Introduction to Algebraic Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Units in Real Quadratic Fields

- Let K be the number field $\mathbb{Q}(\sqrt{d})$, with $d > 0$ a squarefree integer.
- Suppose $\sqrt{d}$ is chosen to be the positive square root of d.
- This is equivalent to choosing an embedding from K into $\mathbb{R}$.
- It allows regarding one element of K as larger or smaller than another.
- We work out some units for $\mathbb{Q}(\sqrt{2})$.
- Previous calculations show that the ring of integers is $\mathbb{Z}[\sqrt{2}]$.
- So a general integer is one of the form

$$a + b\sqrt{2}, \quad a, b \in \mathbb{Z}.$$

Units in Real Quadratic Fields

- A general integer is one of the form
$$a + b\sqrt{2}, \quad a, b \in \mathbb{Z}.$$
- The norm of $a + b\sqrt{2}$ is given by
$$N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2.$$
- Units have the property that their norm is ± 1.
- We therefore need to solve the equation
$$a^2 - 2b^2 = \pm 1.$$
- This is an example of **Pell's equation**,
$$x^2 - ny^2 = 1.$$
- In the next section, we see how to solve it using continued fractions.

Some Solutions of $a^2 - 2b^2 = \pm 1$

- Consider the equation
$$a^2 - 2b^2 = \pm 1.$$
- It certainly has the trivial solutions $a = \pm 1$, $b = 0$.
- These correspond to the elements ± 1 in $\mathbb{Q}(\sqrt{2})$.
- We can see that $a = \pm 1$, $b = \pm 1$, also give solutions.
- They corresponding to units $\pm 1 \pm \sqrt{2}$.
- Notice that:
$$\begin{array}{rcl} -(1+\sqrt{2}) & = & -1-\sqrt{2}; \\ (1+\sqrt{2})^{-1} & = & -1+\sqrt{2}; \\ -(1+\sqrt{2})^{-1} & = & 1-\sqrt{2}. \end{array}$$
- So all these units are easily generated from $1+\sqrt{2}$.

Some Solutions of $a^2 - 2b^2 = \pm 1$ (Cont'd)

- In the imaginary quadratic case, it was always true that the units were roots of unity.
- $1+\sqrt{2}$ is not a root of unity, since it is a real number greater than 1.
- The product of units is again a unit.
- So any power of $1+\sqrt{2}$ is also a unit.
- E.g., $(1+\sqrt{2})^2 = 3+2\sqrt{2}$ is a unit.
- Its inverse is $3-2\sqrt{2}$.
- More generally, $(1+\sqrt{2})^n$ is a unit, for all $n \geq 1$.
- Since $(1+\sqrt{2})^{-1} = (-1+\sqrt{2})$, we can conclude that $(1+\sqrt{2})^n$ is a unit, for every integer n.
- So, from the single unit $1+\sqrt{2}$, we can generate infinitely many units $\{\pm(1+\sqrt{2})^n\}$.
- We will see that these are the only units in $\mathbb{Z}[\sqrt{2}]$.

The Case $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$

- Let $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$.
- An element $\lambda = a + b\sqrt{d}$ is a unit if and only if its norm is ± 1.
- The norm is given by

$$N_{K/\mathbb{Q}}(\lambda) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2.$$

- So we need (a, b) to be a solution of the equation

$$x^2 - dy^2 = \pm 1.$$

- The equation $x^2 - dy^2 = 1$, where d is a positive integer and not a square, is known as **Pell's equation**.

The Case $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$ (Cont'd)

- Pell's equation
$$x^2 - dy^2 = \pm 1$$
always has infinitely many integral solutions.
- To find them, one way is to observe that the equation $x^2 - dy^2 = 1$ implies that x^2 and dy^2 are very close, so that $\frac{x^2}{y^2}$ is approximately d.
- In particular, $\frac{x}{y}$ is very close to $\sqrt{d}$.
- Finding rational numbers close to a given real number can be done using the theory of continued fractions.

Subsection 1

Continued Fractions

Example of a Continued Fraction

- Considered again Euclid's algorithm for the pair 630 and 132.

$$\begin{aligned} 630 &= 4 \cdot 132 + 102 \\ 132 &= 1 \cdot 102 + 30 \\ 102 &= 3 \cdot 30 + 12 \\ 30 &= 2 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 + 0 \end{aligned}$$

One consequence is that we can cancel the highest common factor of 6 from the numerator and denominator to get the fraction $\frac{105}{22}$ in lowest terms.

Example of a Continued Fraction (Cont'd)

- We also see that:

$$\begin{aligned} \frac{630}{132} &= 4+\frac{102}{132} \\ \frac{132}{102} &= 1+\frac{30}{102} \\ \frac{102}{30} &= 3+\frac{12}{30} \\ \frac{30}{12} &= 2+\frac{6}{12} \\ \frac{12}{6} &= 2+\frac{0}{6} \end{aligned}$$

  We see that the left-hand side of each equation is the reciprocal of the final term on the right-hand side of the previous one.

Example of a Continued Fraction (Cont'd)

- We can combine the preceding equations into a single expression.

$$\begin{aligned}
\frac{630}{132} &= 4+\frac{102}{132} \\
&= 3+\frac{1}{\frac{132}{102}} \\
&= 4+\frac{1}{1+\frac{30}{102}} \\
&= 4+\frac{1}{1+\frac{1}{\frac{102}{30}}} \\
&= \cdots \\
&= 4+\frac{1}{1+\frac{1}{3+\frac{1}{2+\frac{1}{2}}}}.
\end{aligned}$$

This last expression is the **continued fraction** for $\frac{630}{132}$.
We use the abbreviated form $[4;1,3,2,2]$.

Example of a Continued Fraction (Cont'd)

- We can obtain fractions which approximate the original expression by taking only the initial parts of the expression.

$$\begin{aligned}
[4] &= 4 \\
[4;1] &= 4+\tfrac{1}{1}=5 \\
[4;1,3] &= 4+\tfrac{1}{1+\frac{1}{3}}=\tfrac{19}{4} \\
[4;1,3,2] &= 4+\tfrac{1}{1+\frac{1}{3+\frac{1}{2}}}=\tfrac{43}{9}.
\end{aligned}$$

These fractions approach the original expression very quickly.

They are known as the **convergents**.

Tabular Representation

- To recover the convergents we list the numbers appearing in the continued fraction expansion, together with two further rows, in a table as follows:

		4	1	3	2	2
0	1					
1	0					

Each column is completed by taking the previous column, multiplying by the integer at the top, and adding the column before that.

		4	1	3	2	2
0	1	$4\times 1+0$				
1	0	$4\times 0+1$				

		4	1	3	2	2
0	1	4	$1\times 4+1$			
1	0	1	$1\times 1+0$			

		4	1	3	2	2
0	1	4	5	$3\times 5+4$		
1	0	1	1	$3\times 1+1$		

		4	1	3	2	2
0	1	4	5	19	43	105
1	0	1	1	4	9	22

The numerator and denominator of the convergents appear as the columns.

Notation for Convergents

- Consider a number $\xi \in \mathbb{R}$.
- Write $\rho_n = \frac{p_n}{q_n}$ for the convergents to ξ.
- $\frac{p_0}{q_0}$ corresponds to the entry below the first number.
- So we have $p_0 = \lfloor \xi \rfloor$ and $q_0 = 1$.
- We extend this to the left.
- We obtain

$$p_{-2} = 0, \quad q_{-2} = 1,$$
$$p_{-1} = 1, \quad q_{-1} = 0.$$

- These represent the first two columns of the table.
- Suppose the continued fraction of ξ is $[a_0; a_1, a_2, \ldots]$.
- Then

$$\begin{array}{rcl} p_k & = & a_k p_{k-1} + p_{k-2}, \\ q_k & = & a_k q_{k-1} + q_{k-2}. \end{array}$$

Successive Convergents

Lemma

If $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$ are successive convergents, then

$$p_{n+1}q_n - p_n q_{n+1} = (-1)^n.$$

- We prove this by induction on n.
  For $n = -2$, $p_{-1}q_{-2} - p_{-2}q_{-1} = 1$.
  Now suppose that $p_{k+1}q_k - p_k q_{k+1} = (-1)^k$.
  We have

$$\begin{aligned} p_{k+2} &= a_{k+2}p_{k+1} + p_k, \\ q_{k+2} &= a_{k+2}q_{k+1} + q_k. \end{aligned}$$

  It follows that

$$\begin{aligned} p_{k+2}q_{k+1} - p_{k+1}q_{k+2} &= (a_{k+2}p_{k+1} + p_k)q_{k+1} - p_{k+1}(a_{k+2}q_{k+1} + q_k) \\ &= -(p_{k+1}q_k - p_k q_{k+1}). \end{aligned}$$

Notation for Continued Fractions

- Suppose

$$\xi = [a_0; a_1, a_2, \ldots] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}.$$

- Set

$$\xi_n = [a_n; a_{n+1}, a_{n+2}, \ldots].$$

- Then we have, e.g.,

$$\begin{aligned} \xi &= a_0 + \frac{1}{\xi_1} \\ &= a_0 + \frac{1}{a_1 + \frac{1}{\xi_2}} \\ &= \cdots. \end{aligned}$$

An Expression in Terms of Continued Fractions

Lemma

We have

$$\xi = [a_0; a_1, \ldots, a_{n-1}, \xi_n] = \frac{\xi_n p_{n-1} + p_{n-2}}{\xi_n q_{n-1} + q_{n-2}}.$$

- By definition, $\xi = [a_0; a_1, \ldots, a_{n-1}, \xi_n]$.

  The second is a special case of the general claim that, for all x,

  $$[a_0; a_1, \ldots, a_n, x] = \frac{x p_n + p_{n-1}}{x q_n + q_{n-1}}.$$

  We prove this by induction.

  For $n = 0$,

  $$[a_0; x] = \frac{x p_0 + p_{-1}}{x q_0 + q_{-1}} = \frac{x \lfloor \xi \rfloor + 1}{x \cdot 1 + 0} = \lfloor \xi \rfloor + \frac{1}{x}.$$

  This is clearly true, by definition.

An Expression in Terms of Continued Fractions (Cont'd)

- Suppose that it is also true when $n=k-1$.

  Then we have

$$\begin{aligned}[a_0;a_1,\ldots,a_k,x] &= [a_0;a_1,\ldots,a_k+\tfrac{1}{x}] \\ &= \frac{(a_k+\frac{1}{x})p_{k-1}+p_{k-2}}{(a_k+\frac{1}{x})q_{k-1}+q_{k-2}} \\ &\quad \text{(induction hypothesis)} \\ &= \frac{x(a_kp_{k-1}+p_{k-2})+p_{k-1}}{x(a_kq_{k-1}+q_{k-2})+q_{k-1}} \\ &= \frac{xp_k+p_{k-1}}{xq_k+q_{k-1}}.\end{aligned}$$

Rational Approximations Using Convergents

- If ξ is irrational, the continued fraction convergents are very close rational approximations.

Proposition

Suppose that ξ is irrational. For any $n \geq 0$,

$$\left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}.$$

- We have, using the lemma,

$$\begin{aligned}
\xi - \frac{p_n}{q_n} &= \frac{\xi_{n+1} p_n + p_{n-1}}{\xi_{n+1} q_n + q_{n-1}} - \frac{p_n}{q_n} \\
&= \frac{p_{n-1} q_n - p_n q_{n-1}}{q_n(\xi_{n+1} q_n + q_{n-1})} \\
&= \frac{(-1)^n}{q_n(\xi_{n+1} q_n + q_{n-1})}.
\end{aligned}$$

Rational Approximations Using Convergents (Cont'd)

- We got
$$\xi - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n(\xi_{n+1}q_n + q_{n-1})}.$$
So
$$\begin{aligned} \left|\xi - \frac{p_n}{q_n}\right| &= \frac{1}{q_n(\xi_{n+1}q_n + q_{n-1})} \\ &\stackrel{a_{n+1} = \lfloor \xi_{n+1} \rfloor < \xi_{n+1}}{<} \frac{1}{q_n(a_{n+1}q_n + q_{n-1})} \\ &= \frac{1}{q_n q_{n+1}}. \end{aligned}$$

Relative Size of a Number and its Convergents

Corollary

If $\rho_n = \frac{p_n}{q_n}$ are the convergents to ξ, then if $\xi < \rho_n$, it follows that $\xi > \rho_{n+1}$ and vice versa.

- Recall the expression

$$\xi - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n(\xi_{n+1}q_n + q_{n-1})}.$$

It is clearly alternating in sign.

This yields the conclusion.

Rational Numbers and Convergents

Proposition

Suppose $\frac{a}{b}$ is a rational number such that

$$|b\xi - a| < |q_n\xi - p_n|.$$

Then $b \geq q_{n+1}$.

- Suppose that we have $|b\xi - a| < |q_n\xi - p_n|$, for some $b < q_{n+1}$.

  We know $p_nq_{n+1} - p_{n+1}q_n = \pm 1$.

  So there are integers x and y, such that

$$\begin{aligned} xp_n + yp_{n+1} &= a, \\ xq_n + yq_{n+1} &= b. \end{aligned}$$

  Clearly $x \neq 0$, for otherwise $yq_{n+1} = b$, and so $b \geq q_{n+1}$.

Rational Numbers and Convergents (Cont'd)

- Suppose $y = 0$.
  Then $a = xp_n$ and $b = xq_n$.
  Hence,
  $$|b\xi - a| = |x| \cdot |q_n\xi - p_n| \geq |q_n\xi - p_n|.$$
  This gives a contradiction.
  Suppose $y < 0$. Then $xq_n = b - yq_{n+1}$. So $x > 0$.
  Suppose $y > 0$. Then, as $b < q_{n+1}$, $xq_n = b - yq_{n+1} < 0$. So, $x < 0$.
  So x and y have opposite signs.
  Then $x(q_n\xi - p_n)$ and $y(q_{n+1}\xi - p_{n+1})$ have the same signs, by the preceding corollary.
  So we have
  $$|b\xi - a| = |x(q_n\xi - p_n) + y(q_{n+1}\xi - p_{n+1})| > |x(q_n\xi - p_n)| \geq |q_n\xi - p_n|.$$
  This gives a contradiction.

Optimality Property of Convergents

- We next show that $\frac{p_n}{q_n}$ is the best convergent amongst rationals with denominators of the same size or smaller.

Corollary

If $\frac{a}{b}$ is a rational number such that

$$\left|\xi - \frac{a}{b}\right| < \left|\xi - \frac{p_n}{q_n}\right|, \quad \text{for some } n,$$

then $b > q_n$.

- Suppose that there is some $\frac{a}{b}$, with $|\xi - \frac{a}{b}| < |\xi - \frac{p_n}{q_n}|$ and $b \leq q_n$. Then

$$b\left|\xi - \frac{a}{b}\right| < q_n\left|\xi - \frac{p_n}{q_n}\right|.$$

So $|b\xi - a| < |q_n\xi - p_n|$.

This contradicts the proposition.

Criterion for Convergents

Proposition

Suppose that ξ is irrational and that $\frac{a}{b}$ is a rational, with

$$\left|\xi - \frac{a}{b}\right| < \frac{1}{2b^2}.$$

Then $\frac{a}{b}$ is a continued fraction convergent to ξ.

- As before, write $\frac{p_n}{q_n}$ for the convergents to ξ.
  Suppose that $\frac{a}{b}$ is not a convergent.
  Then $q_n \leq b < q_{n+1}$, for some n.
  By a preceding proposition, we also have $|b\xi - a| \geq |q_n\xi - p_n|$.
  Then
  $$|q_n\xi - p_n| \leq |b\xi - a| < \frac{1}{2b}.$$

Criterion for Convergents (Cont'd)

- We found $|q_n\xi - p_n| < \frac{1}{2b}$.
  So
  $$\left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{2bq_n}.$$
  But this means that
  $$\begin{aligned} \frac{1}{bq_n} &\leq \frac{|bp_n - aq_n|}{bq_n} \\ &= \left|\frac{p_n}{q_n} - \frac{a}{b}\right| \\ &\leq \left|\xi - \frac{p_n}{q_n}\right| + \left|\xi - \frac{a}{b}\right| \\ &< \frac{1}{2bq_n} + \frac{1}{2b^2}. \end{aligned}$$
  This implies that $b < q_n$, a contradiction.

Subsection 2

Continued Fractions of Square Roots

Example

- We compute the continued fraction of $\sqrt{19}$.

  It turns out that we just need to know that $4 < \sqrt{19} < 5$.

  Start with the integer part and remainder

$$\sqrt{19} = 4 + (\sqrt{19} - 4).$$

  Then do the same for the reciprocal of the remainder, rationalizing the denominator:

$$\frac{1}{\sqrt{19} - 4} = \frac{\sqrt{19} + 4}{3} = 2 + \frac{\sqrt{19} - 2}{3}.$$

Example (Cont'd)

- This repeats:

$$\begin{aligned}
\frac{3}{\sqrt{19}-2} &= \frac{\sqrt{19}+2}{5} = 1 + \frac{\sqrt{19}-3}{5};\\
\frac{5}{\sqrt{19}-3} &= \frac{\sqrt{19}+3}{2} = 3 + \frac{\sqrt{19}-3}{2};\\
\frac{2}{\sqrt{19}-3} &= \frac{\sqrt{19}+3}{5} = 1 + \frac{\sqrt{19}-2}{5};\\
\frac{5}{\sqrt{19}-2} &= \frac{\sqrt{19}+2}{3} = 2 + \frac{\sqrt{19}-4}{3};\\
\frac{3}{\sqrt{19}-4} &= \sqrt{19}+4 = 8 + (\sqrt{19}-4).
\end{aligned}$$

Then the process repeats and we get the infinite continued fraction

$$[4;2,1,3,1,2,8,2,1,3,1,2,8,2,1,3,1,2,8,\ldots].$$

This is abbreviated $[4;\overline{2,1,3,1,2,8}]$.

Real Square Roots as Continuous Fractions

Proposition

Let d be a positive integer, not a square. Define

$$M_0 = 0, \quad N_0 = 1, \quad \xi_0 = \sqrt{d}, \quad a_0 = \lfloor \xi_0 \rfloor.$$

Then define recursively sequences by

$$M_{n+1} = a_n N_n - M_n, \quad N_{n+1} = \frac{d - M_{n+1}^2}{N_n},$$
$$\xi_{n+1} = \frac{\sqrt{d} + M_{n+1}}{N_{n+1}}, \quad a_{n+1} = \lfloor \xi_{n+1} \rfloor.$$

Then:

1. M_n and N_n are integers for all n;
2. $\xi_n = a_n + \frac{1}{\xi_{n+1}}$, and so $\xi = [a_0; a_1, a_2, \ldots]$.

Real Square Roots as Continuous Fractions (Cont'd)

1. We prove this by induction.

   Clearly M_0 and N_0 are integers.

   The inductive hypothesis is that M_k and N_k are integers for $k \leq n$.

   By definition, a_n is always an integer.

   So clearly $M_{n+1} = a_n N_n - M_n$ is an integer.

   The real content of this proposition is that N_{n+1} should be an integer.

   Now we have

$$N_{n+1} = \frac{d - M_{n+1}^2}{N_n} = \frac{d - (a_n N_n - M_n)^2}{N_n} = \frac{d - M_n^2}{N_n} + 2a_n M_n - a_n^2 N_n.$$

   So we just need to check that $\frac{d-M_n^2}{N_n}$ is an integer.

   If $n \geq 1$, $N_n = \frac{d-M_n^2}{N_{n-1}}$. So $N_n \mid d - M_n^2$.

   If $i = 0$, $N_0 = 1$. So $N_0 \mid d - M_0^2$.

Real Square Roots as Continuous Fractions (Cont'd)

2. We work by substituting the expressions for ξ_{n+1} into $a_n + \dfrac{1}{\xi_{n+1}}$.

$$\begin{aligned} a_n + \frac{1}{\xi_{n+1}} &= a_n + \frac{N_{n+1}}{\sqrt{d} + M_{n+1}} \\ &= a_n + \frac{\frac{d - M_{n+1}^2}{N_n}}{\sqrt{d} + M_{n+1}} \\ &= a_n + \frac{\sqrt{d} - M_{n+1}}{N_n} \\ &= a_n + \frac{\sqrt{d} + M_n - a_n N_n}{N_n} \\ &= \frac{\sqrt{d} + M_n}{N_n} = \xi_n. \end{aligned}$$

Real Square Roots as Continuous Fractions (Cont'd)

Lemma

With the notation of the previous result, $N_n > 0$ for all sufficiently large n.

- Write $\xi'_n = \frac{-\sqrt{d}+M_n}{N_n}$ for the conjugate of ξ_n.

  By a previous lemma, $\xi = \xi_0 = \frac{\xi_n p_{n-1} + p_{n-2}}{\xi_n q_{n-1} + q_{n-2}}$. So $\xi'_0 = \frac{\xi'_n p_{n-1} + p_{n-2}}{\xi'_n q_{n-1} + q_{n-2}}$.

  Solving for ξ'_n, we have $\xi'_n = -\frac{q_{n-2}\xi'_0 - p_{n-2}}{q_{n-1}\xi'_0 - p_{n-1}}$. Rearranging, we get

  $$\xi'_n = -\frac{q_{n-2}}{q_{n-1}} \left(\frac{\xi'_0 - \frac{p_{n-2}}{q_{n-2}}}{\xi'_0 - \frac{p_{n-1}}{q_{n-1}}} \right).$$

  As $k \to \infty$, $\frac{p_k}{q_k} \to \xi_0$. So the bracket tends to 1.

  Thus, for large enough n, $\xi'_n < 0$.

  Hence, $\xi_n > 0$ and $\xi'_n < 0$ for such n.

  We get $\frac{2\sqrt{d}}{N_n} = \xi_n - \xi'_n > 0$. Therefore, $N_n > 0$.

Repetition of the ξ's

Lemma

With the notation of the previous results, there exists an integer $k > 0$ with $\xi_j = \xi_{j+k}$, for some j.

- We know that $\xi_n = \frac{\sqrt{d}+M_n}{N_n}$.

  Moreover, $N_n N_{n+1} = d - M_{n+1}^2$ and $N_n > 0$, for sufficiently large n.

  For all such n, $M_{n+1}^2 < d$.

  So there are only finitely many possibilities for each M_n.

  Also, $N_n N_{n+1} < d$.

  Hence, if $N_n > 0$, we get $N_{n+1} < d$.

  So that there are only finitely many possibilities for N_n also.

  This shows that eventually, $\xi_j = \xi_{j+k}$, for some j and $k > 0$.

Form of the Continued Fraction for $\sqrt{d}$

Theorem

The continued fraction of $\sqrt{d}$ has the form $[b_0;\overline{b_1,\ldots,b_k}]$ where $b_k = 2b_0$.

- Take $\xi_0 = \sqrt{d} + \lfloor\sqrt{d}\rfloor$.
  We work out the continued fraction $[a_0, a_1, \ldots]$ of ξ_0.
  Certainly $\xi_0 > 1$ and $a_0 \geq 1$.
  $\xi_0' = \lfloor\sqrt{d}\rfloor - \sqrt{d}$ satisfies $-1 < \xi_0' < 0$.
  Claim: $-1 < \xi_n' < 0$, for all non-negative integers n.
  By induction.
  We have $\frac{1}{\xi_{n+1}} = \xi_n - a_n$. So $\frac{1}{\xi'_{n+1}} = \xi'_n - a_n$.
  Suppose $\xi'_n < 0$. Then $\frac{1}{\xi'_{n+1}} < 0$. Hence, $\xi'_{n+1} < 0$.
  Suppose, again, $\xi'_n < 0$.
  Since $a_n \geq 1$ as d is not a square, $\frac{1}{\xi'_{n+1}} < -1$.
  So $-1 < \xi'_{n+1}$. Thus, $-1 < \xi'_{n+1} < 0$.

Form of the Continued Fraction for $\sqrt{d}$ (Cont'd)

- Now we have $-1 < \xi'_n < 0$.
  So we get $-1 < \frac{1}{\xi'_{n+1}} - a_n < 0$.
  Thus, $a_n = \left\lfloor -\frac{1}{\xi'_{n+1}} \right\rfloor$.
  By the previous lemma, there are integers j and $k > 0$, with $\xi_j = \xi_{j+k}$.
  But this implies that $\xi'_j = \xi'_{j+k}$.
  Then
  $$a_{j-1} = \left\lfloor -\frac{1}{\xi'_j} \right\rfloor = \left\lfloor -\frac{1}{\xi'_{j+k}} \right\rfloor = a_{j+k-1}.$$
  Finally,
  $$\xi_{j-1} = a_{j-1} + \frac{1}{\xi_j} = a_{j+k-1} + \frac{1}{\xi_{j+k}} = \xi_{j+k-1}.$$
  Applying this repeatedly, we see that $\xi_0 = \xi_k$.
  So the continued fraction repeats.

Form of the Continued Fraction for $\sqrt{d}$ (Cont'd)

- We get that $\xi_0 = [\overline{a_0, a_1, \ldots, a_{k-1}}]$.

  We have $\xi_0 = \sqrt{d} + \lfloor\sqrt{d}\rfloor$.

  So the continued fraction $[a_0, a_1, \ldots]$ of ξ_0 is identical to the continued fraction $[b_0, b_1, \ldots]$ of $\sqrt{d}$ except that $b_0 = a_0 - \lfloor\sqrt{d}\rfloor$.

  But $a_0 = \lfloor\xi_0\rfloor = 2\lfloor\sqrt{d}\rfloor$.

  So $b_0 = \lfloor\sqrt{d}\rfloor$ and $a_0 = 2b_0$.

  By the periodicity of the continued fraction for ξ_0, we have $a_0 = a_k = b_k$. So $b_k = 2b_0$, as claimed.

Definition

We say that $k > 0$ is the **period** of $\sqrt{d}$ if it is the smallest index with $\xi_k = \xi_0$.

Relation Between Convergents and the ξ_n's

- Recall that if $\xi = \sqrt{d}$, we put $\xi_n = \frac{\sqrt{d}+M_n}{N_n}$.

Proposition

If $\frac{p_n}{q_n}$ denotes the nth convergent to $\sqrt{d}$, then $p_n^2 - dq_n^2 = (-1)^{n+1} N_{n+1}$.

- Put $\xi_0 = \sqrt{d}$, and define $\xi_n = \frac{\sqrt{d}+M_n}{N_n}$.
  By a previous lemma, $\sqrt{d} = \frac{\xi_{n+1} p_n + p_{n-1}}{\xi_{n+1} q_n + q_{n-1}}$.
  By definition, $\xi_{n+1} = \frac{\sqrt{d}+M_{n+1}}{N_{n+1}}$.
  We substitute this in and simplify to get

$$\begin{aligned}\sqrt{d} &= \frac{\xi_{n+1} p_n + p_{n-1}}{\xi_{n+1} q_n + q_{n-1}} = \frac{\frac{\sqrt{d}+M_{n+1}}{N_{n+1}} p_n + p_{n-1}}{\frac{\sqrt{d}+M_{n+1}}{N_{n+1}} q_n + q_{n-1}} \\ &= \frac{M_{n+1} p_n + N_{n+1} p_{n-1} + p_n \sqrt{d}}{M_{n+1} q_n + N_{n+1} q_{n-1} + q_n \sqrt{d}}.\end{aligned}$$

Relation Between Convergents and the ξ_n's (Cont'd)

- Rearranging this gives

$$dq_n + \sqrt{d}(M_{n+1}q_n + N_{n+1}q_{n-1}) = M_{n+1}p_n + N_{n+1}p_{n-1} + \sqrt{d}p_n.$$

Equating coefficients of $\sqrt{d}$ and the remaining terms gives the two equations

$$M_{n+1}p_n + N_{n+1}p_{n-1} = dq_n, \quad M_{n+1}q_n + N_{n+1}q_{n-1} = p_n.$$

Multiply the first equation by q_n, and the second by p_n, to get

$$\begin{array}{rcl} M_{n+1}p_nq_n + N_{n+1}p_{n-1}q_n & = & dq_n^2; \\ M_{n+1}p_nq_n + N_{n+1}q_{n-1}p_n & = & p_n^2. \end{array}$$

Subtract to get

$$p_n^2 - dq_n^2 = N_{n+1}(p_nq_{n-1} - q_np_{n-1}).$$

The result follows from a previous lemma.

Solutions of Pell's Equation

- We deduce the main result on Pell's equation.
- If $x^2 - dy^2 = 1$, then $\frac{x^2}{y^2}$ will be close to d.
- So $\frac{x}{y}$ will be close to $\sqrt{d}$.
- So we look for solutions among the convergents to $\sqrt{d}$.

Theorem

Let $d > 0$ be an integer, not a square.

- The equation $x^2 - dy^2 = 1$ has infinitely many solutions;
- The equation $x^2 - dy^2 = -1$ has infinitely many solutions if the continued fraction for $\sqrt{d}$ has odd period.

Solutions of Pell's Equation (Cont'd)

- From the previous result, we know that

$$p_n^2 - dq_n^2 = (-1)^{n+1} N_{n+1},$$

where:
  - $\frac{p_n}{q_n}$ is a convergent to $\sqrt{d}$;
  - N_{n+1} is the denominator of ξ_{n+1}.

We also know that the sequence (ξ_n) repeats with some period k.

This means that (N_n) repeats with period k.

As $N_0 = 1$, we deduce that $N_{sk} = 1$, for all integers $s \geq 0$.

Suppose s or k even and n is of the form $sk - 1$.

Then (p_n, q_n) solves $x^2 - dy^2 = 1$.

So there are always infinitely many solutions.

Suppose k and s are odd and $n = sk - 1$.

Then (p_n, q_n) solves $x^2 - dy^2 = -1$.

Example

- We repeat the table of convergents for $\sqrt{19}$.

  We add an extra row corresponding to the $p_n^2 - dq_n^2$.

		4	2	1	3	1	2	8
0	1	4	9	13	48	61	170	1421
1	0	1	2	3	11	14	39	326
	$p_n^2 - dq_n^2$	-3	5	-2	5	-3	1	-3

Subsection 3

Real Quadratic Fields

Work Plan

- Write K for the number field $\mathbb{Q}(\sqrt{d})$, where $d > 0$ is squarefree.
- We know that numbers of the form $\pm(1+\sqrt{2})^n$ were all units in $\mathbb{Z}[\sqrt{2}]$.
- So $\mathbb{Q}(\sqrt{2})$ has infinitely many units.
- We suggested that, in general, units $s+t\sqrt{d}$ (for the moment, we will suppose $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$) should have the property that $\frac{s}{t}$ is a continued fraction convergent to $\sqrt{d}$.
- In the previous sections we have shown how to compute these.
- We now turn to proving this is indeed the case.

Solutions of Pell's Equation and Convergents

Theorem

Let d be a squarefree positive integer, and write $\frac{p_n}{q_n}$ for the convergents to $\sqrt{d}$. Suppose that m is an integer with $|m| < \sqrt{d}$. Then any solution (s,t) to $x^2 - dy^2 = m$, with $(s,t) = 1$ satisfies $s = p_n$ and $t = q_n$, for some n.

- First consider the case $m > 0$. Suppose that $s^2 - dt^2 = m$.

  Then we have

$$\begin{array}{rcl} \frac{s}{t} & = & \sqrt{d + \frac{m}{t^2}} > \sqrt{d}; \\ 0 & < & \frac{s}{t} - \sqrt{d} = \frac{m}{t(s+t\sqrt{d})} < \frac{\sqrt{d}}{t(s+t\sqrt{d})} = \frac{1}{t^2(\frac{s}{t\sqrt{d}}+1)}. \end{array}$$

  As $\frac{s}{t} > \sqrt{d}$, we get $\frac{s}{t\sqrt{d}} > 1$. So $\left|\frac{s}{t} - \sqrt{d}\right| < \frac{1}{2t^2}$.
  The result follows from a previous proposition.

Solutions of Pell's Equation and Convergents (Cont'd)

- A similar argument applies when $m<0$, but with some complications.
- We can check that $\frac{s}{t}$ is a convergent to $\sqrt{d}$ precisely when $\frac{t}{s}$ is a convergent to $\frac{1}{\sqrt{d}}$.
- Rewrite the expression $s^2-dt^2=m$ as

$$t^2-\left(\frac{1}{d}\right)s^2=\left(-\frac{m}{d}\right).$$

- Observe that $-\frac{m}{d}>0$ and $\left|\frac{m}{d}\right|<\sqrt{\frac{1}{d}}$.
- So we may apply the preceding argument.
- In the same way, we conclude that $\frac{t}{s}$ is a convergent to $\sqrt{\frac{1}{d}}$.
- Therefore, $\frac{s}{t}$ is a convergent to $\sqrt{d}$.

Finding Units Using Convergents

- It follows that units $s+t\sqrt{d}$ can be computed by:
  - Looking through the continued fraction convergents to $\sqrt{d}$;
  - Finding those convergents $\frac{p_n}{q_n}$ with
$$p_n^2-dq_n^2=\pm 1.$$
- There are always solutions to this equation.
- We have already remarked that $N_{sk}=1$, for all values of s, where k denotes the period of $\sqrt{d}$.
- This means that there are convergents $\frac{p_n}{q_n}$, with
$$p_n^2-dq_n^2=\pm 1.$$

Finding Units Using Convergents ($d \equiv 1 \pmod 4$)

- The same method works also for the case $d \equiv 1 \pmod 4$.
- Here, though, integers are of two forms.
  - Some integers are of the form $a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$.
    We can find units of this form by solving $a^2 - db^2 = \pm 1$ as above.
  - Other integers are of the form $a + b\sqrt{d}$, with a, b halves of odd integers.
    In this case, we need solutions to $a^2 - db^2 = \pm 1$, with $a, b \in \frac{1}{2}\mathbb{Z}$.
    Multiplying by 4, we need to solve $A^2 - dB^2 = \pm 4$, with $A, B \in \mathbb{Z}$.
    The theorem guarantees that all solutions may be found in the continued fraction convergents to $\sqrt{d}$ (at least for $d \geq 17$; smaller cases can be treated by hand).

Example $\mathbb{Q}(\sqrt{61})$

- We find some units for $\mathbb{Q}(\sqrt{61})$.

  The continued fraction expansion of $\sqrt{61}$ is given by

  $$[7;\overline{1,4,3,1,2,2,1,3,4,1,14}].$$

  We can compute:

  - The convergents $\frac{p_n}{q_n}$;
  - The corresponding values of $p_n^2 - 61q_n^2$.

  The 7th convergent is $\frac{39}{5}$.

  Moreover, $39^2 - 61 \cdot 5^2 = -4$.

  It follows that $\frac{39+5\sqrt{61}}{2}$ is a unit.

  Then, for any integer n, $\pm(39+5\sqrt{61})^n$ are also units.

Example $\mathbb{Q}(\sqrt{2})$

- We explain that the units $\pm(1+\sqrt{2})^n$ are the only units of $\mathbb{Z}[\sqrt{2}]$.

  We first compute the continued fraction.

$$\sqrt{2}=1+(\sqrt{2}-1), \quad \frac{1}{\sqrt{2}-1}=\sqrt{2}+1=2+(\sqrt{2}-1).$$

  Then the process repeats with period 1.

  Thus, the continued fraction is $[1;\overline{2}]$.

  The table of convergents begins:

	a_n	1	2	2	2	2	2
0	1	1	3	7	17	41	99
1	0	1	2	5	12	29	70
	$p_n^2-2q_n^2$	-1	1	-1	1	-1	1

Example $\mathbb{Q}(\sqrt{2})$ (Cont'd)

- Suppose η denotes the smallest unit of $\mathbb{Z}[\sqrt{2}]$ satisfying
$$\eta > 1 \quad \text{and} \quad \eta = a + b\sqrt{2}.$$
Then $\frac{a}{b}$ must be a continued fraction convergent of $\sqrt{2}$.
The calculation above shows that $\eta = 1 + \sqrt{2}$.
Claim: The units in $\mathbb{Z}[\sqrt{2}]$ are all necessarily of the form $\pm\eta^n$.
Suppose that λ is a unit of $\mathbb{Z}[\sqrt{2}]$, and that $\lambda \neq \pm 1$.
Then one of $\lambda, -\lambda, \frac{1}{\lambda}$ and $-\frac{1}{\lambda}$ is greater than 1.
Suppose it is λ (if not, redefine λ so that it is this unit).
For some n, we have $\eta^n \leq \lambda < \eta^{n+1}$.
By multiplying throughout by η^{-n}, we get $1 \leq \lambda\eta^{-n} < \eta$.
So we find a unit $\lambda\eta^{-n}$ strictly less than η, and at least 1.
But η was chosen to be the smallest unit which was greater than 1.
So we must have $\lambda\eta^{-n} = 1$.
Then $\lambda = \eta^n$, as required.

Units in Real Quadratic Fields

Theorem

Suppose that K is a real quadratic field. Then there exists some unit $\eta > 1$, such that every unit of $\mathbb{Z}_K$ is of the form $\pm\eta^n$, for some integer n.

- Let η denote the smallest unit of $\mathbb{Z}_K$ greater than 1.
  This can always be found from the convergents of $\sqrt{d}$.
  Let λ be a unit of $\mathbb{Z}_K$, and that $\lambda \neq \pm 1$ (corresponding to $n = 0$).
  Suppose first that $\lambda > 1$.
  For some $n \geq 1$, we have $\eta^n \leq \lambda < \eta^{n+1}$.
  By multiplying throughout by η^{-n}, we get $1 \leq \lambda\eta^{-n} < \eta$.
  So we find a unit $\lambda\eta^{-n}$ strictly less than η, and at least 1.
  But η was chosen to be the smallest unit which was greater than 1.
  So we must have $\lambda\eta^{-n} = 1$.
  Then $\lambda = \eta^n$, for some integer $n \geq 1$.

Units in Real Quadratic Fields (Cont'd)

- Suppose $\lambda \neq \pm 1$ is any unit.
  Then one of $\lambda, -\lambda, \frac{1}{\lambda}$ and $-\frac{1}{\lambda}$ is greater than 1.
  Thus, it is of the form η^n, for some $n \geq 1$.
  So $\lambda = \pm \eta^n$, for some $n \in \mathbb{Z}$.

Fundamental Units

Definition

A unit $\eta > 1$, such that every unit in $\mathbb{Z}_K$ is of the form $\pm\eta^n$ is called a **fundamental unit**.

- From the proof of the theorem, it is clear that η may be chosen to be the smallest unit of $\mathbb{Z}_K$ greater than 1.
- We know that these may be found by examining the continued fraction expansion of $\sqrt{d}$.
- The units in $\mathbb{Z}_K$, written $U(\mathbb{Z}_K)$ or $\mathbb{Z}_K^\times$, are therefore given by $\{\pm 1\} \times \eta^{\mathbb{Z}}$, and are isomorphic as an abstract group to $C_2 \times \mathbb{Z}$.
  - The first component corresponds to the choice of sign;
  - The second component corresponds to the power of the fundamental unit.

Subsection 4

Biquadratic Fields

Biquadratic Fields

- We consider degree 4 extensions of the form $\mathbb{Q}(\sqrt{m}, \sqrt{n})$, where m and n are two squarefree integers, with $m \neq n$.
- Such fields are known as **biquadratic**.
- Let $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$.
- Consider
$$k = \frac{mn}{(m,n)^2}.$$
- Note that $\sqrt{k} \in K$.
- The three fields $\mathbb{Q}(\sqrt{m})$, $\mathbb{Q}(\sqrt{n})$ and $\mathbb{Q}(\sqrt{k})$ form the three quadratic subfields of K.

Embeddings

- There are four embeddings from K into $\mathbb{C}$:

$$a+b\sqrt{m}+c\sqrt{n}+d\sqrt{k} \mapsto \begin{cases} a+b\sqrt{m}+c\sqrt{n}+d\sqrt{k}, \\ a+b\sqrt{m}-c\sqrt{n}-d\sqrt{k}, \\ a-b\sqrt{m}+c\sqrt{n}-d\sqrt{k}, \\ a-b\sqrt{m}-c\sqrt{n}+d\sqrt{k}. \end{cases}$$

- These can be viewed as "conjugations" fixing each of the three quadratic subfields in turn.
- Each embedding actually has image equal to K.
- So these embeddings are automorphisms of K.

Possible Cases for m, n and k

Lemma

If $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$, then we can assume, without loss of generality, that we are in one of the following cases:

1. $m \equiv 3 \pmod 4$, $k \equiv n \equiv 2 \pmod 4$;
2. $m \equiv 1 \pmod 4$, $k \equiv n \equiv 2 \pmod 4$;
3. $m \equiv 1 \pmod 4$, $k \equiv n \equiv 3 \pmod 4$;
4. $m \equiv 1 \pmod 4$, $k \equiv n \equiv 1 \pmod 4$.

- First, suppose $2 \mid m$ and $2 \mid n$.

  As m and n are squarefree, $k = \frac{mn}{(m,n)^2}$ is odd.

  We have $\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m}, \sqrt{k})$.

  So we can always assume that (at least) one of the two generators is the square root of an odd integer.

Possible Cases for m, n and k (Cont'd)

- Suppose $m \equiv 3 \pmod 4$ and $n \equiv 1 \pmod 4$.
  We can simply interchange m and n as $\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{n}, \sqrt{m})$.
- Suppose $m \equiv 3 \pmod 4$ and $n \equiv 3 \pmod 4$.
  We can replace n by k.
  Now $mn = k(m,n)^2$, and (m,n) is odd (as m and n are).
  So (m,n) has square congruent to $1 \pmod 4$.
  So $k \equiv mn \pmod 4$.
  This implies that $k \equiv mn \equiv 1 \pmod 4$, and $\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m}, \sqrt{k})$.

Thus after permuting m, n and k, we can assume that m and n satisfy the given congruences.

Now m is always odd.

So (m,n) is always odd, as well.

Hence, $k \equiv mn \pmod 4$ by the argument given above.

So k also satisfies the given congruence.

Integral Basis for Biquadratic Fields

Proposition

With the numbering of the preceding lemma, an integral basis for (the rings of integers of) $\mathbb{Q}(\sqrt{m},\sqrt{n})$ are given by:

1. $\left\{1,\sqrt{m},\sqrt{n},\frac{\sqrt{n}+\sqrt{k}}{2}\right\}$;
2. $\left\{1,\frac{1+\sqrt{m}}{2},\sqrt{n},\frac{\sqrt{n}+\sqrt{k}}{2}\right\}$;
3. $\left\{1,\frac{1+\sqrt{m}}{2},\sqrt{n},\frac{\sqrt{n}+\sqrt{k}}{2}\right\}$;
4. $\left\{1,\frac{1+\sqrt{m}}{2},\frac{1+\sqrt{n}}{2},\frac{(1+\sqrt{m})(1+\sqrt{n})}{4}\right\}$.

Integral Basis for Biquadratic Fields (Cont'd)

- Let $\alpha \in \mathbb{Z}_K$.
  Then we can write
  $$\alpha = a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}, \quad a, b, c, d \in \mathbb{Q}.$$
  As $\alpha \in \mathbb{Z}_K$, all of its conjugates
  $$\begin{array}{rcl} \alpha_2 & = & a - b\sqrt{m} + c\sqrt{n} - d\sqrt{k}, \\ \alpha_3 & = & a + b\sqrt{m} - c\sqrt{n} - d\sqrt{k}, \\ \alpha_4 & = & a - b\sqrt{m} - c\sqrt{n} + d\sqrt{k} \end{array}$$
  are also algebraic integers.
  The set of algebraic integers is closed under addition.
  So the following are also algebraic integers
  $$\begin{array}{rcl} \alpha + \alpha_2 & = & 2a + 2c\sqrt{n}, \\ \alpha + \alpha_3 & = & 2a + 2b\sqrt{m}, \\ \alpha + \alpha_4 & = & 2a + 2d\sqrt{k}. \end{array}$$

Integral Basis for Biquadratic Fields (Case 1)

- Suppose $m \equiv 3 \pmod 4$ and $k \equiv n \equiv 2 \pmod 4$.

  By a previous proposition, these are integral if $2a, 2b, 2c, 2d \in \mathbb{Z}$.

  Thus,
  $$\alpha = \frac{A + B\sqrt{m} + C\sqrt{n} + D\sqrt{k}}{2},$$
  for $A, B, C, D \in \mathbb{Z}$, where $A = 2a$, $B = 2b$, $C = 2c$ and $D = 2d$.

  We also have
  $$\begin{aligned} \alpha\alpha_3 &= (a + b\sqrt{m})^2 - (c\sqrt{n} + d\sqrt{k})^2 \\ &= a^2 + 2\sqrt{m}ab + mb^2 - nc^2 - 2ncd\frac{\sqrt{m}}{(m,n)} - kd^2 \\ &= \frac{A^2 + mB^2 - nC^2 - kD^2}{4} + \frac{AB - nCD/(m,n)}{2}\sqrt{m}. \end{aligned}$$

  This is also integral.

  Thus $4 \mid A^2 + mB^2 - nC^2 - kD^2$ and $2 | AB - nCD/(m,n)$.

Integral Basis for Biquadratic Fields (Case 1 Cont'd)

- We know that n is even and m is odd.
  So (m,n) is odd and $n/(m,n)$ is even.
  Hence, $2|AB - nCD/(m,n)$ implies that $2 \mid AB$.
  So at least one of A and B is even.
  If only one were even, then $A^2 + mB^2 - nC^2 - kD^2$ would be odd.
  So the first requirement would fail.
  So both A and B are even.
  The second divisibility is automatic.
  The first reduces to $4 \mid nC^2 + kD^2$. Equivalently, $2 \mid C^2 + D^2$.
  So C and D are both even or both odd.
  So integers are all of the form

$$\alpha = a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k},$$

  $a, b \in \mathbb{Z}$ and c and d both integral or both halves of odd integers.

Integral Basis for Biquadratic Fields (Case 1 Conclusion)

- Such elements are integer linear combinations of

$$1, \quad \sqrt{m}, \quad \sqrt{n}, \quad \frac{\sqrt{n}+\sqrt{k}}{2}.$$

The first three are obviously integral.

Let $\gamma = \frac{\sqrt{n}+\sqrt{k}}{2}$.

Then

$$(4\gamma^2 - (n+k))^2 = \frac{4mn^2}{(m,n)^2}.$$

The congruence conditions on m, n and k imply that this simplifies to a monic polynomial with integer coefficients,

$$\gamma^4 - \frac{n+k}{2}\gamma^2 + \left(\frac{n+k}{4}\right)^2 = \frac{mn^2}{4(m,n)^2}.$$

So γ is also integral.

Thus, an integral basis is $\left\{1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right\}$.

Integral Basis for Biquadratic Fields (Cases 2 and 3)

- The remaining cases are similar and will be sketched.

  In the second and third cases, which can be treated together,

  $$m \equiv 1 \pmod 4 \quad \text{and} \quad k \equiv n \equiv 2 \text{ or } 3 \pmod 4.$$

  Suppose

  $$\alpha = a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k} \in \mathbb{Z}_K.$$

  One shows as in the first case that

  $$\alpha = a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}, \quad 2a, 2b, 2c, 2d \in \mathbb{Z}.$$

  Let α_2, α_3 and α_4 denote the conjugates of α.

Integral Basis for Biquadratic Fields (Cases 2 and 3 Cont'd)

- Considering $\alpha + \alpha_i$ again, one sees that:
  - a and b are both integers or both halves of odd integers;
  - c and d are both integers or both halves of odd integers.

  Then every integer must be an integer linear combination of

$$1, \quad \frac{1+\sqrt{m}}{2}, \quad \sqrt{n}, \quad \frac{\sqrt{n}+\sqrt{k}}{2}.$$

  We can then show that these are all integral.

Integral Basis for Biquadratic Fields (Case 4)

- The final case, $m \equiv k \equiv n \equiv 1 \pmod 4$ is a little different.

  Again we consider $\alpha + \alpha_2$, $\alpha + \alpha_3$ and $\alpha + \alpha_4$.

  By a previous proposition, these are integral if $4a, 4b, 4c, 4d \in \mathbb{Z}$, with $2a, 2b, 2c$ and $2d$ all integral or all halves of odd integers.

  Thus,

  $$\alpha = \frac{A + B\sqrt{m} + C\sqrt{n} + D\sqrt{k}}{4}, \quad A, B, C, D \in \mathbb{Z},$$

  where $A = 4a, B = 4b, C = 4c$ and $D = 4d$ are all even or all odd.

  So we can write

  $$\alpha = \frac{A' + B'\sqrt{m} + C'\sqrt{n}}{4} + D'\left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{n}}{2}\right), \quad D' \in \mathbb{Z}.$$

Integral Basis for Biquadratic Fields (Case 4 Cont'd)

- But
$$\frac{A'+B'\sqrt{m}+C'\sqrt{n}}{4}=\alpha-D'\left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{n}}{2}\right)$$
must be integral.
So A',B',C' are all even (the coefficient of $\sqrt{k}$ is 0, which is even).
Thus, $A'=2a'$, $B'=2b'$ and $C'=2c'$, and we consider
$$\frac{a'+b'\sqrt{m}+c'\sqrt{n}}{2}.$$
This is the sum of
$$b'\left(\frac{1+\sqrt{m}}{2}\right)+c'\left(\frac{1+\sqrt{n}}{2}\right) \quad \text{and} \quad \frac{a'-b'-c'}{2}.$$
It is an integer. So $2 \mid a'-b'-c'$.
It follows that the integral basis is $\left\{1,\frac{1+\sqrt{m}}{2},\frac{1+\sqrt{n}}{2},\frac{(1+\sqrt{m})(1+\sqrt{n})}{4}\right\}$.

Order of the Roots of Unity

Lemma

If $K=\mathbb{Q}(\sqrt{m},\sqrt{n})$, then the roots of unity in K have order 2, 4, 6, 8 or 12.

- Suppose K contains the r-th roots of unity.

  Then $\mu_r \subseteq K$. So $\mathbb{Q}(\mu_r) \subseteq K$.

  Then we must have $[\mathbb{Q}(\mu_r):\mathbb{Q}] \leq 4$.

  However, we will see that $[\mathbb{Q}(\mu_r):\mathbb{Q}] = \phi(r)$.

  So r must satisfy $\phi(r) \leq 4$.

  Suppose $r=\prod_{p|r} p^{r_p}$. Then, $\phi(r)=\prod_{p|r} p^{r_p-1}(p-1)$.

  We conclude that:
  - No prime $p \geq 7$ can divide n (otherwise $p-1 \geq 6$ would divide $\phi(r)$);
  - $5^2 \nmid r$, $3^2 \nmid r$ and $2^4 \nmid r$.

Order of the Roots of Unity (Cont'd)

- This leads to a small list of possibilities for r.

  We find that $r = 1, 2, 3, 4, 5, 6, 8, 10$ or 12.

  Of course, $-1 \in K$.

  So we always have square roots.

  So r will be even.

  $K = \mathbb{Q}(\mu_{10})$ is ruled out as it is not biquadratic.

  On the one hand, it contains $\mathbb{Q}(\sqrt{5})$.

  On the other, there is no other integer d, with $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\mu_{10})$.

  So $\mathbb{Q}(\mu_{10})$ cannot be written $\mathbb{Q}(\sqrt{5}, \sqrt{n})$ for any n.

  This just leaves the list in the statement.

Remarks on Roots of Unity in the Real Case

- The only possibility with $r = 12$ is $\mathbb{Q}(\mu_{12}) = \mathbb{Q}(\mu_4, \mu_6) = \mathbb{Q}(i, \sqrt{-3})$.
- The only possibility with $r = 8$ is $\mathbb{Q}(\mu_8) = \mathbb{Q}(i, \sqrt{2})$.
- If both $m > 0$ and $n > 0$, then also $k > 0$.
- So every embedding of $\sqrt{m}, \sqrt{n}$ and $\sqrt{k}$ is real.
- We shall refer to this case as a **real biquadratic field**.
- Now the only real roots of unity are ± 1.
- So, by Dirichlet's Unit Theorem, there are three units, ϵ_1, ϵ_2 and ϵ_3, such that every unit can be written in the form

$$\pm \epsilon_1^{a_1} \epsilon_2^{a_2} \epsilon_3^{a_3},$$

where a_1, a_2 and a_3 are in $\mathbb{Z}$.
- The fundamental units ϵ_i are, in general, difficult to compute.

Remarks on Roots of Unity in the Imaginary Case

- If $m < 0$, say, then each embedding maps $\sqrt{m}$ to $\pm\sqrt{m}$, not a real.
- So all the embeddings are complex.
- Moreover, they occur in two complex conjugate pairs.
- We shall refer to this case as an **imaginary biquadratic field**.
- By Dirichlet's Unit Theorem, there is a single unit ϵ such that every unit can be written as $\zeta\epsilon^a$, where ζ is a root of unity in K, and $a \in \mathbb{Z}$.
- In this case, the computation of the fundamental unit ϵ is more tractable.

Subsection 5

Cubic Fields

Cubic Fields

- A cubic field is a degree 3 extension of $\mathbb{Q}$.
- It can therefore be defined as

$$K = \mathbb{Q}(\gamma),$$

where γ is a root of an irreducible cubic equation $f(X) \in \mathbb{Q}[X]$.
- Let $\gamma_1 = \gamma$, γ_2 and γ_3 denote the three complex roots of $f(X)$.
- The three embeddings from K into $\mathbb{C}$ are given by sending γ to each of the three roots,

$$\begin{array}{rcl} \tau_i : \mathbb{Q}(\gamma) & \to & \mathbb{C}; \\ \sum_k a_k \gamma^k & \mapsto & \sum_k a_k \gamma_i^k. \end{array}$$

Image of the Embeddings

- A new phenomenon in the cubic case is that the image of the embeddings may differ from K.
- Indeed, the image of the embedding τ_i is $\mathbb{Q}(\gamma_i)$.
- It may happen that $\gamma_i \notin \mathbb{Q}(\gamma)$.

  Example: Suppose that

  $$f(X) = X^3 - 2.$$

  Then $K = \mathbb{Q}(\sqrt[3]{2})$.

  Set $\omega = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$.

  The other roots of $f(X)$ are $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$.

  They do not belong to K.

Splitting Field

- Consider again an irreducible cubic polynomial $f(X) \in \mathbb{Q}[X]$.
- The **splitting field** L of $f(X)$ is the field generated over $\mathbb{Q}$ by all of the roots of $f(X)$,

$$L = \mathbb{Q}(\gamma_1, \gamma_2, \gamma_3).$$

- Notice that

$$\begin{array}{rcl} \gamma_3 & = & \omega^2 \sqrt[3]{2} \\ & = & \frac{1}{2}(\omega \sqrt[3]{2})^2 (\sqrt[3]{2})^2 \\ & = & \frac{1}{2}\gamma_1^2 \gamma_2^2 \\ & \in & \mathbb{Q}(\gamma_1, \gamma_2). \end{array}$$

- So $L = \mathbb{Q}(\gamma_1, \gamma_2)$.

Degree of Splitting Field

Lemma

If L is the splitting field of an irreducible cubic equation $f(X)$, then

$$[L:\mathbb{Q}] = 3 \text{ or } 6.$$

- Certainly L contains γ_1. So $L \supseteq \mathbb{Q}(\gamma_1)$.
  As the minimal polynomial of γ_1 is a cubic, $[\mathbb{Q}(\gamma_1):\mathbb{Q}] = 3$.
  Over $\mathbb{Q}(\gamma_1)$, the cubic $f(X)$ must factor as

  $$f(X) = (X - \gamma_1) f_1(X),$$

  where $f_1(X) \in \mathbb{Q}(\gamma_1)[X]$ is a quadratic with roots γ_2 and γ_3.
  - Suppose $\gamma_2 \in \mathbb{Q}(\gamma_1)$. Then so is γ_3. So $L = \mathbb{Q}(\gamma_1)$, of degree 3.
  - Suppose $\gamma_2 \notin \mathbb{Q}(\gamma_1)$.
    γ_2 and γ_3 are roots of an irreducible quadratic $f_1(X)$ over $\mathbb{Q}(\gamma_1)$.
    So $[\mathbb{Q}(\gamma_1, \gamma_2) : \mathbb{Q}(\gamma_1)] = 2$.
    The tower law for degrees of field extensions now gives $[L:\mathbb{Q}] = 6$.

Roots of the Cubic Equation

- The cubic equation might have three real roots.
- In this case, each of the embeddings τ_i are real.
- By Dirichlet's Unit Theorem, the units are of the form

$$\pm\eta_1^{a_1}\eta_2^{a_2},$$

where:
    - η_1 and η_2 are fundamental units;
    - a_1 and a_2 run through integers.

Roots of the Cubic Equation (Cont'd)

- Alternatively, the cubic might have one real root, and one complex conjugate pair of roots.
- Then there is one real embedding, and one conjugate pair of complex embeddings.
- By Dirichlet's Unit Theorem, the units are of the form

$$\zeta \eta^a,$$

  where:
  - ζ is a root of unity in K;
  - η is a fundamental unit;
  - $a \in \mathbb{Z}$.

Example

- The most natural family of cubics to consider are those of the form

$$\mathbb{Q}(\sqrt[3]{a}),$$

where a is an integer not divisible by a cube.
The minimal polynomial of $\sqrt[3]{a}$ is

$$X^3 - a.$$

Letting $\omega = e^{2\pi i/3}$, the three roots of this are

$$\sqrt[3]{a}, \quad \omega\sqrt[3]{a}, \quad \omega^2\sqrt[3]{a}.$$

Note that

$$\omega^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2} = -\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) - 1 = -\omega - 1.$$

We therefore have one real root, and one complex conjugate pair.

Rings of Integers of Cubic Fields

Theorem

Suppose that $K = \mathbb{Q}(\sqrt[3]{m})$, where $m = m_1 m_2^2$, with m_1 and m_2 coprime and squarefree. Write $m' = m_1^2 m_2$.

- Then if $m^2 \not\equiv 1 \pmod 9$, the ring of integers has integral basis
$$\left\{1, \sqrt[3]{m}, \sqrt[3]{m'}\right\},$$
and K has discriminant $-27 m_1^2 m_2^2$.
- If $m^2 \equiv 1 \pmod 9$, the ring of integers has integral basis
$$\left\{1, \sqrt[3]{m}, \frac{m_2 \pm m_2 \sqrt[3]{m} + \sqrt[3]{m'}}{3}\right\},$$
and K has discriminant $-3 m_1^2 m_2^2$.