Lecture 2-21: Factorization of ideals in number fields

February 21, 2025

Continuing from last time, I prove existence and uniqueness of prime factorizations for ideals rather than elements in rings of integers. Let $R = \mathcal{O}_K$ be such a ring.

The key step in putting a group structure on the set of nonzero ideals of R is the following one, in which I use the integral closedness of R for the first time.

Proposition 4.6, p. 23

If $I \subset R$ is a nonzero ideal then there is a nonzero ideal J of R such that $IJ = (\alpha)$ is principal.

Proof.

Let $\alpha \in I$ and let $J = \{\beta \in R : \beta I \subset (\alpha)$. Clearly J is an ideal with $IJ \subset \alpha$; i will show that in fact $IJ = (\alpha)$. Letting $L = \frac{1}{\alpha} IJ$, I must show that $L = R$. If not then by Lemma 4.5 last time there is $\gamma \in K, \gamma \notin R$ with $\gamma L \subset R$. Then $\gamma IJ = \gamma \alpha L \subset (\alpha)$, whence $\gamma J \cap R \subset J$. But we also have $(\alpha) \subset I$, whence $J \subset L$, whence $\gamma J \subset \gamma L \subset R$. Thus $\gamma J \subset J$. Since I observed last time that J is free over $\mathbb{Z}$ of finite rank, it follows from the Cayley-Hamilton Theorem that γ is a root of a monic polynomial over $\mathbb{Z}$ so lies in R, a contradiction. □

As a consequence, we can cancel nonzero ideals: if I, J, J' are nonzero ideals of R and $IJ = IJ'$, then $J = J'$. Indeed, choosing I' with $II' = (\alpha)$ principal, we see that $IJ = IJ'$ implies $\alpha J = \alpha J'$ and then $J = J'$.

Corollary 4.8, p. 12

If I and J are ideals of R with $I \supset J$, then there is an ideal L with $IL = J$.

If $I \supset J$, then choose a nonzero ideal I' with $II' = (\alpha)$ principal. Then $L = \frac{1}{\alpha} JI' \subset R$ is an ideal and $IL = J$, as desired. We write $I|J$ and say that I divides J in this situation; thus $I \supset J$ if and only if $I|J$.

I can now prove the ideal factorization theorem.

Theorem 4.9, p. 12

Any nonzero ideal I is a product $P_1 \dots P_r$ of nonzero prime ideals P_i; this product is unique up to reordering the factors.

Proof.

As before, assume not and let I be a counterexample of minimal norm, which cannot be prime. Choose a prime ideal P with $P \supset I$; then we can write $I = PJ$ for some ideal $J \supset I$. If $I = J$ then we can cancel I to get $I = P$, a contradiction; so J properly contains I and must have smaller norm, whence J is a product of prime ideals. Then $I = PJ$ is also such a product, a contradiction. If $I = P_1 \dots P_r = Q_1 \dots Q_s$ with the P_i and Q_j prime, then $P_1 \supset I$, so $P_1 \supset Q_i$ for some i, forcing $P_1 = Q_i$. We can then rearrange terms in the second product and cancel $P_1 = Q_i$ from both products; continuing in this way, we see that $r = s$ and the Q_j are a reordering of the P_i, as claimed; of course neither the Q_j nor the P_i need be distinct here. □

As mentioned above, there is no need to worry about units in this result, unlike the corresponding result about elements of PIDs. I now put a group structure on the set of nonzero ideals; there are two ways to do this. One way is to introduce fractional ideals; that is, R-submodules J of K such that $\alpha J \subset R$ for some nonzero $\alpha \in R$. Then every nonzero ideal I of R has a multiplicative inverse I^{-1} that is a fractional ideal, so that $II^{-1} = R$ (choose J with $IJ = (\alpha)$ and set $I^{-1} = \alpha^{"-1}J$). It is more common and useful, however, to proceed differently, introducing an equivalence relation $\sim$ just on nonzero ideals via $I \sim J$ if there is is $\alpha \in K^*$ with $\alpha I = J$. Multiplication is then well defined on equivalence classes (as it was on equivalence classes for the Brauer group) and every class has a multiplicative inverse. As every fractional ideal is equivalent to an ordinary one, one can also define $\sim$ on fractional ideals if desired. The equivalence class of an ideal (or fractional ideal) I is denoted $[I]$; note that the second group structure, unlike the first one, identifies any two principal ideals.

The abelian group of ideal classes under multiplication is called the class group of R and denoted $\mathrm{Cl}(R)$ or $\mathrm{Cl}(\mathcal{O}_K)$. Its order is called the class number of R (Definition 4.10, p. 13). The class group is the group of nonzero fractional ideals modulo the subgroup of principal ones. Clearly $\mathrm{Cl}(R)$ is trivial if and only if R is a PID. The simplest example where this does *not* hold has $K = \mathbb{Q}[\sqrt{-5}], R = \mathbb{Z}[\sqrt{-5}]$. Here the prime ideal $P = (2, 1 + \sqrt{-5})$ generated by 2 and $1 + \sqrt{-5}$ is not principal, since a generator x of it would have to be a common divisor of 2 and $1 + \sqrt{-5}$ and thus have norm dividing $N(2) = 4$ and $N(1 + \sqrt{-5}) = 6$, respectively, forcing its norm to be 1 or 2. But the only elements of norm 1 ad ± 1 and there are no elements of norm 2, so this is a contradiction. To see that P is prime, observe first that moding R out by (2) gives the ring extension $\mathbb{Z}_2[\sqrt{-5}]$ of $\mathbb{Z}_2$; identifying $\sqrt{-5}$ with 1 (which of course is a square root of -5 modulo 2), one sees that $R/P \cong \mathbb{Z}_2$, whence P is indeed prime (and of norm 2).

In a similar way one shows that $Q = (3, 1 + \sqrt{-5})$ is also nonprincipal and prime in R, as is $Q' = (3, 1 - \sqrt{-5})$. Since R fails to be a PID, it is not surprising that it also fails to be a UFD: the element 6 has two essentially distinct factorizations into primes, namely $2 \cdot 3$ and $(1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. The ideal (6), by contrast, must factor uniquely as a product of prime ideals. This product is $P^2QQ' = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$. More precisely, we have $P^2 = (2)$, $QQ' = (3)$. We say that the prime 2 in $\mathbb{Z}$ ramifies in R, since the ideal it generates is the square of a prime ideal. The prime 3 splits completely in R since the ideal it generates is the product of distinct prime ideals. Finally, the prime 11 in $\mathbb{Z}$ remains prime in R, since if 11 had a nontrivial factor in R it would have to have norm 11, which is impossible. We say that 11 is inert in R, since the ideal it generates is prime. See Definition 5.2 on p. 14. The class number of R turns out to be 2. In general the class number of any $\mathcal{O}_K$ is known to be finite (Theorem 6.13, p. 21).

The class numbers of the rings of integers $R = \mathcal{O}_K$ of quadratic fields $K = \mathbb{Q}[\sqrt{d}]$ where d is a square-free integer exhibit a fascinating behavior. The most familiar case is $d = -1$, where $R = \mathbb{Z}[i]$ is the ring of Gaussian integers, which probably some of you have seen. This ring is well known to be a PID; in fact it is a (norm-)Euclidean domain in the sense that given $a, b \in R$ with $a \neq 0$, one can write $b = qa + r$ for some $q, r \in R$ with $N(r) < N(a)$ (this element r is not unique). The same argument that proves this can be adapted to show that R is also a norm-Euclidean domain for $d < 0$, $d \equiv 1 \bmod 4$, and $|d| < 15$, bearing in mind that $R = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ in these cases. All such R have class number 1.

This pattern breaks when $d = -15$, however; here the class number is 2, as it is when $d = -5$. There is a famous complete list of all square-free $d < 0$ such that $\mathcal{O}_K$ has class number 1, namely $-1, -2, -3, -7, -11, -19, -43, -67, -163$. It is surprisingly elementary (but too much of a digression here) to prove that the class number is indeed 1 in all these cases; it is much harder to prove that the list is complete. In fact, a proof of this was announced in 1952, but not widely accepted at the time; later, in 1967, another proof was given which was accepted. The author of that proof (Harold Stark) later acknowledged, however, that the original 1952 proof (of Karl Heegner) was in fact correct. It is conjectured that there are only finitely many values of $d < 0$ with a given class number for $\mathcal{O}_K$,, but this is still unknown. The fields $\mathbb{Q}[\sqrt{d}]$ for $d < 0$ are called (naturally enough) imaginary number fields.

For positive d, the situation is much less well understood. The fields corresponding to such d are called real quadratic. Here the class number is 1 in many more cases, conceivably infinitely many. It is also possible for $R = \mathcal{O}_K$ to be Euclidean but not norm-Euclidean, so that there is another function d (not the norm function) from R^* to the natural numbers such that for any $a, b \in R$ with $a \neq 0$ there are q, r with $b = qa + r$ and $d(r) < d(a)$. You can get a good sense of why this case is so much harder than the case $d < 0$ by looking at the formula for the norm: $N(a + b\sqrt{d}) = a^2 - db^2$. For $d > 0$ this can be small even if a and b are both large, so that it is harder to understand the set of elements with a fixed norm than it is in the imaginary case. It is known that in all the real cases there is an infinite cyclic group of units in R, consisting of elements of norm 1.

The other most interesting special case is that of the cyclotomic field $K_n = \mathbb{Q}[\epsilon_n]$, where $\epsilon_n = e^{2\pi i/n}$ is a primitive nth root of 1 in $\mathbb{C}$. I will show next time that we have $R_n = \mathcal{O}_{K_n} = \mathbb{Z}[\epsilon_n]$ if n is prime; in fact this holds for all n. What makes this case so interesting is its connection to the famous Fermat equation $x^n + y^n = z^n$, where x, y, z are nonzero integers (that we can assume to be relatively prime) and $n > 2$. Fermat claimed to have proved that there are no solutions to this equation. The proof quickly reduces to the case where $n = p$ is prime (since the case $n = 4$ is elementary).

Passing to the ring of integers R_p, the left side of the equation factors as $(x+y)(x+\epsilon_p y)\dots(x+\epsilon_p^{p-1}y)$, where the relative primeness of x and y forces the factors $x+\epsilon_p^i y$ to be pairwise relatively prime. From here one can (with some work) get a contradiction *if* the class number of R_p is 1, so that unique factorization of elements holds in R_p. (The key observation is that then every factor $x+\epsilon_p^i$ must be a pth power, since their product is the pth power z^p.) Many leading mathematicians in the early 19th century took unique factorization for granted (or in one case thought they had proved it), but in fact this fails for all primes $p \geq 23$.

Kummer was able to prove Fermat's conjecture under the stronger hypothesis that p does not divide the class number of R_p (the case of a so-called regular prime). Much later, in 1995, Wiles and Taylor used much more complicated methods to prove Fermat's conjecture in general.