

1. MOTIVATION

Let K be a number field. The class group $\text{Cl}(K)$ of K is a finite group, and the proof gives a concrete set of generators: the classes $[\mathfrak{p}]$ of the prime ideals \mathfrak{p} of \mathcal{O}_K lying over rational primes p not exceeding the “Minkowski constant” λ_K . In general there are a lot of relations among such prime ideals, and so to compute the class group one needs a method to find the relations. There is no universal procedure for doing so, and especially to prove that certain prime ideals are *not* principal can require some real technique, but one useful way to at least cut down the possibilities is to use norms to find some nontrivial relations among various prime ideals.

The basic idea is this: if $x \in \mathcal{O}_K$ is nonzero then $n = N_{K/\mathbf{Q}}(x) \in \mathbf{Z}$ is a nonzero integer, and from the prime factorization of n we can deduce some information about the prime ideal factorization of $x\mathcal{O}_K$. If n has only “small” prime factors and these appear with only “small” multiplicities in the prime factorization of n then we can often restrict the possibilities for the prime factorization $x\mathcal{O}_K = \prod \mathfrak{p}_i^{m_i}$, and this in turn becomes the relation $\prod [\mathfrak{p}_i]^{m_i} = 1$ in the class group $\text{Cl}(K)$. If we succeed in finding enough x with “small” norm then we can get many relations. There are a few other useful tricks to make this strategy work, as we illustrate below, and it is most effective when trying to prove that the class group is trivial. If we eventually get the class group down to a very small size but can’t find some more relations (and so suspect we may have found the class group but it is nontrivial) then there are other methods which can sometimes (e.g., in the quadratic case) tell us the exact size of the class group and thereby confirm that there are no more relations to be found.

2. WORKED EXAMPLE

Let $K = \mathbf{Q}(\alpha)$ with α a root of the 3-Eisenstein polynomial $f(X) = X^3 - 9X - 6 \in \mathbf{Z}[X]$. By calculus we check that f has three real roots, so K is totally real. That is, $r_2 = 0$. This simplifies the computation of the Minkowski constant λ_K , as the term involving π is trivial. Is the order $\mathbf{Z}[\alpha]$ in \mathcal{O}_K equal to the full ring of integers? Since f is 3-Eisenstein, we know that the index $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ is not divisible by 3. Also, one computes that $d(1, \alpha, \alpha^2) = 2^3 \cdot 3^5$, so the only prime that can divide $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ is 2. In other words, $[\mathcal{O}_K : \mathbf{Z}[\alpha]] = 2^m$ for some $m \geq 0$. But then its square 4^m divides $d(1, \alpha, \alpha^2)$, so $m \leq 1$. In other words, either $\mathbf{Z}[\alpha] = \mathcal{O}_K$ or it is an order of index 2 inside of \mathcal{O}_K . Thus, $\text{disc}(K)$ is equal to either $2^3 \cdot 3^5$ or $2 \cdot 3^5$. In particular, 2 and 3 are precisely the ramified primes of K over \mathbf{Q} (or rather, of \mathcal{O}_K over \mathbf{Z}).

From the upper bound on the discriminant we get $\lambda_K = (2/9)\sqrt{|\text{disc}(K)|} \leq 4\sqrt{6} < 10$, so by Minkowski’s Lemma we deduce that the class group of K is generated by the classes $[\mathfrak{p}]$ of the prime ideals \mathfrak{p} lying over the rational primes $p < 10$, which is to say $p \in \{2, 3, 5, 7\}$. We now seek to do two things: deduce information about the prime ideal factorization of $p\mathcal{O}_K$ for such small p , and to find nonzero elements $x \in \mathcal{O}_K$ (in fact, in $\mathbf{Z}[\alpha]$) such that $N_{K/\mathbf{Q}}(x) \in \mathbf{Z} - \{0\}$ has only such small prime factors (and with low multiplicity, preferably 1).

To get started, we see from the constant term of the cubic f that $N_{K/\mathbf{Q}}(\alpha) = 6$, so $(\alpha) = \mathfrak{p}_2\mathfrak{p}_3$ for some prime ideals \mathfrak{p}_2 and \mathfrak{p}_3 lying over 2 and 3 respectively. We will now find more such principal ideal relations by calculating $N_{K/\mathbf{Q}}(\alpha + r)$ for some small nonzero $r \in \mathbf{Z}$ (i.e., this is the negative $-f(-r)$ of the constant term of $f(X - r)$) and hope for the best (with some luck and cleverness). A basic strategy is to hope that a prime q admits a prime \mathfrak{q} over it with residue field \mathbf{F}_q , for then $\alpha + r$ will vanish mod \mathfrak{q} for some $0 \leq r < q$, which is to say that $N_{K/\mathbf{Q}}(\alpha + r)$ would be divisible by q for some such r . For example, for $q = 5$ we would try to compute $N_{K/\mathbf{Q}}(\alpha + r)$ for $-2 \leq r \leq 2$ and hope that one of these is divisible by 5. If we get 5-divisibility more than once, then the corresponding prime ideal factors over 5 cannot be the same (as they are dividing numbers $\alpha + r$ and $\alpha + s$ whose difference $r - s$ is a unit mod 5). On the other hand, if no such 5-divisibility occurs for $0 \leq r < 5$ then \mathbf{F}_5 cannot arise as a residue field and so *all* primes over 5 must have residue field degree > 1 , which can also be useful information when trying to figure out how many primes there are over 5!

To carry out this strategy, we first compute $N_{K/\mathbf{Q}}(\alpha - 1) = 14$ and $N_{K/\mathbf{Q}}(\alpha + 1) = 2$. Hence, $(\alpha + 1) = \mathfrak{p}'_2$ is a prime over 2, and it is distinct from the prime \mathfrak{p}_2 over 2 that divides (α) since (α) and $(\alpha + 1)$ cannot share a common prime factor (as together they generate the unit ideal). Note also that since $\alpha + 1$ and $\alpha - 1$ differ by 2, we also have $\alpha - 1 \in \mathfrak{p}'_2$. Since 2 is ramified in K and $[K : \mathbf{Q}] = 3$, we must have either $(2) = \mathfrak{p}'_2 \mathfrak{p}_2$ or $(2) = \mathfrak{p}_2 (\mathfrak{p}'_2)^2$. But which one happens? More advanced techniques give the “right” way to figure this out, but here we use a trick inspired by the advanced viewpoint (which I am not explaining) to show that it is the second option that occurs. The element $\alpha - 1$ has minimal polynomial $f(X + 1) = X^3 + 3X^2 - 6X - 14 = X^3 + 3X^2 - 2(3X - 7)$, and so by working modulo $(\alpha - 1)^2$ the vanishing of $f(X + 1)$ at $X = \alpha - 1$ gives that $2(3(\alpha - 1) - 7) \equiv 0 \pmod{(\mathfrak{p}'_2)^2}$. But $3(\alpha - 1) - 7$ is a unit modulo \mathfrak{p}'_2 , so $2 \equiv 0 \pmod{(\mathfrak{p}'_2)^2}$. This shows that $(\mathfrak{p}'_2)^2$ appears in the prime factorization of (2) , so indeed $(2) = \mathfrak{p}_2 (\mathfrak{p}'_2)^2$. But \mathfrak{p}'_2 is principal (it equals $(\alpha + 1)$), so therefore the prime factorization of (2) shows that \mathfrak{p}_2 is principal. We also have that $\mathfrak{p}_2 \mathfrak{p}_3 = (\alpha)$ is principal, so \mathfrak{p}_3 is principal as well. This is the only prime ideal over 3. Indeed, although a rational prime that is ramified in a cubic field (such as 3 in K) may have two prime ideal factors over it in general (but not more than two), in our case there really is just one such prime ideal: since $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ divides 2 we have the equality $\mathbf{Z}[\alpha]_{(3)} = (\mathcal{O}_K)_{(3)}$ after localizing at $3\mathbf{Z}$ and so passing to the quotient modulo $3\mathbf{Z}$ gives $\mathcal{O}_K/(3) = \mathbf{Z}[\alpha]/(3) \simeq \mathbf{F}_3[X]/(f) = \mathbf{F}_3[X]/(X^3)$ since f is 3-Eisenstein. This ring has just one maximal ideal, so \mathcal{O}_K has only one prime ideal over 3 (and we have seen that it is principal).

Continuing with the norm calculations, we find $N_{K/\mathbf{Q}}(\alpha + 2) = -f(-2) = -4$ and $N_{K/\mathbf{Q}}(\alpha - 2) = -f(2) = 16$. Since $\alpha + r$ for $-2 \leq r \leq 2$ never has a prime factor over 5, we conclude that *all* primes \mathfrak{p} over 5 satisfy $f(\mathfrak{p}|5) \geq 2$. But $3 = \sum e_i f_i$, so there is no room for two such primes, so in fact there is a single such \mathfrak{p}_5 . That is, $(5) = \mathfrak{p}_5^e$ for some $e \geq 1$, and in fact $e = 1$ since 5 is unramified (so the residue field is \mathbf{F}_{5^3}). In particular, $\mathfrak{p}_5 = (5)$ is principal.

It remains to consider primes over 7. Recall that we have found one such prime \mathfrak{p}_7 in the factorization of $(\alpha - 1)$. We now compute some more norms: $N_{K/\mathbf{Q}}(\alpha + 3) = 6$ and $N_{K/\mathbf{Q}}(\alpha - 3) = 6$. Thus, for $-3 \leq r \leq 3$, $N_{K/\mathbf{Q}}(\alpha + r)$ is divisible by 7 only for $r = -1$, so \mathfrak{p}_7 is the *only* prime over 7 with residue field \mathbf{F}_7 (i.e., all other primes have residue field degree ≥ 2 over \mathbf{F}_7). Since 7 is unramified, we conclude that $(7) = \mathfrak{p}_7 \mathfrak{p}'_7$ with $f(\mathfrak{p}'_7|7) = 2$. But $(\alpha - 1) = \mathfrak{p}_2 \mathfrak{p}_7$ with \mathfrak{p}_2 shown to be principal, so \mathfrak{p}_7 is also principal. Then the equality $(7) = \mathfrak{p}_7 \mathfrak{p}'_7$ forces \mathfrak{p}'_7 to be principal as well.

We have shown that for all primes $p < 10$, every prime ideal \mathfrak{p} over p in K is principal, so K has trivial class group.

Remark 2.1. A classical observation of Euler was that for the odd prime $p = 41$, the values of $x^2 + x + p$ are prime for integers $0 \leq x \leq p - 2$. (This is “best possible” since for $n = p - 1$ this is $(p - 1)^2 + (p - 1) + p = p^2$.) Note that for the negative integer $d_p = 1 - 4p \equiv 1 \pmod{4}$ this is the minimal polynomial of the generator $\alpha = (-1 + \sqrt{d})/2$ of the ring of integers of $K = \mathbf{Q}(\sqrt{d_p})$ when d_p is squarefree (as it is for $p = 41$, with $d_p = -163$). The same happens for $p = 17, 11, 5, 3$, and curiously the imaginary quadratic field $\mathbf{Q}(\sqrt{d_p})$ has class number 1 in all of these cases (with $d_p = -163, -67, -43, -19, -11$).

This is not a coincidence! It is a general fact when $d_p = 1 - 4p$ is squarefree that $x^2 + x + p$ has prime values for all integers $0 \leq x \leq p - 2$ if and only if $\mathbf{Q}(\sqrt{d_p})$ has class number 1. This is proved by a conceptual argument based on our knowledge about prime splitting behavior in quadratic fields and the norms of prime ideals in the split and ramified cases: see Theorem 6 on page 156 of Chapter IX of Harvey Cohn’s somewhat idiosyncratic book *Advanced Number Theory* (where \mathbf{Q} is denoted as R , for example), where the proof relies on some earlier results in the book that (up to differences in notation) have all been treated in this course.

Much deeper lies the fact that $p = 41$ is the last such prime: there are only finitely many imaginary quadratic fields with class number 1 and $\mathbf{Q}(\sqrt{-163})$ is the last one. This is an instance of Gauss’ “class number” problem for quadratic fields (which Gauss expressed in the language of binary quadratic forms, since the language of rings and ideals did not exist at the time); you can read about it on Wikipedia.