Math 129: Algebraic Number Theory
Lecture 11: Units

William Stein

Thursday, March 11, 2004

Questions:

1. What do you want to do your projects on? Discuss.
2. Is every ideal in an order necessarily generated by at most two elements?

1 Finishing the proof of Dirichlet's Unit Theorem

We begin by finishing Dirichlet's proof that the group of units U_K of $\mathcal{O}_K$ is isomorphic to $\mathbf{Z}^{r+s-1} \oplus \mathbf{Z}/m\mathbf{Z}$, where r is the number of real embeddings, s is half the number of complex embeddings, and m is the number of roots of unity in K. Recall that we defined a map $\varphi : U_K \to \mathbf{R}^{r+s}$ by

$$\varphi(x) = (\log|\sigma_1(x)|, \ldots, \log|\sigma_{r+s}(x)|).$$

Without much trouble, we proved that the kernel of φ if finite and the image φ is discrete, and near the end of Lecture 10 we were finishing the proof that the image of φ spans the subspace H of elements of $\mathbf{R}^{r+s}$ that are orthogonal to $v = (1, \ldots, 1, 2, \ldots, 2)$, where r of the entries are 1's and s of them are 2's. The somewhat indirect route we followed was to suppose

$$z \notin H^{\perp} = \mathrm{Span}(v),$$

i.e., that z is not a multiple of v, and prove that z is not orthogonal to some element of $\varphi(U_K)$. Writing $W = \mathrm{Span}(\varphi(U_K))$, this would show that $W^{\perp} \subset H^{\perp}$, so $H \subset W$. We ran into two problems: (1) we ran out of time, and (2) the notes contained an incomplete argument that a quantity $s = s(c_1, \ldots, c_{r+s})$ can be chosen to be arbitrarily large. Today we will finish going through a complete proof, then compute many examples of unit groups using MAGMA.

Recall that $f : K^* \to \mathbf{R}$ was defined by

$$f(x) = z_1 \log|\sigma_1(x)| + \cdots + z_{r+s} \log|\sigma_{r+s}(x)| = z \bullet \varphi(x) \qquad \text{(dot product)},$$

and our goal is to show that there is a $u \in U_K$ such that $f(u) \neq 0$.

Our strategy is to use an appropriately chosen a to construct a unit $u \in U_K$ such $f(u) \neq 0$. Recall that we used Blichfeld's lemma to find an $a \in \mathcal{O}_K$ such that $1 \leq |\operatorname{Norm}_{K/\mathbf{Q}}(a)| \leq A$, and

$$\frac{c_i}{|\sigma_i(a)|} \leq A \quad \text{for } i \leq r \quad \text{and} \quad \left(\frac{c_i}{|\sigma_i(a)|}\right)^2 \leq A \quad \text{for } i = r+1, \ldots, r+s. \quad (1.1)$$

Let $b_1, \ldots, b_m$ be representative generators for the finitely many nonzero principal ideals of $\mathcal{O}_K$ of norm at most $A = A_K = \sqrt{|d_K|} \cdot \left(\frac{2}{\pi}\right)^s$. Modify the b_i to have the property that $|f(b_i)|$ is minimal among generators of (b_i) (this is possible because ideals are discrete). Note that the set $\{|f(b_i)| : i = 1, \ldots, m\}$ depends only on A. Since $|\operatorname{Norm}_{K/\mathbf{Q}}(a)| \leq A$, we have $(a) = (b_j)$, for some j, so there is a unit $u \in \mathcal{O}_K$ such that $a = ub_j$.

Let

$$s = s(c_1, \ldots, c_{r+s}) = z_1 \log(c_1) + \cdots + z_{r+s} \log(c_{r+s}) \in \mathbf{R}.$$

Lemma 1.1. *We have*

$$|f(u) - s| \leq B = \max_i(|f(b_i)|) + \log(A) \cdot \left(\sum_{i=1}^{r} |z_i| + \frac{1}{2} \cdot \sum_{i=r+1}^{s} |z_i|\right),$$

and B depends only on K and our fixed choice of $z \in H^{\perp}$.

Proof. By properties of logarithms, $f(u) = f(a/b_j) = f(a) - f(b_j)$. We next use the triangle inequality $|a + b| \leq |a| + |b|$ in various ways, properties of logarithms, and the bounds (1.1) in the following computation:

$$\begin{aligned}
|f(u) - s| &= |f(a) - f(b_j) - s| \\
&\leq |f(b_j)| + |s - f(a)| \\
&= |f(b_j)| + |z_1(\log(c_1) - \log(|\sigma_1(a)|)) + \cdots + z_{r+s}(\log(c_{r+s}) - \log(|\sigma_{r+s}(a)|))| \\
&= |f(b_j)| + |z_1 \cdot \log(c_1/|\sigma_1(a)|) + \cdots + \frac{1}{2} \cdot z_{r+s} \log((c_{r+s}/|\sigma_{r+s}(a)|)^2)| \\
&\leq |f(b_j)| + \log(A) \cdot \left(\sum_{i=1}^{r} |z_i| + \frac{1}{2} \cdot \sum_{i=r+1}^{s} |z_i|\right).
\end{aligned}$$

The inequality of the lemma now follows. That B only depends on K and our choice of z follows from the formula for A and how we chose the b_i. □

The amazing thing about Lemma 1.1 is that the bound B on the right hand side does not depend on the c_i. Suppose we could somehow cleverly choose the positive real numbers c_i in such a way that

$$c_1 \cdots c_r \cdot (c_{r+1} \cdots c_{r+s})^2 = A \qquad \text{and} \qquad |s(c_1, \ldots, c_{r+s})| > B.$$

Then the facts that $|f(u)-s| \leq B$ and $|s| > B$ would together imply that $|f(u)| > 0$ (since $f(u)$ is closer to s than s is to 0), which is exactly what we aimed to prove. We finish the proof by showing that it is possible to choose such c_i. Note that if we change the c_i, then a could change, hence the j such that a/b_j is a unit could change, but the b_j don't change, just the subscript j. Also note that if $r+s=1$, then we are trying to prove that $\varphi(U_K)$ is a lattice in $\mathbf{R}^0 = \mathbf{R}^{r+s-1}$, which is automatically true, so we may assume that $r+s>1$.

Lemma 1.2. *Assume $r+s>1$. Then there is a choice of $c_1, \ldots, c_{r+s} \in \mathbf{R}_{>0}$ such that*

$$|z_1 \log(c_1) + \cdots + z_{r+s}\log(c_{r+s})| > B.$$

Proof. It is easier if we write

$$\begin{aligned} &z_1 \log(c_1) + \cdots + z_{r+s}\log(c_{r+s}) = \\ &\qquad z_1\log(c_1) + \cdots + z_r \log(c_r) + \frac{1}{2}\cdot z_{r+1}\log(c_{r+1}^2) + \cdots + \frac{1}{2}\cdot z_{r+s}\log(c_{r+s}^2) \\ &\qquad = w_1\log(d_1) + \cdots + w_r\log(d_r) + w_{r+1}\log(d_{r+1}) + \cdots + \cdot w_{r+s}\log(d_{r+s}), \end{aligned}$$

where $w_i = z_i$ and $d_i = c_i$ for $i \leq r$, and $w_i = \frac{1}{2}z_i$ and $d_i = c_i^2$ for $r < i \leq s$,

The condition that $z \notin H^\perp$ is that the w_i are not all the same, and in our new coordinates the lemma is equivalent to showing that $|\sum_{i=1}^{r+s} w_i \log(d_i)| > B$, subject to the condition that $\prod_{i=1}^{r+s} d_i = A$. Order the w_i so that $w_1 \neq 0$. By hypothesis there exists a w_j such that $w_j \neq w_1$, and again re-ordering we may assume that $j=2$. Set $d_3 = \cdots = d_{r+s} = 1$. Then $d_1 d_2 = A$ and $\log(1) = 0$, so

$$\begin{aligned} \left|\sum_{i=1}^{r+s} w_i \log(d_i)\right| &= |w_1\log(d_1) + w_2\log(d_2)| \\ &= |w_1\log(d_1) + w_2\log(A/d_1)| \\ &= |(w_1-w_2)\log(d_1) + w_2\log(A)| \end{aligned}$$

Since $w_1 \neq w_2$, we have $|(w_1-w_2)\log(d_1) + w_2\log(A)| \to \infty$ as $d_1 \to \infty$. □

2 Some Examples of Units in Number Fields

The classical Pell's equation is, given square-free $d > 0$, to find all positive integer solutions (x,y) to the equation $x^2 - dy^2 = 1$. Note that if $x + y\sqrt{d} \in \mathbf{Q}(\sqrt{d})$, then

$$\mathrm{Norm}(x+y\sqrt{d}) = (x+y\sqrt{d})(x-y\sqrt{d}) = x^2 - dy^2.$$

The solutions to Pell's equation thus form a finite-index subgroup of the group of units in the ring of integers of $\mathbf{Q}(\sqrt{d})$. Dirichlet's unit theorem implies that for any d the solutions to Pell's equation form an infinite cyclic group, a fact that takes substantial work to prove using only elementary number theory (for example, using continued fractions).

We first solve the Pell equation $x^2 - 5y^2 = 1$ by finding the units of a field using MAGMA (we will likely discuss algorithms for computing unit groups later in the course...).

```
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^2-5);
> G, phi := UnitGroup(K);
> G;
Abelian Group isomorphic to Z/2 + Z
Defined on 2 generators
Relations:
    2*G.1 = 0
> K!phi(G.1);
-1
> u := K!phi(G.2); u;
1/2*(a + 1)
> u^2;
1/2*(a + 3)
> u^3;
a + 2
> Norm(u);
-1
> Norm(u^3);
-1
> Norm(u^6);
1
> fund := u^6;
> fund;
4*a + 9
> 9^2 - 5*4^2;
1
> fund^2;
72*a + 161
> fund^3;
1292*a + 2889
> fund^4;
23184*a + 51841
> fund^5;
416020*a + 930249
```

I think in practice for solving Pell's equation it's best to use the ideas in the following paper: Lenstra, H. W., Jr., *Solving the Pell equation.* Notices Amer. Math. Soc. **49** (2002), no. 2, 182–192. A review of this paper says: "This wonderful article begins with history and some elementary facts and proceeds to greater and greater depth about the existence of solutions to Pell equations and then later the algorithmic issues of finding those solutions. The cattle problem is discussed, as are modern smooth number methods for solving Pell equations and the algorithmic issues of representing very large solutions in a reasonable way." You can get the paper freely online from the Notices web page or the Math 129 web page.

The simplest solutions to Pell's equation can be huge, even when d is quite small. Read Lenstra's paper for some awesome examples from antiquity.

```
K<a> := NumberField(x^2-NextPrime(10^7));
> G, phi := UnitGroup(K);
> K!phi(G.2);
    1635802598803463282255922381210946254991426776931429155067472530\
    003400641003657678728904388162492712664239981750303094365756\
    106316392723776016806037958837914778176119741840754457028237\
    899759459100428895693238165048098039*a +
    517286692885814967470170672368346798303629034373575202975075\
    605058714958080893991274427903448098643836512878351227856269\
    086856679078304979321047765031073345259902622712059164969008\
    633603603640331175663456220418293622240930
```

The MAGMA `Signature` command returns the number of real and complex conjugate embeddings of K into $\mathbf{C}$. The command `UnitGroup`, which we used above, returns the unit group U_K as an abstract abelian group and a homomorphism $U_K \to \mathcal{O}_K$. Note that we have to bang (!) into K to get the units as elements of K.

First we consider $K = \mathbf{Q}(i)$.

```
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^2+1);
> Signature(K);
0 1    // r=0, s=1
> G,phi := UnitGroup(K);
> G;
Abelian Group isomorphic to Z/4
Defined on 1 generator
Relations:
    4*G.1 = 0
> K!phi(G.1);
-a
```

Next we consider $K = \mathbf{Q}(\sqrt[3]{2})$.

```
> K<a> := NumberField(x^3-2);
> Signature(K);
1 1
> G,phi := UnitGroup(K);
> G;
Abelian Group isomorphic to Z/2 + Z
```

```
Defined on 2 generators
Relations:
    2*G.1 = 0
> K!phi(G.2);
-a + 1
```

The `Conjugates` command returns the sequence $(\sigma_1(x), \ldots, \sigma_{r+2s}(x))$ of all embeddings of $x \in K$ into $\mathbf{C}$. The `Logs` command returns the sequence

$$(\log(|\sigma_1(x)|), \ldots, \log(|\sigma_{r+s}(x)|)).$$

Continuing the above example, we have

```
> Conjugates(K!phi(G.2));
[ -0.2599210498948731647672106072782283505702514647009999999995,
1.6299605249474365823836053036391141752851257323513843923104 -
1.09112363597172140356007261418980888132587333874018547370560*i,
1.6299605249474365823836053036391141752851257323513843923104 +
1.09112363597172140356007261418980888132587333874018547370560*i ]
> Logs(K!phi(G.2));   // image of infinite order unit -- generates a lattice
[ -1.3473773483293841009181878914456530462830622733209999999989\
, 0.6736886741646920504590939457228265231415311366603288999999 ]
> Logs(K!phi(G.1));   // image of -1
[ 0.E-57, 0.E-57 ]
```

Let's try a field such that $r + s - 1 = 2$. First, one with $r = 0$ and $s = 3$:

```
> K<a> := NumberField(x^6+x+1);
> Signature(K);
0 3
> G, phi := UnitGroup(K);
> G;
Abelian Group isomorphic to Z/2 + Z + Z
Defined on 3 generators
Relations:
    2*G.1 = 0
> u1 := K!phi(G.2); u1;
a
> u2 := K!phi(G.3); u2;
-2*a^5 - a^3 + a^2 + a
> Logs(u1);
[ 0.11877157353322375762475480482285510811783185904379239999998,
0.048643909752673399635150940533329986148342128393119899999997,
-0.16741548328589715725990574535618509426617398743691229999999 ]
> Logs(u2);
[ 1.6502294567845884711894772749682228152154948421589999999997,
-2.0963853913452777953249166008337095194338210890229999999997,
0.4461559345606893241354393258654867042183262468643346999994 ]
```

Notice that the log image of u_1 is clearly not a real multiple of the log image of u_2 (e.g., the scalar would have to be positive because of the first coefficient, but negative because of the second). This illustrates the fact that the log images of u_1 and u_2 span a two-dimensional space.

Next we compute a field with $r = 3$ and $s = 0$. (A field with $s = 0$ is called "totally real".)

```
> K<a> := NumberField(x^3 + x^2 - 5*x - 1);
> Signature(K);
3 0
> G, phi := UnitGroup(K);
> G;
Abelian Group isomorphic to Z/2 + Z + Z
Defined on 3 generators
Relations:
    2*G.1 = 0
> u1 := K!phi(G.2); u1;
1/2*(a^2 + 2*a - 1)
> u2 := K!phi(G.3); u2;
a
> Logs(u1);
[ 1.1676157469275875715959825186368130294698776047489999999995,
-0.3928487245813982612917986258343595187584142264304436999996,
-0.774767022346189310304183892802453510711463378318176699998 ]
> Logs(u2);
[ 0.6435429462288618773851817227686467257757954024463081999999,
-1.640224150322317146910150555170085057558346422666999999999,
0.996681204093455269524968832401438331782551020220549899998 ]
```

A family of fields with $r = 0$ (totally complex) is the *cyclotomic fields* $\mathbf{Q}(\zeta_n)$. The degree of $\mathbf{Q}(\zeta_n)$ over $\mathbf{Q}$ is $\varphi(n)$ and $r = 0$, so $s = \varphi(n)/2$ (assuming $n > 2$).

```
> K := CyclotomicField(11); K;
Cyclotomic Field of order 11 and degree 10
> G, phi := UnitGroup(K);
> G;
Abelian Group isomorphic to Z/22 + Z + Z + Z + Z
Defined on 5 generators
Relations:
    22*G.1 = 0
> u := K!phi(G.2); u;
zeta_11^9 + zeta_11^8 + zeta_11^7 + zeta_11^6 + zeta_11^5 +
    zeta_11^3 + zeta_11^2 + zeta_11 + 1
> Logs(u);
[ -1.256566324178728487453222159299768039916630803888999999999969,
0.651796894033140007971792388468509918282328440230327399999,
-0.185330046559862140949221639201972215564315421718192699999999,
0.520284982030074939330698573411850755138895506527223699998,
0.26981449467537568109995283662137958205972227885009159999993 ]
> K!phi(G.3);
zeta_11^9 + zeta_11^7 + zeta_11^6 + zeta_11^5 + zeta_11^4 +
    zeta_11^3 + zeta_11^2 + zeta_11 + 1
> K!phi(G.4);
zeta_11^9 + zeta_11^8 + zeta_11^7 + zeta_11^6 + zeta_11^5 +
    zeta_11^4 + zeta_11^3 + zeta_11^2 + zeta_11
> K!phi(G.5);
zeta_11^9 + zeta_11^8 + zeta_11^7 + zeta_11^6 + zeta_11^5 +
    zeta_11^4 + zeta_11^2 + zeta_11 + 1
```

How far can we go computing unit groups of cyclotomic fields directly with MAGMA?

```
> time G,phi := UnitGroup(CyclotomicField(13));
Time: 2.210
> time G,phi := UnitGroup(CyclotomicField(17));
Time: 8.600
> time G,phi := UnitGroup(CyclotomicField(23));
.... I waited over 10 minutes (usage of 300MB RAM) and gave up.
```

3 Preview

Next week will skip Section I.4 (pages 23–26 of the text) and jump into Section I.5 which is about extra structure in the case when K is Galois over $\mathbf{Q}$; the results are nicely algebraic, beautiful, and have interesting ramifications. We'll learn about Frobenius elements, the Artin symbol, decomposition groups, and how the Galois group of K is related to Galois groups of residue class fields. These are the basic structures needed to make any sense of representations of Galois groups, which is at the heart of much of number theory.