + \alpha + \alpha^2 \).

Claim: \( \mathcal{O}_K^\times = \{ \pm \epsilon_1^i \epsilon_2^j : i, j \in \mathbb{Z} \} \)

Proof. We can consider \( \{ \epsilon_1^i \epsilon_2^j \} \) as a lattice in \( \mathbb{R}^2 \). That is, if \( \mathcal{O}_K^\times \) is not as claimed, there would be an \( \alpha \in \mathcal{O}_K^\times \) such that \( \alpha^p = \epsilon_1 \) or \( \epsilon_2 \) for some prime \( p \geq 2 \). If \( N = N_{K/\mathbb{Q}} \), define a “norm” on the elements in \( \mathcal{O}_K \) as follows,
\[ M(a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4) = \frac{1}{N(|a|)} + N(|b|\alpha) + N(|c|\alpha^2) + N(|d|\alpha^3) + N(|e|\alpha^4) \]
\[ = |a|^5 + 2|b|^5 + 4|c|^5 + 8|d|^5 + 16|e|^5 \in \mathbb{Z}_{\geq 0} \]

Now it is clear that \( M(xy) \neq M(x)M(y) \) in most cases; however we can show that \( M \) is a submultiplicative norm, that is \( M(xy) \geq M(x)M(y) \) on \( \mathcal{O}_K \). Certainly \( M(\epsilon_1) = M(1 - \alpha) = 3 \), and \( M(\epsilon_2) = M(1 + \alpha + \alpha^2) = 11 \). As \( (1 - \alpha)^2 = 1 - 2\alpha + \alpha^2 \neq \epsilon_2 \) and \( M((1 - \alpha)^k) \geq 3^k > 11 \) for all \( k \geq 3 \), we have that \( \epsilon_1^i \neq \epsilon_2 \). On the other hand, since \( M(\epsilon_2) > M(\epsilon_1) \), we cannot have \( \epsilon_2^j = \epsilon_1 \). By further examination of \( M \), and brute force, we see that no \( a \in \mathcal{O}_K^\times \) is “smaller” than \( \epsilon_1 \) or \( \epsilon_2 \). Therefore, \( \mathcal{O}_K^\times \) is as claimed. \( \square \)

Naturally, we can use Computer Algebra Systems, such as Magma and Mathematica, to find rings of integers and fundamental units. In fact, this is a good place to start. However it is a useful exercise to go through and develop arguments as to why such claims are true. For the magma code used in preparing this document, see below.
Magma Code: The initial examination of the field $\mathbb{Q}(\sqrt[5]{2})$.

```magma
> P<t>:=PolynomialRing(Rationals());
> K:=NumberField(t^5-2);
> OK:=Integers(K);
> /* To see the generators for OK, we print their minimal polynomials. */
> for i in {1,2,3,4,5} do
> MinimalPolynomial(OK.i);
> end for;
t - 1
t^5 - 2
t^5 - 4
t^5 - 8
t^5 - 16
> /* Unit groups are endowed with maps to the ring they are contained in. */
> UK, mUK := UnitGroup(OK);
> /* The generators for UK are given by their OK basis representation when we */
> use the mUK map. */
> for i in {1,2,3} do
> mUK(UK.i);
> end for;
[-1, 0, 0, 0, 0]
[1, -1, 0, 0, 0]
[1, 1, 0, 1, 0]
```

Mathematica Code: Verifying the generators of the ring of integers.

```mathematica
alpha := 2^(1/5)
zeta := Exp[2Pi*I/5]
F[a_, b_, c_, d_, e_] :=
Expand[
  FullSimplify[
    Expand[
      Product[
        T - (a + b*alpha*zeta^i + c*alpha^2*zeta^(2*i) + d*alpha^3*zeta^(3*i) + e*alpha^4*zeta^(4*i)),
        {i, 0, 4}]])]
F[a/2, b/2, c/2, d/2, e/2]
F[a/5, b/5, c/5, d/5, e/5]
```

Mathematica Output: Evaluation of the $F^y_k(T)$.

- $y = \frac{1}{5}x$
- $F^y_k(T) = \left(-\frac{a^5}{3125} - \frac{b^5}{3125} + \frac{2}{625}ab^2c - \frac{2}{625}a^2bc^2 - \frac{4}{625}a^2b^2d - \frac{2}{625}a^3cd + \frac{4}{625}bc^3d - \right.$
\[
\begin{aligned}
\frac{4}{625}b^2 cd^2 - \frac{4}{625}ac^2d^2 + \frac{4}{625} abd^3 - \frac{8}{625} \frac{a^2}{3125} + \frac{2}{625} a^3be - \frac{4}{625} b^2 c^2e + \frac{4}{625} ac^3e + \frac{4}{625} b^3de + \frac{4}{625} abcde - \\
\frac{4}{625}a^2 d^2e + \frac{8}{625} cd^3e - \frac{1}{625} ab^2 e^2 - \frac{4}{625} a^2 ce^2 - \frac{8}{625} c^2 de^2 - \frac{8}{625} bd^2 e^2 + \frac{8}{625} bce^3 + \frac{8}{625} ade^3 - \\
\frac{16}{3125} + (\frac{a^4}{125} - \frac{2}{125} a^3 c + \frac{4}{125} abc^2 + \frac{4}{125} ab^2 d - \frac{6}{125} a c^2 d + \frac{4}{125} c^2 d^2 - \frac{4}{125} bd^3 - \frac{6}{125} a^2 be - \frac{4}{125} c^3 e - \\
\frac{4}{125} abd e + \frac{8}{125} a d^2 e + \frac{4}{125} b^2 e^2 + \frac{8}{125} ace^2 - \frac{8}{125} de^3)T + (-\frac{2a^3}{25} - \frac{2}{25} be^2 - \frac{2}{25} b d + \frac{6}{25} acd + \\
\frac{6}{25} abe - \frac{4}{25} d^2 e - \frac{4}{25} c e^2)T^2 + (\frac{2a^2}{5} - \frac{2}{5} cd - \frac{2}{5} be)T^3 - aT^4 + T^5
\end{aligned}
\]

- \( y = \frac{1}{2} x \)

\[
F_k^y(T) = \left( -\frac{a^5}{32} - \frac{b^5}{16} + \frac{5}{16} ab^3c - \frac{5}{16} a^2 bc^2 - \frac{c^6}{8} - \frac{5}{16} a^2 b^2 d + \frac{5}{16} a^3 cd + \frac{5}{8} bc^3 d - \frac{5}{8} b^2 cd^2 - \frac{5}{8} ac^2 d^2 + \\
\frac{5}{8} abd^3 - \frac{d^6}{4} + \frac{5}{16} a^3 be - \frac{5}{8} b^2 c^2 e + \frac{5}{8} ac^3 e + \frac{5}{8} b^2 d e + \frac{5}{8} abcde - \frac{5}{8} a^2 d^2 e + \frac{5}{4} cd^3 e - \frac{5}{8} ab^2 e^2 - \\
\frac{5}{8} a^2 c e^2 - \frac{5}{8} c^2 d e^2 - \frac{5}{4} bd^2 e^2 + \frac{5}{4} b c e^3 + \frac{5}{4} ade^3 - \frac{a^5}{2} \right) + \left( \frac{5a^4}{16} - \frac{5}{8} b^3 c + \frac{5}{8} abc^2 + \frac{5}{4} ab^2 d - \frac{15}{8} a^2 cd + \\
\frac{5}{4} c^2 d^2 - \frac{5}{4} bd^3 - \frac{15}{8} a^2 be - \frac{5}{4} c^3 e - \frac{5}{8} b c d e + \frac{5}{4} a d^2 e + \frac{5}{4} b^2 e^2 + \frac{5}{2} ac^2 e - \frac{5}{2} de^3 \right) T + \left( \frac{5a^3}{4} - \frac{5}{4} b c^2 - \\
\frac{5}{4} b^2 d + \frac{15}{4} acd + \frac{15}{4} abe - \frac{5}{2} d^2 e - \frac{5}{2} c e^2 \right) T^2 + \left( \frac{5a^2}{2} - \frac{5}{2} cd - \frac{5}{2} be \right) T^3 - \frac{5a}{2} T^4 + T^5
\]