INTERNATIONAL ATOMIC ENERGY AGENCY
UNITED NATIONS EDUCATICNAL, SCIENTIFIC AND CULTURAL ORGANIZATION
INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS
I.C.T.P., P.O. BOX 586, 34100 TRIESTE, ITALY, CABLE: CENTRATOM TRIESTE

SMR.637/37

ADVANCED WORKSHOP ON ARITHMETIC ALGEBRAIC GEOMETRY

(31 August - 11 September 1992)

Calculation of a class group

R. Schoof
Dipartimento di Matematica
Università degli Studi di Trento
I-38050 Povo (Trento)
Italy

These are preliminary lecture notes, intended only for distribution to participants

Calculation of a class group

René Schoof

Dipartimento di Matematica
Università degli Studi di Trento
I-38050 Povo (Trento) ITALY
Email: schoof@itnvax.cineca.it

In this note we illustrate the theory of algebraic number fields by means of an explicit example.

Let $g(T) \in \mathbf{Z}[T]$ be the polynomial

$$g(T) = T^3 + T^2 + 5T - 16.$$

It is easily checked that g has no zeroes in $\mathbf{Z}$. By Gauß's lemma it is therefore irreducible in $\mathbf{Q}[T]$. Let F be the field $\mathbf{Q}[T]/(g(T))$ or, equivalently, let $F = \mathbf{Q}(\alpha)$ where α denotes a zero of $g(T)$. We will calculate the ideal class group of the ring of integers of F.

As we will see below, most of our information about the arithmetic of F will be deduced from the values of g at the first few small integers. Therefore we begin our calculation by computing a table of the values $g(k)$ at the integers k with $-10 \le k \le 9$. The contents of the last column will be explained below.

Table I.

	k	$g(k)$	$(\alpha - k)$
(i)	0	-2^4	$\mathfrak{p}_2^4$
(ii)	1	-3^2	${\mathfrak{p}'_3}^2$
(iii)	2	$2 \cdot 3$	$\mathfrak{p}_2\mathfrak{p}_3$
(iv)	3	$5 \cdot 7$	$\mathfrak{p}_5\mathfrak{p}'_7$
(v)	4	$2^2 \cdot 3 \cdot 7$	$\mathfrak{p}_2^2\mathfrak{p}'_3\mathfrak{p}''_7$
(vi)	5	$3 \cdot 53$	
(vii)	6	$2 \cdot 7 \cdot 19$	$\mathfrak{p}_2\mathfrak{p}_7\mathfrak{p}_{19}$
(viii)	7	$3 \cdot 137$	
(ix)	8	$2^3 \cdot 3 \cdot 5^2$	$\mathfrak{p}_2^3\mathfrak{p}_3{\mathfrak{p}_5}^2$
(x)	9	839	

	k	$g(k)$	$(\alpha - k)$
(xi)	-1	$-3 \cdot 7$	$\mathfrak{p}_3\mathfrak{p}_7$
(xii)	-2	$-2 \cdot 3 \cdot 5$	$\mathfrak{p}_2\mathfrak{p}'_3\mathfrak{p}_5$
(xiii)	-3	-7^2	${\mathfrak{p}''_7}^2$
(xiv)	-4	$-2^2 \cdot 3 \cdot 7$	$\mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}'_7$
(xv)	-5	$-3 \cdot 47$	
(xvi)	-6	$-2 \cdot 113$	
(xvii)	-7	$-3 \cdot 5 \cdot 23$	$\mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_{23}$
(xviii)	-8	$-2^3 \cdot 3^2 \cdot 7$	$\mathfrak{p}_2^3{\mathfrak{p}'_3}^2\mathfrak{p}_7$
(xix)	-9	-709	
(xx)	-10	$-2 \cdot 3 \cdot 7 \cdot 23$	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}''_7\mathfrak{p}'_{23}$

For instance, the fact that none of the values $g(0), g(1), g(2), \ldots, g(10)$ is divisible by 11 implies that g has no zeroes modulo 11. Therefore it is irreducible in $\mathbf{F}_{11}[T]$ and we have another proof that g is irreducible in $\mathbf{Q}[T]$.

To evaluate the *discriminant* of $g(T)$, we compute the sums p_i of the ith powers of its roots. Using Newton's relations, these can be expressed in terms of the symmetric polynomials $s_1 = -1$, $s_2 = 5$ and $s_3 = 16$ in the roots of $g(T)$. We have

$$\begin{aligned}
p_0 &= 3,\\
p_1 &= s_1 = -1,\\
p_2 &= -2s_2 + p_1 s_1 = -2 \cdot 5 + (-1) \cdot (-1) = -9,\\
p_3 &= 3s_3 + p_2 s_1 - p_1 s_2 = 3 \cdot 16 + (-9) \cdot (-1) - (-1) \cdot 5 = 62,\\
p_4 &= -4s_4 + p_3 s_1 - p_2 s_2 + p_1 s_3 = -4 \cdot 0 + 62 \cdot (-1) - (-9) \cdot 5 + (-1) \cdot 16 = -33.
\end{aligned}$$

This gives us

$$\det \begin{pmatrix} 3 & -1 & -9 \\ -1 & -9 & 62 \\ -9 & 62 & -33 \end{pmatrix} = -8763 = -3 \cdot 23 \cdot 127$$

Since 8763 is squarefree, the discriminant Δ_F is equal to -8763, and the ring of integers O_F is equal to $\mathbf{Z}[\alpha]$. It is easily verified that the polynomial $g(T)$ has precisely one zero in $\mathbf{R}$. Therefore $r_1 = 1$ and $r_2 = 1$ as well. We conclude that Minkowski's constant is equal to

$$\frac{3!}{3^3}\frac{4}{\pi}\sqrt{8763} = 26.4864\ldots$$

This implies that the class group of O_F is generated by the classes of the prime ideals of norm less than 26. The prime ideals of O_F all occur in the factorization of the principal ideals (p) of O_F, where p is an ordinary prime number. By means of the following proposition we can explicitly calculate these prime ideals.

Proposition. *Let $g(T) \in \mathbf{Z}[T]$ be an irreducible monic polynomial, let α be a zero of g and let $F = \mathbf{Q}(\alpha)$. Suppose that $\mathbf{Z}[\alpha]$ is the ring of integers of F. Then*

$$(p) = \prod_{i=1}^{t} \mathfrak{p}_i$$

where $\mathfrak{p}_i = (p, \varphi_i(\alpha))$ is a prime ideal of O_F and the $\varphi_1(T), \ldots, \varphi_t(T)$ are the irreducible factors of $g(T)$ in the ring $\mathbf{F}_p[T]$.

Proof. Since

$$O_F/\mathfrak{p}_i = \mathbf{Z}[\alpha]/(p, \varphi_i(\alpha)) \cong \mathbf{F}_p[T]/(\varphi_i(T))$$

is a field, we see that the ideals $\mathfrak{p}_i$ are indeed all prime ideals. It is easy to see that

$$\prod_{i=1}^{t}(p, \varphi_i(\alpha)) \subset (p).$$

Since the norms of both sides are equal, we conclude that the ideals are equal. This completes the proof of the proposition.

With the aid of the values of the polynomial $g(T)$ at the first few integers, given in table I above, we easily find the zeroes of g modulo p. This gives us the factorization of $g(T)$ modulo p. Using the proposition it is then easy to obtain the factorizations of the ideals (p) in the ring O_F:

Table II.

p	(p)	
2	$\mathfrak{p}_2\mathfrak{p}_4$	$\mathfrak{p}_2 = (\alpha, 2)$ and $\mathfrak{p}_4 = (\alpha^2 + \alpha + 1, 2)$
3	$\mathfrak{p}_3^2\mathfrak{p}_3'$	$\mathfrak{p}_3 = (\alpha + 1, 3)$ and $\mathfrak{p}_3' = (\alpha - 1, 3)$
5	$\mathfrak{p}_5\mathfrak{p}_{25}$	$\mathfrak{p}_5 = (\alpha + 2, 5)$ and $\mathfrak{p}_{25} = (\alpha^2 - \alpha + 2, 5)$
7	$\mathfrak{p}_7\mathfrak{p}_7'\mathfrak{p}_7''$	$\mathfrak{p}_7 = (\alpha + 1, 7)$, $\mathfrak{p}_7' = (\alpha - 3, 7)$ and $\mathfrak{p}_7'' = (\alpha + 3, 7)$
11	(11)	
13	(13)	
17	(17)	
19	$\mathfrak{p}_{19}\mathfrak{p}_{361}$	$\mathfrak{p}_{19} = (\alpha - 6, 19)$
23	$\mathfrak{p}_{23}^2\mathfrak{p}_{23}'$	$\mathfrak{p}_{23} = (\alpha + 7, 23)$ and $\mathfrak{p}_{23}' = (\alpha + 10, 23)$

Now we explain the contents of the third column of Table I. For $k \in \mathbf{Z}$ one has that $g(k) = N(k-\alpha)$ and hence that $|g(k)|$ is the norm of the principal ideal $(k-\alpha)$. Using these norms and the explicit descriptions of the prime ideals of O_F, given in Table II, it is easy to find the factorization of the principal ideals $(k-\alpha)$.

For instance, since $g(4) = 84 = 2^2 \cdot 3 \cdot 7$, the principal ideal $(\alpha - 4)$ is only divisible by prime ideals with norm a power of 2 or 3 or 7. It remains to decide *which* prime ideals actually occur. Since, by Table II, we have $\alpha - 4 \in \mathfrak{p}_2$ but $\alpha - 4 \notin \mathfrak{p}_4$ we see that $\mathfrak{p}_2$ divides $\alpha - 4$, but $\mathfrak{p}_4$ does not. Similarly, $\mathfrak{p}_3$ does not divide $\alpha - 4$, but $\mathfrak{p}_3'$ does. Finally, the only prime of norm 7 that contains $\alpha - 4$ is $\mathfrak{p}_7''$. We conclude that the factorization of $(\alpha - 4)$ is given by

$$(\alpha - 4) = \mathfrak{p}_2^2 \mathfrak{p}_3' \mathfrak{p}_7''.$$

As we have seen above, the class group is generated by the classes of the prime ideals of norm less than 26. Using the relations that are implied by the factorizations of the principal ideals $(\alpha - k)$, we can reduce the number of generators of the class group. For example, entry (xx) tells us that

$$\mathfrak{p}_{23}' \sim (\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_7'')^{-1},$$

i.e the ideals $\mathfrak{p}_{23}'$ and $(\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_7'')^{-1}$ belong to the same ideal class. This implies that the class of $\mathfrak{p}_{23}'$ is in the group generated by the classes of $\mathfrak{p}_2$, $\mathfrak{p}_3$, and $\mathfrak{p}_7''$. Similarly, entry (xvii) says that

$$\mathfrak{p}_{23} \sim (\mathfrak{p}_3\mathfrak{p}_5)^{-1}.$$

We conclude that the class group is already generated by the classes of the prime ideals dividing the primes $p \leq 19$. Continuing in this way, we can eliminate many of the generators, each time expressing the class of a prime ideal as a product of classes of primes of smaller norm.

By entry (vi), we eliminate $\mathfrak{p}_{19}$; by means of the entries (iii), (iv) and (xi) we eliminate the primes over 7. Entry (xii) implies that $\mathfrak{p}_5$ can be missed as a generator. Since $\mathfrak{p}_{25} \sim \mathfrak{p}_5^{-1}$, we see that $\mathfrak{p}_{25}$ can be missed as well. The prime $\mathfrak{p}_3$ is taken care of by the relation implied by entry (ii). Since $\mathfrak{p}_3' \sim \mathfrak{p}_3^{-2}$ we don't need the prime $\mathfrak{p}_3'$ either. Finally $\mathfrak{p}_4 \sim \mathfrak{p}_2^{-1}$.

We conclude that the class group of O_F is generated by the class of the prime $\mathfrak{p}_2$. Entry (i) implies that

$$\mathfrak{p}_2^4 \sim (1).$$

This shows that the class group is a quotient of $\mathbf{Z}/4\mathbf{Z}$.

Further attempts turn out not to give any new relations This leads us to believe that the class group is perhaps isomorphic to $\mathbf{Z}/4\mathbf{Z}$. To *prove* this, it suffices to show that the ideal $\mathfrak{p}_2^2$ is not principal. Since, by entry (ii) we have that $\mathfrak{p}_3' \sim \mathfrak{p}_3^{-2} \sim \mathfrak{p}_2^2$, this is equivalent to showing that the ideal $\mathfrak{p}_3'$ is not principal.

Suppose $\mathfrak{p}_3' = (\gamma)$ for some $\gamma \in O_F$. By entry (ii) of Table I, we would have that $(\gamma)^2 = (\alpha - 1)$. Therefore

$$\gamma^2 \cdot u = \alpha - 1 \qquad \text{for some unit } u \in O_F^*.$$

In order to show that this cannot happen, we need to know the unit group O_F^*, or, at least, the units modulo squares. By Dirichlet's Unit Theorem, the unit group has rank 1. Since F admits an embedding into $\mathbf{R}$, the only roots of unity in F are ±1. Therefore

$$O_F^* = \{\pm\varepsilon^k : k \in \mathbf{Z}\}$$

for some unit $\varepsilon \in O_F^*$.

To find a unit different form ± 1, we exploit the *redundancy* in the relations implied by Table I. Consider the principal ideals generated by $(\alpha - 1)(\alpha - 2)^4$ and 9α. Entries (i), (ii) and (iii) of the table imply that both these ideals factor as

$$\mathfrak{p}_2^4 \mathfrak{p}_3^4 \mathfrak{p}_3'^2 .$$

Therefore $((\alpha - 1)(\alpha - 2)^4) = (9\alpha)$ and

$$\varepsilon = \frac{(\alpha - 1)(\alpha - 2)^4}{9\alpha} = 4\alpha^2 + \alpha - 13.$$

is a unit. In fact, its multiplicative inverse is equal to $129\alpha^2 + 346\alpha + 1227$, but we won't use this fact.

Consider the images of ε and -1 under the following homomorphism:

$$\begin{array}{ccccc} O_F^*/(O_F^*)^2 & \longrightarrow & (O_F/\mathfrak{p}_3)^* \times (O_F/\mathfrak{p}_7)^*/((O_F/\mathfrak{p}_7)^*)^2 & \cong & \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \\ \varepsilon & \mapsto & (-1, 4) & \mapsto & (1, 0) \\ -1 & \mapsto & (-1, -1) & \mapsto & (1, 1) \end{array}$$

Since the vectors $\binom{1}{0}$ and $\binom{1}{1}$ are independent, we conclude that ε and -1 generate the unit group O_F^* modulo squares.

Therefore the unit u is, modulo squares, of the form

$$u = \pm \varepsilon^k$$

for some $k \in \mathbf{Z}$. The equation satisfied by α now becomes

$$\pm \varepsilon^k \cdot \gamma^2 = \alpha - 1 \qquad \text{for some } \gamma \in O_F \text{ and } k \in \mathbf{Z}.$$

Consider this equation modulo $\mathfrak{p}_5$. More precisely consider the image in the following group of order 2:

$$(O_F^*/\mathfrak{p}_5)^*/((O_F^*/\mathfrak{p}_5)^*)^2.$$

Since -1 is a square mod 5 and since $\varepsilon \equiv 4 \cdot (-2)^2 - 2 - 13 \equiv 1$ is square modulo $\mathfrak{p}_5$ as well, the left hand side of this equation is trivial. The right hand side, however, is congruent to $-2 - 1 \equiv 2$ which is *not* a square.

We conclude that the equation has no solutions and hence that the ideal class group is cyclic of order 4.

Bibliography

[1] Lenstra, H.W.: *Elementaire algebraïsche getaltheorie*, Syllabus, Univ. van Amsterdam 1982.

[2] Ono, T.: *An introduction to algebraic number theory*, Plenum Press, New York 1990.

[3] Samuel, P.: *Théorie algebrique des nombres*, Hermann, Paris 1971.

[4] Stewart, I.N. and Tall, D.O.: *Algebraic number theory*, Chapman and Hall, London 1987.