5 Non-unique factorizations

In this chapter we briefly discuss some aspects of non-unique factorization, ending with an application of quadratic forms (and more generally ideals) to factorization problems in rings of integers.

5.1 Principalization

Let K be a number field. Kummer approach to resolving the non-unique factorization of $\mathcal{O}_K$ was essentially to work in a larger ring of integers R where every (nonzero nonunit) element of $\mathcal{O}_K$ factors uniquely (up to order and units) into irreducibles in R. We can recast this approach in Dedekind's language of ideals with the following notion.

Definition 5.1.1. *We say an finite extension L of K is a* **principalization field** *for K, or* **principalizes** *K, if $\mathcal{I}\mathcal{O}_L$ is a a principal ideal of L for any ideal $\mathcal{I}$ of $\mathcal{O}_K$.*

Some authors instead say K *capitulates* in L.

Proposition 5.1.2. *Suppose L principalizes K. Leta be a nonzero nonunit in $\mathcal{O}_K$ and write $a\mathcal{O}_K = \prod \mathfrak{p}_i$ be the prime ideal factorization of $a\mathcal{O}_K$ in $\mathcal{O}_K$. Write $\mathfrak{p}_i\mathcal{O}_L = (\alpha_i)$ for some $\alpha_i \in \mathcal{O}_L$. If $a = \prod \beta_j$ is any irreducible factorization of a in $\mathcal{O}_K$, then each β_j is, up to a unit of $\mathcal{O}_L$, a subproduct of the α_i's.*

In other words all irreducible factorizations of a in $\mathcal{O}_K$, comes from different groupings of a single (not necessarily irreducible) factorization $a = \prod \alpha_j$ in $\mathcal{O}_L$. E.g., we may have something like

$$a = \underbrace{(\alpha_1 \cdots \alpha_{i_1})}_{\beta_1}\underbrace{(\alpha_{i_1+1} \cdots \alpha_{i_2})}_{\beta_2} \cdots \underbrace{(\alpha_{i_k+1} \cdots \alpha_m)}_{\beta_{k+1}}$$

and any irreducible (or even non-irreducible) factorization of a in $\mathcal{O}_K$, just comes from a regrouping of the α_i's.

Proof. Since L principalizes K, then for each i, we can write $\mathfrak{p}_i\mathcal{O}_L = (\alpha_i)$ for some $\alpha_i \in \mathcal{O}_L$. (It is not necessarily true that each α_i is irreducible.) Hence

$$a\mathcal{O}_L = \prod(\mathfrak{p}_i\mathcal{O}_L) = \prod(\alpha_i).$$

On the other hand,

$$a\mathcal{O}_K = \prod(\beta_j)$$

so each (β_j) is a subproduct of the $\mathfrak{p}_i$'s, say $\beta_j = \mathfrak{p}_{j_1}\mathfrak{p}_{j_2}\cdots\mathfrak{p}_{j_k}$ so $\beta_j = u\alpha_{j_1}\ldots\alpha_{j_k}$ for some unit $u \in \mathcal{O}_L$. □

Example 5.1.3. *Let $K = \mathbb{Q}(\sqrt{-5})$ and $L = \mathbb{Q}(\sqrt{-5}, \sqrt{2})$. To show L principalizes K, it suffices to show $(2, \sqrt{-5})\mathcal{O}_L$ is principal since $(2, \sqrt{-5}) \subseteq \mathcal{O}_K$ generates the class group of K. (Justify to yourself that this is sufficient.) Note that $(2, \sqrt{-5})^2 = (2)$. On the other hand $(2) = (\sqrt{2})^2$ in $\mathcal{O}_L$. Since $(\sqrt{2})$ is prime in $\mathcal{O}_L$, we must have $(\sqrt{2}) = (2, \sqrt{-5})\mathcal{O}_L$ by the unique prime ideal factorization in $\mathcal{O}_L$. Thus L is a principalization field for K.*

Let's see how we can resolve the non-unique factorization

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

in $\mathcal{O}_K$ using principalization. Recall the prime ideal factorization of (6) *in $\mathcal{O}_K$ is*

$$(6) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}).$$

One can check that

$$(2, 1+\sqrt{-5})\mathcal{O}_L = (\sqrt{2})$$

(we did this above) and

$$(3, 1+\sqrt{-5})\mathcal{O}_L = (\frac{\sqrt{2}+\sqrt{-10}}{2})$$

$$(3, 1-\sqrt{-5})\mathcal{O}_L = (\frac{\sqrt{2}-\sqrt{-10}}{2})$$

(we'll discuss this below). The above proposition say the irreducible factorizations of 6 *in $\mathcal{O}_K$ come from different groupings of the factorization*

$$6 = \underbrace{(\sqrt{2}\cdot\sqrt{2})}_{2}\underbrace{(\frac{\sqrt{2}+\sqrt{-10}}{2}\cdot\frac{\sqrt{2}-\sqrt{-10}}{2})}_{3} = \underbrace{(\sqrt{2}\cdot\frac{\sqrt{2}+\sqrt{-10}}{2})}_{1+\sqrt{-5}}\underbrace{(\sqrt{2}\cdot\frac{\sqrt{2}-\sqrt{-10}}{2})}_{1-\sqrt{-5}}.$$

Thus we see principalization provides an alternative viewpoint to the resolution of non-unique factorization in a ring of integers $\mathcal{O}_K$. Furthermore, we will see there are some advantages to using principalization (essentially Kummer's approach) instead of ideal theory (Dedekind's approach) by giving an application of principalization in the next section, even though these two approaches are more or less equivalent by Proposition 5.1.2.

Now of course it is natural to ask when K has a principalization field and how can we find one. It turns out to be quite easy to answer.

Proposition 5.1.4. *Let $\mathcal{I}_1, \ldots, \mathcal{I}_h$ be ideals of $\mathcal{O}_K$ which generate the class group. If e_j is the order of $\mathcal{I}_j$ in $\mathcal{C}l_K$, then we can write $\mathcal{I}_j^{e_j} = (\alpha_j)$ for some $\alpha_j \in \mathcal{O}_K$. Then $L = K(\sqrt[e_1]{\alpha_1}, \ldots, \sqrt[e_h]{\alpha_h})$ is a principalization field for K.*

The proof is immediate.

It is worthwhile to remark that even though passing to $\mathcal{O}_L$ resolves non-unique factorization in $\mathcal{O}_K$ (in the sense of Proposition 5.1.2, it is not necessarily the case that any element of $\mathcal{O}_K$ has a unique irreducible factorization in $\mathcal{O}_L$. In particular, there are examples of number fields K, such that no finite extension L of K has class number 1. This was shown by Golod and Shafarevich in 1964 with the example of $K = \mathbb{Q}(\sqrt{-3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19})$.

One particular principalization field is particularly noteworthy, and is important for studying primes of the form $x^2 + dy^2$.

We say L/K is an **abelian** extension if it is Galois and $\mathrm{Gal}(L/K)$ is abelian. Further, L/K is **unramified** if every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is unramified in L.

Definition 5.1.5. *The* **Hilbert class field** *$HCF(K)$ is the maximal unramified abelian extension of K.*

An important component of *class field theory*, which we hope to discuss in Part III, is the following result.

Theorem 5.1.6. *$H = HCF(K)$ is a well-defined finite extension of K satisfying $\mathrm{Gal}(H/K) = \mathcal{C}l_K$. Further H principalizes K.*

Example 5.1.7. *Let $K = \mathbb{Q}$. Then any nontrivial extension L of K must be ramified (since the $|\Delta_L| > 1$ and any $p|\Delta_L$ ramifies in L), hence there is only one unramifed extension of $\mathbb{Q}$—namely $\mathbb{Q}$ itself. Thus $HCF(\mathbb{Q}) = \mathbb{Q}$.*

More generally if $h_K = 1$, the above theorem tells us $HCF(K) = K$.

Example 5.1.8. *Let $K = \mathbb{Q}(\sqrt{-5})$. If L/K is unramified, then $p|\Delta_L$ implies $p|\Delta_K = -20$. One might be tempted to guess the Hilbert class field of K is $L = \mathbb{Q}(\sqrt{-5}, \sqrt{2})$ from Example 5.1.3. Indeed L/K is abelian with Galois group $\simeq C_2 \simeq \mathcal{C}l_K$, but it is not unramified. The Hilbert class field of K is $\mathbb{Q}(\sqrt{-5}, i)$.*

Exercise 5.1. *Check $HCF(\mathbb{Q}(\sqrt{-5})) = \mathbb{Q}(\sqrt{-5}, i)$ using the definition and the theorem above.*

One use of the Hilbert class field can be seen in the following result ([Cox]).

Theorem 5.1.9. *Let $d > 0$ be squarefree and $d \not\equiv 3 \bmod 4$. Let $K = \mathbb{Q}(\sqrt{-d})$, $H = HCF(K)$, and p be an odd prime not dividing $\Delta = -4d$. Write $H = K(\alpha)$ and let $f(x)$ be the minimum polynomial for α. Then the following are equivalent:*

(i) p is represented by $x^2 + dy^2$

(ii) p splits completely in H

(iii) $\left(\frac{\Delta}{p}\right) = 1$ and $f(x)$ has a root mod p.

Exercise 5.2. *Check the above theorem in the case of $d = 5$.*

5.2 Counting non-unique factorizations

In this section, we will show how one can use quadratic forms to determine and count the irreducible factorizations of an integer in $\mathcal{O}_K$, where K is a quadratic field with class number 2. (In fact, one can treat the case of $\mathcal{C}l_K \simeq C_2^r$ by the same approach.) For simplicity, we will just go through the specific case of $K = \mathbb{Q}(\sqrt{-5})$.

Afterwards, we will discuss what happens in an arbitrary number field, where one must use ideal theory to obtain the analogous result. In particular, this gives a qualitative and quantitative way to see that the class group $\mathcal{C}l_K$ really does measure the failure of unique factorization in $\mathcal{O}_K$ in a precise way. Both these results and this approach using principalization seems to be new (in fact I proved it just to show you how the class group measures the failure of unique factorization in $\mathcal{O}_K$!), see [Martin] for more details. For an introduction to other work on irreducible factorizations (in different directions), see [Narkiewicz].

Let $K = \mathbb{Q}(\sqrt{-5})$ so $\Delta = \Delta_K = -20$. Denote by $\mathfrak{C}_1$ the set of principal ideals in $\mathcal{O}_K$ and $\mathfrak{C}_2$ the set of nonprinicpal ideals of $\mathcal{O}_K$. The reduced forms of discriminant Δ are $Q_1(x, y) = x^2 + 5y^2$ and $Q_2(x, y) = 2x^2 + 2xy + 3y^2$.

Let $\mathcal{P}_0$ denote the primes $p \in \mathbb{N}$ which are not represented by Q_1 or Q_2 and $\mathcal{P}_i$ denote the primes $p \in \mathbb{N}$ which are represented by Q_i for $i = 1, 2$. Then $\mathcal{P}_0$ is the set of inert primes in $K/\mathbb{Q}$, $\mathcal{P}_1$ is the set of primes p such that the ideal $p\mathcal{O}_K$ factors into two principal ideals in $\mathcal{O}_K$, and $\mathcal{P}_2$ is the set of primes p such that $p\mathcal{O}_K$ factors into two nonprincipal ideals of $\mathcal{O}_K$.

Set

$$\mathcal{P}_i^{ram} = \{p \in \mathcal{P}_i : p \text{ is ramified in } K\}, \text{ and}$$
$$\mathcal{P}_i^{unr} = \{p \in \mathcal{P}_i : p \text{ is unramified in } K\}.$$

Explicitly, we have $\mathcal{P}_0 = \{p : p \equiv 11, 13, 17, 19 \bmod 20\}$, $\mathcal{P}_1^{ram} = \{5\}$, $\mathcal{P}_1^{unr} = \{p : p \equiv 1, 9 \bmod 20\}$, $\mathcal{P}_2^{ram} = \{2\}$ and $\mathcal{P}_2^{unr} = \{p : p \equiv 3, 7 \bmod 20\}$.

If $p \in \mathcal{P}_0 \cup \mathcal{P}_1$ then any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying above p is in $\mathfrak{C}_1$, and if $q \in \mathcal{P}_2$, then any prime ideal of $\mathcal{O}_K$ lying above q is in $\mathfrak{C}_2$. Specifically, if $q = 2 \in \mathcal{P}_2^{ram}$, then $q\mathcal{O}_K = \mathfrak{r}^2$ where $\mathfrak{r}$ is the prime ideal $(2, 1 + \sqrt{-5})$ of $\mathcal{O}_K$, and if $q \in \mathcal{P}_2^{unr}$ then $q = \mathfrak{q}\overline{\mathfrak{q}}$ where $\mathfrak{q}$ and $\overline{\mathfrak{q}}$ are distinct prime ideals of $\mathcal{O}_K$. Here $\overline{\mathfrak{q}}$ denotes the conjugate ideal of $\mathfrak{q}$ in $K/\mathbb{Q}$.

Now let $n > 1$ and write the prime ideal factorization of $n\mathcal{O}_K$ as

$$(n) = \mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_r^{d_r} \mathfrak{q}_1^{e_1} \overline{\mathfrak{q}}_1^{e_1} \cdots \mathfrak{q}_s^{e_s} \overline{\mathfrak{q}}_s^{e_s} \mathfrak{r}^f,$$

where each $\mathfrak{p}_i \in \mathfrak{C}_1$, $\mathfrak{q}_j \in \mathfrak{C}_2$ with conjugate $\overline{\mathfrak{q}}_j$, and the $\mathfrak{p}_i$'s, $\mathfrak{q}_j$'s, $\overline{\mathfrak{q}}_j$'s and $\mathfrak{r}$ are all distinct. Since each $\mathfrak{p}_i = (\pi_i)$ for some irreducible π_i of $\mathcal{O}_K$, any irreducible factorization of n must contain (up to units) $\pi_1^{d_1} \cdots \pi_r^{d_r}$. Thus it suffices to consider irreducible factorizations of $n' = n/(\pi_1^{d_1} \cdots \pi_r^{d_r})$.

Let q_j be the prime in $\mathbb{N}$ such that $\mathfrak{q}_j$ lies above q_j. Since $\mathfrak{q}_j$ is nonprincipal, we must have that $q_j \in \mathcal{P}_2$, i.e., q_j is represented by Q_2. Note that we can factor the quadratic form into linear factors

$$Q_2(x, y) = (\sqrt{2}x + \frac{\sqrt{2} + \sqrt{-10}}{2}y)(\sqrt{2}x + \frac{\sqrt{2} - \sqrt{-10}}{2}y) \tag{5.1}$$

over the field $L = K(\sqrt{2})$. Hence, while q_j is irreducible over $\mathcal{O}_K$ (otherwise the prime ideal factors of $q_j\mathcal{O}_K$ would be principal), the fact that $q_j = Q_2(x, y)$ for some x, y gives us a factorization $q_j = \alpha_j\overline{\alpha}_j$ in L where $\alpha_j = \sqrt{2}x + \frac{\sqrt{2}+\sqrt{-10}}{2}y$ and $\overline{\alpha}_j = \sqrt{2}x + \frac{\sqrt{2}-\sqrt{-10}}{2}y$. Since $\sqrt{2}, \frac{\sqrt{2}\pm\sqrt{-10}}{2} \in \mathcal{O}_L$, we have $\alpha_j \in \mathcal{O}_L$ (in fact irreducible).

Since α_j and $\overline{\alpha}_j$ are conjugate with respect to the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$, the ideals $(\alpha_j) \cap \mathcal{O}_K$ and $(\overline{\alpha}_j) \cap \mathcal{O}_K$ must be conjugate ideals of $\mathcal{O}_K$ which divide q_j, and hence in some order equal $\mathfrak{q}_j$ and $\overline{\mathfrak{q}}_j$. Thus, up to a possible switching α_j and $\overline{\alpha}_j$, we can write $\mathfrak{q}_j\mathcal{O}_L = (\alpha_j)$ and $\overline{\mathfrak{q}}_j\mathcal{O}_L = (\overline{\alpha}_j)$. Similarly $\mathfrak{r}\mathcal{O}_L = (\sqrt{2})$.

This means the following. If $n' = \prod \beta_i$ is any irreducible factorization of n' in $\mathcal{O}_K$, we have

$$\prod(\beta_i) = (n') = \mathfrak{r}^f \mathfrak{q}_1^{e_1} \overline{\mathfrak{q}}_1^{e_1} \cdots \mathfrak{q}_s^{e_s} \overline{\mathfrak{q}}_s^{e_s} = (\sqrt{2})^f \prod_{j=1}^{s} (\alpha_j)^{e_j} (\overline{\alpha}_j)^{e_j}$$

as ideals of $\mathcal{O}_L$. From Proposition 5.1.2, we know that each (β_i) is a subproduct of the product of ideals on the right. In other words, to the irreducible factorizations of $\mathcal{O}_K$ come from different groupings of the factorization

$$n' = \sqrt{2}^f \prod_{j=1}^{s} \alpha_j^{e_j} \overline{\alpha}_j^{e_j}. \tag{5.2}$$

Thus to determine the factorizations of of n' in $\mathcal{O}_K$, it suffices to determine when a product of the α_{ij} is an irreducible element of $\mathcal{O}_K$. But this is simple! Note from the factorization of $Q_2(x, y)$ in (5.1), we see that each $\alpha_{ij} \in \sqrt{2}K$. Hence the product of any two α_i's (or $\sqrt{2} \cdot \alpha_j$ or $\sqrt{2} \cdot \sqrt{2}$) lies in K, and therefore $\mathcal{O}_K$, and must be irreducible since no individual $\alpha_j \in \mathcal{O}_K$. In other words,

the irreducible factorizations of n' in $\mathcal{O}_K$ are precisely what we get from grouping the terms on the right of (5.2) in pairs. What we have proved is the following.

If $\{a_i\}$ is a collection of distinct objects, denote the multiset containing each a_i with cardinality m_i by $\left\{a_i^{(m_i)}\right\}$. Let $\eta_K(n)$ denote the number of distinct (up to order and units) irreducible factorizations of n in $\mathcal{O}_K$.

Proposition 5.2.1. *With notation as above ($K = \mathbb{Q}(\sqrt{-5})$, the irreducible factorizations of n in $\mathcal{O}_K$ are, up to units, $n = \prod \pi_i \prod \beta_k$ where each β_k is a product of two numbers of the following types: $\sqrt{2}, \alpha_j$, or $\overline{\alpha}_j$. In particular, $\eta_K(n)$ is the number of ways we can arrange the multiset $\left\{\sqrt{2}^{(f)}, \alpha_j^{(e_j)}, \overline{\alpha}_j^{(e_j)}\right\}$ in pairs.*

The **length** of an irreducible factorization is the number of irreducibles occurring in the factoriziation, with multiplicity.

Corollary 5.2.2. *Any two irreducible factorizations of n in $\mathcal{O}_K$ have the same length.*

Hence the above result tells us about the structure of the irreducible factorizations in $\mathcal{O}_K$, not just their number. In fact, the above approach tells us how to explicitly obtain all irreducible factorizations of some n in $\mathcal{O}_K$.

Example 5.2.3. *Let $n = 2 \cdot 7^2 \cdot 29$. Here $29 \in \mathcal{P}_1$ and $2, 7 \in \mathcal{P}_2$. We have*

$$2 = Q_2(1,0) = \sqrt{2} \cdot \sqrt{2}$$

$$7 = Q_2(1,1) = \underbrace{(\sqrt{2} + \frac{\sqrt{2} + \sqrt{-10}}{2})}_{\alpha}\underbrace{(\sqrt{2} + \frac{\sqrt{2} - \sqrt{-10}}{2})}_{\overline{\alpha}}$$

$$29 = Q_1(3,2) = 3^2 + 5 \cdot 2^2 = \underbrace{(3 + 2\sqrt{-5})}_{\pi}\underbrace{(3 - 2\sqrt{-5})}_{\overline{\pi}}$$

using the factorization of Q_1 and Q_2 into linear forms over $\mathcal{O}_L$. Then the above tells us the irreducible factorizations of n in $\mathcal{O}_K$ are precisely those obtained from grouping the terms in square brackets on the right in pairs in the following factorization in $\mathcal{O}_L$:

$$n = \pi\overline{\pi}\left[\sqrt{2} \cdot \sqrt{2} \cdot \alpha \cdot \alpha \cdot \overline{\alpha} \cdot \overline{\alpha}\right].$$

Precisely, we have $\eta_K(n) = 5$ factorizations and they are explicitly given by

$$n = \pi\overline{\pi}(\sqrt{2}\sqrt{2})(\alpha\alpha)(\overline{\alpha}\overline{\alpha})$$

$$n = \pi\overline{\pi}(\sqrt{2}\sqrt{2})(\alpha\overline{\alpha})(\alpha\overline{\alpha})$$

$$n = \pi\overline{\pi}(\sqrt{2}\alpha)(\sqrt{2}\alpha)(\overline{\alpha}\overline{\alpha})$$

$$n = \pi\overline{\pi}(\sqrt{2}\alpha)(\sqrt{2}\overline{\alpha})(\alpha\overline{\alpha})$$

$$n = \pi\overline{\pi}(\sqrt{2}\overline{\alpha})(\sqrt{2}\overline{\alpha})(\alpha\alpha).$$

(Each product of two terms in $\mathcal{O}_L$ in parentheses above is an irreducible element of $\mathcal{O}_K$. If you feel a need, you can compute these products explicitly, and check that they are all distinct factorizations in $\mathcal{O}_K$.)

Exercise 5.3. *Determine all irreducible factorizations of $n = 60$ in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$.*

Exercise 5.4. *Let $p \in \mathbb{N}$ be prime and $e \geq 1$. Determine a formula for $\eta_K(p^e)$ where $K = \mathbb{Q}(\sqrt{-5})$. (It will depend on the value of $p \bmod 20$ as well as e.)*

Exercise 5.5. *Let $q_1, \ldots, q_k$ be distinct primes in $\mathcal{P}_2^{unr}$. Show $\eta_K(q_1 \cdots q_k) = (2k-1)!! = (2k-1)(2k-3)(2k-5)\cdots 3 \cdot 1$. (Again $K = \mathbb{Q}(\sqrt{-5})$.)*

We remark that there seems to be no simple algebraic formula for $\eta_K(n)$ for general n, despite the fairly simple combinatorial description. However, there is a simple way to compute $\eta_K(n)$ in terms of generating functions, a technique often used in combinatorics. We give it precisely in the following alternate version of the above proposition.

Proposition 5.2.4. *Let $K = \mathbb{Q}(\sqrt{-5})$, $L = K(\sqrt{2})$ and $n > 1$. Write the prime ideal factorization of (n) in $\mathcal{O}_K$ as $(n) = \prod \mathfrak{p}_i^{d_i} \prod \mathfrak{q}_j^{e_j}$, where each $\mathfrak{p}_i \in \mathfrak{C}_1$, $\mathfrak{q}_j \in \mathfrak{C}_2$ and the $\mathfrak{p}_i$'s and $\mathfrak{q}_j$'s are all distinct. Let $\pi_i \in \mathcal{O}_K$ and $\alpha_j \in \mathcal{O}_L$ such that $\mathfrak{p}_i = (\pi_i)$ and $\mathfrak{q}_j \mathcal{O}_L = (\alpha_j)$. Then the irreducible nonassociate factorizations of n are precisely $n = u \prod \pi_i^{d_i} \prod \beta_k$ where u is a unit, each β_k is a product of two (not necessarily distinct) α_j's and $\prod \beta_k = \prod \alpha_j^{e_j}$.*

In particular $\eta_K(n)$ is the number of ways we can arrange the multiset $\left\{\alpha_j^{(e_j)}\right\}$ in pairs, i.e., the number of partitions of this multiset into sub-multisets of size 2. In other words, if the number of distinct $\mathfrak{q}_j$'s is m, then $\eta_K(n)$ is the coefficient of $\prod x_j^{e_j}$ in the formal power series expansion of $\prod_{i \leq j} \frac{1}{1-x_i x_j}$ in $\mathbb{Z}[[x_1, x_2, \ldots, x_m]]$.

In fact we stated this proposition for $n \in \mathcal{O}_K$, not just $n \in \mathbb{Z}$, but it is no more difficult to prove. Moreover, the description of $\eta_K(n)$ in terms of coefficients of a power series is essentially a tautology (use the geometric series expansion for $\frac{1}{1-x_i x_j}$ and count).

In general, one can prove an analogue of the above using (just) ideals, and the proof is just as simple as the case of $K = \mathbb{Q}(\sqrt{-5})$ we did with quadratic forms. The advantage of the quadratic forms approach above however is one can explicitly write down the irreducible factorizations of a rational integer n in $\mathcal{O}_K$ in terms of the explicit representations of $p|n$ by quadratic forms of discriminant Δ_K, provided $\mathcal{C}l_K \simeq C_2^r$. See [Martin] for the details when $r > 1$.

(The problem when $\mathcal{C}l_K \simeq C_2^r$, which is tied to the one class per genus problem, is that if Q is a quadratic form which does not have order 2 in $\mathcal{C}l(\Delta)$, then there is no number field L such that Q factors into linear forms over $\mathcal{O}_L$. One can always factor Q into linear forms over some quadratic field, since Q is just a quadratic polynomial, but the problem is that the coefficients of these linear forms will only be algebraic *integers* when Q is ambiguous, hence of order 2 in $\mathcal{C}l(\Delta)$.)

In [Martin], we prove the following.

Theorem 5.2.5. *Let K be a number field and $\mathcal{C}l_K = \{\mathfrak{C}_i\}$. Let $n \in \mathcal{O}_K$ be a nonzero nonunit. Suppose the prime ideal factorization of $n\mathcal{O}_K$ is $(n) = \prod_{(i,j) \in T} \mathfrak{p}_{ij}$ where the $\mathfrak{p}_{ij}$'s are (not necessarily distinct) prime ideals such that $\mathfrak{p}_{ij} \in \mathfrak{C}_i$, and T is some finite index set. Let K_i be a principalization field for $\mathfrak{C}_i$, so $\mathfrak{p}_{ij}\mathcal{O}_{K_i} = (\alpha_{ij})$ for some $\alpha_{ij} \in \mathcal{O}_{K_i}$. Let $L = \prod K_i$.*

Then the irreducible factorizations of n in $\mathcal{O}_K$ are precisely the factorizations of the form $n = \prod \beta_l$ where $\prod \beta_l \sim \prod \alpha_{ij}$ in $\mathcal{O}_L$ and each β_l is of the form $\beta_l \sim \prod_{(i,j) \in S} \alpha_{ij}$ in $\mathcal{O}_L$ for S a minimal (nonempty) subset of T such that $\prod_{(i,j) \in S} \mathfrak{C}_i = \mathfrak{I}$. (Here each β_l is irreducible in $\mathcal{O}_K$.)

In other words, all irreducible factorizations n in $\mathcal{O}_K$ come from different groupings of the factorization $n \sim \prod \alpha_{ij}$ in $\mathcal{O}_L$. Now a grouping of terms of this factorization in $\mathcal{O}_L$ gives an

irreducible factorization in $\mathcal{O}_K$ if and only if every group of terms gives an irreducible element of $\mathcal{O}_K$ (possibly up to a unit in $\mathcal{O}_L$). A product of α_{ij}'s gives an element of $\mathcal{O}_K$ if and only if the corresponding product of ideal classes $\mathfrak{C}_i$ is trivial in $\mathcal{C}l_K$, and this element of $\mathcal{O}_K$ will be irreducible if and only if no proper subproduct of the corresponding ideal classes is trivial.

It should be clear that this theorem gives a precise way that the class group measures the failure of unique factorization in $\mathcal{O}_K$. In particular, the larger the class group, the more complicated the structure of the irreducible factorizations of an element can become.

Corollary 5.2.6. *Let K be a number field and $\mathcal{C}l_K = \{\mathfrak{C}_i\}$. Let $n \in \mathcal{O}_K$ be a nonzero nonunit. Suppose $(n) = \prod_{(i,j)\in T} \mathfrak{p}_{ij}^{e_{ij}}$, where the $\mathfrak{p}_{ij}$'s are distinct prime ideals, each $\mathfrak{p}_{ij} \in \mathfrak{C}_j$ and T is some index set. Let U be the multiset $U = \left\{(i,j)^{(e_{ij})} : (i,j) \in T\right\}$. Then $\eta_K(n)$ is the number of ways one can partition the multiset $\left\{x_{ij}^{e_{ij}}\right\}$ into minimal subsets V such that $\prod_{x_{ij}\in V} \mathfrak{C}_i = \mathfrak{I}$.*

Exercise 5.6. *Deduce the following result of Carlitz: Let K be a number field. We say $\mathcal{O}_K$ is half-factorial if every irreducible factorization of a given $n \in \mathcal{O}_K$ has the same length. Then $\mathcal{O}_K$ if half-factorial if and only if $h_K \leq 2$.*

In general, one defines the **elasticity** ρ_K of $\mathcal{O}_K$ to be $\max_{n\in\mathcal{O}_K} \rho_K(n)$ where $\rho_K(n)$ is the maximum ratio of lengths of two irreducible factorizations of n in $\mathcal{O}_K$. Similarly, one can use our theorem above to determine ρ_K in terms of the structure of the class group (it depends upon more than just h_K). See [Narkiewicz] for complete statements (needless to say, proved there without recourse to our theorem).