2 Primes in extensions

This chapter is about the following basic question: given an extension of number fields L/K and a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$, how does $\mathfrak{p}\mathcal{O}_L$ factor into prime ideals of $\mathcal{O}_L$? This question is intimately tied up with many questions of arithmetic. Going back to our motivating question of which primes p are of the form $p = x^2 + ny^2$ ($n \neq 1$ squarefree), we will see that these are essentialy the p for which (p) is a product of two principal ideals in $\mathbb{Q}(\sqrt{-n})$. After addressing this general question about splitting of prime ideals, we will apply this to primes of the form $x^2 + ny^2$.

Afterwards, we may do some more stuff, but then again maybe we won't.

Note: we will sometimes talk about "ideals" of K or L, or "primes" of K or L. This is merely a simplification of terminology and simply means (ordinary) ideals of $\mathcal{O}_K$ or $\mathcal{O}_L$, or prime ideals of $\mathcal{O}_K$ or $\mathcal{O}_L$.

Another piece of notation to be careful of: if $\alpha \in \mathcal{O}_K$, then (α) may represent $\alpha\mathcal{O}_K$ or $\alpha\mathcal{O}_L$ depending upon whether we are talking about ideals of K or ideals of L. This should hopefully be clear from context in most cases. If not, we will explicitly write $\alpha\mathcal{O}_K$ or $\alpha\mathcal{O}_L$.

The presentation of this material in this chapter is, for the most part, based on [Marcus] and, to a lesser extent, [Cohn] (for the quadratic case) and [Neukirch].

2.1 Splitting of primes

Throughout L/K denotes an extension of number fields. Before we give the basic definitions, let's recall what happens in the simplest example, which we studied last semester.

Example 2.1.1. *Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$. Since $\mathcal{O}_K = \mathbb{Z}$ is a PID, any prime ideal of $\mathcal{O}_K$ is of the form (p) where p is a prime of $\mathbb{Z}$. If $p = x^2 + y^2 = N_{L/K}(x + yi)$, then $p = \alpha\beta$ for some $\alpha, \beta \in \mathcal{O}_L$ and $(p) = (\alpha)(\beta)$ in $\mathcal{O}_L$, i.e., (p) is a product of two principal ideals in $\mathcal{O}_L$. Furthermore $\mathfrak{p}_1 = (\alpha)$ and $\mathfrak{p}_2 = (\beta)$ are both prime since they have norm p. The ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are distinct except in the case $p = 2 = (1+i)(1-i)$ since $1 + i = -i(1 - i)$, i.e., $1 + i$ and $1 - i$ differ by units.*

If p is not a sum of two squares, then this means there is no element of norm p in $\mathcal{O}_L$, so p is irreducible in $\mathcal{O}_L$. Hence if some prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$ divides (p) but $\mathfrak{p} \neq (p)$, then it can't be principal (otherwise, the generator of $\mathfrak{p}$ would divide p). However $h_L = 1$ so $\mathcal{O}_L$ is a PID. Thus $(p) = p\mathcal{O}_L = \{p\alpha : \alpha \in \mathcal{O}_L\}$ is itself a prime ideal.

Hence in this example, there are 3 possibilities for what happens to a prime ideal $p\mathcal{O}_K$ of K in the extension L:

(1) it splits *as a product of two distinct prime ideals $(p) = \mathfrak{p}_1\mathfrak{p}_2$ in $\mathcal{O}_L$ iff $\pm p = x^2 + y^2$ and $p \neq 2$, i.e., iff $p \equiv 1 \bmod 4$;*

(2) it ramifies *as the square of a prime ideal $(p) = 2\mathcal{O}_L = (1 + i)^2 = \mathfrak{p}^2$ in $\mathcal{O}_L$ iff $\pm p = 2$; and*

(3) it remains prime *or is* inert*, i.e., $p\mathcal{O}_L$ is a prime ideal of $\mathcal{O}_L$, if and only if $\pm p \neq x^2 + y^2$, i.e., iff $p \equiv 3 \bmod 4$.*

If $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$, we define

$$\mathfrak{a}\mathcal{O}_L = \{a_1x_1 + a_2x_2 + \cdots + a_kx_k : a_i \in \mathfrak{a}, x_i \in \mathcal{O}_L\}.$$

Notice this is just like the definition of the product of two ideals of the same ring. It is easy to see that this is the smallest ideal of $\mathcal{O}_L$ which contains the set $\mathfrak{a}$ (see exercise below). Note if $\mathfrak{a} = (a)$ is a principal ideal of $\mathcal{O}_K$, then $\mathfrak{a}\mathcal{O}_L = (a) = \{ax : x \in \mathcal{O}_L\}$.

Exercise 2.1. *Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$ and $\mathfrak{A}$ be an ideal of $\mathcal{O}_L$. Show $\mathfrak{a}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$ and $\mathfrak{A} \cap K = \mathfrak{A} \cap \mathcal{O}_K$ (justify this equality) is an ideal of $\mathcal{O}_K$. We call $\mathfrak{a}\mathcal{O}_L$ the* **extension** *of $\mathfrak{a}$ to L and $\mathfrak{A} \cap \mathcal{O}_K$ the* **restriction** *of $\mathfrak{A}$ to K.*

It is tradition to use gothic lower case letters for ideals of $\mathcal{O}_K$ and upper case gothic letters for ideals of $\mathcal{O}_L$. (Though I suppose it's also tradition to write $\mathcal{O}_K$ as $\mathfrak{O}_K$, I'm not as fond of that one.) However if $K = \mathbb{Q}$, we just use integers for the ideals of $\mathcal{O}_K = \mathbb{Z}$ since they are all principal, and lower case gothic letters for ideals of the extension L, as in the example above. If you have trouble writing gothic letters by hand, you can just write the corresponding roman letter with an underscore, or use another script.

While the extension and restriction of ideals are defined uniquely, this is not a 1-to-1 correspondence, as there are more ideals of $\mathcal{O}_L$ than ideals of $\mathcal{O}_K$. Precisely, we will see that different ideals of $\mathcal{O}_K$ extend to different ideals of $\mathcal{O}_L$, but different ideals of $\mathcal{O}_L$ can restrict to the same ideal of $\mathcal{O}_K$.

Definition 2.1.2. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$. We say $\mathfrak{P}$* **lies over** *(or* **lies above***) $\mathfrak{p}$ in L/K if $\mathfrak{P}|\mathfrak{p}\mathcal{O}_L$. We sometimes write this as $\mathfrak{P}|\mathfrak{p}$.*

Going back to the previous example, in case (1) $\mathfrak{p}_1$ and $\mathfrak{p}_2$ lie above (p); in case (2) $\mathfrak{p}$ lies above (p) and in case (3) $(p) = p\mathcal{O}_L$ lies above $(p) = p\mathcal{O}_K$.

Let $\mathfrak{p}$ be a prime (ideal) of $\mathcal{O}_K$ and $\mathfrak{P}$ be a prime (ideal) of $\mathcal{O}_L$.

Lemma 2.1.3. *The following are equivalent:*
(a) $\mathfrak{P}|\mathfrak{p}$, i.e., $\mathfrak{P}|\mathfrak{p}\mathcal{O}_L$
(b) $\mathfrak{P} \supseteq \mathfrak{p}$
(c) $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{P} \cap K = \mathfrak{p}$.

Proof. (a) $\Rightarrow$ (b) since $\mathfrak{P} \supseteq \mathfrak{p}\mathcal{O}_L \supseteq \mathfrak{p}$.

To see (b) $\Rightarrow$ (c), observe that $\mathfrak{P} \supseteq \mathfrak{p}$ implies $\mathfrak{P} \cap \mathcal{O}_K \supseteq \mathfrak{p}$. Since $\mathfrak{p}$ is maximal, and $\mathfrak{P} \cap \mathcal{O}_K$ is an ideal by the exercise above, we have $\mathfrak{P} \cap \mathcal{O}_K$ is either $\mathfrak{p}$ or $\mathcal{O}_K$. The latter is impossible since it would imply $1 \in \mathfrak{P}$.

To see (c) $\Rightarrow$ (b) $\Rightarrow$ (a), note that (c) implies $\mathfrak{P} \supseteq \mathfrak{p}$ is obvious, and then $\mathfrak{P} \supseteq \mathfrak{p}\mathcal{O}_L$ since $\mathfrak{P}$ is an ideal of $\mathcal{O}_L$. □

In light of the equivalence (a) $\iff$ (b), the notation $\mathfrak{P}|\mathfrak{p}$ for one ideal lying over another agrees with the usage of the notation $\mathcal{I}|\mathcal{J}$ to mean divides (contains) for ideals of $\mathcal{O}_K$.

Another thing this lemma shows is that two different ideals of L can restrict to the same ideal of K. For example if p is a prime of $K = \mathbb{Q}$, and $p\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 \neq \mathfrak{p}_2$, then $\mathfrak{p}_1$ and $\mathfrak{p}_2$ both restrict to the ideal $p\mathbb{Z}$ of $\mathbb{Z}$. More generally, all primes $\mathfrak{P}$ of $\mathcal{O}_L$ lying above a prime $\mathfrak{p}$ of $\mathcal{O}_K$ restrict to $\mathfrak{p}$.

Proposition 2.1.4. *Every prime $\mathfrak{P}$ of $\mathcal{O}_L$ lies above a unique prime $\mathfrak{p}$ of K. Conversely, every prime $\mathfrak{p}$ of K is contained in some prime $\mathfrak{P}$ of $\mathcal{O}_L$, i.e., there is some prime $\mathfrak{P}$ of $\mathcal{O}_L$ such that $\mathfrak{P}|\mathfrak{p}$.*

Proof. Suppose $\mathfrak{P} \cap \mathcal{O}_K|\mathfrak{a}\mathfrak{b}$ for some ideals $\mathfrak{a}$, $\mathfrak{b}$ of $\mathcal{O}_K$. Then $\mathfrak{P} \supseteq (\mathfrak{a}\mathcal{O}_L)(\mathfrak{b}\mathcal{O}_L)$ so $\mathfrak{P} \supset \mathfrak{a}\mathcal{O}_L$ or $\mathfrak{P} \supset \mathfrak{b}\mathcal{O}_L$ since $\mathfrak{P}$ is prime. Restricting to K, we see $\mathfrak{P} \cap \mathcal{O}_K|\mathfrak{a}$ or $\mathfrak{P} \cap \mathcal{O}_K|\mathfrak{b}$. Hence $\mathfrak{P} \cap \mathcal{O}_K$ is a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ by definition, i.e., $\mathfrak{P}|\mathfrak{p}$. By the previous lemma, $\mathfrak{P}|\mathfrak{p}$ implies $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, hence

$\mathfrak{p}$ is unique. This proves the first statement, though technically one should also show $\mathfrak{P} \cap \mathcal{O}_K \neq \{0\}$. This is easy—see the exercise below.

The second statement is seemingly obvious: given $\mathfrak{p}$, the extension $\mathfrak{p}\mathcal{O}_L$ has a prime ideal factorization in $\mathcal{O}_L$, so any prime ideal $\mathfrak{P}$ occurring in the factorization lies above $\mathfrak{p}$. However as before, one needs to show a seemingly obvious technicality: $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$ (otherwise $\mathfrak{p}\mathcal{O}_L$ would not have a prime ideal factorization). This is also an exercise. □

Exercise 2.2. *Let L/K be an extension of number fields and $\mathcal{I}$ be a (nonzero) ideal of $\mathcal{O}_L$. Show $\mathcal{I} \cap \mathcal{O}_K \neq \{0\}$. (You may want to consider using norms.)*

Exercise 2.3. *(a) Let $\mathfrak{a}$ be a proper ideal of $\mathcal{O}_K$. Show there exists a $\gamma \in K - \mathcal{O}_K$ such that $\gamma\mathfrak{a} \subseteq \mathcal{O}_K$.*

(b) Let L/K be an extension of number fields and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$. Show $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$. (Use (a) to get a contradiction if $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$.)

Exercise 2.4. *(a) Let $\mathfrak{a}, \mathfrak{b}$ be ideals of K. Show $\mathfrak{a}\mathcal{O}_L | \mathfrak{b}\mathcal{O}_L \implies \mathfrak{a}|\mathfrak{b}$. (Think about prime factorizations in K and L.)*

(b) Show $\mathfrak{a}\mathcal{O}_L \cap \mathcal{O}_K = \mathfrak{a}$ for any ideal $\mathfrak{a}$ of $\mathcal{O}_K$, i.e., the restriction of an extension gives the ideal you started with. (Use (a) with $\mathfrak{b} = \mathfrak{a}\mathcal{O}_L \cap \mathcal{O}_K$.)

(c) Determine which ideals $\mathfrak{A}$ of L satisfy $(\mathfrak{A} \cap \mathcal{O}_K)\mathcal{O}_L = \mathfrak{A}$, i.e., determine when the extension of the restriction of an ideal is the ideal you started with.

Looking back at the case of $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$ from Example 2.1.1, we see sometimes the number of primes lying above $\mathfrak{p}$ is 1 and sometimes it is 2. In general, the number of primes above $\mathfrak{p}$ is never greater than $n = [L : K]$, and if we count with primes with "multiplicty" and "weight" it will always be n. Multiplicity is easy to imagine: if $[L : K] = 2$ and $\mathfrak{p} = \mathfrak{P}^2$ then it makes sense to count $\mathfrak{P}$ two times—technically this multiplicity is called the *ramification index* (or *ramification degree*). There is only one prime that is ramified in the extension $\mathbb{Q}(i)/\mathbb{Q}$, namely $2\mathbb{Z}[i] = (1+i)^2$.

The notion of some primes being "weighted" is a little more subtle, but it can obviously happen that $\mathfrak{p} = \mathfrak{P}$, i.e., a prime $\mathfrak{p}$ of K *remains prime* (or is *inert*) in L, i.e., $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}$ is prime in L. If we go back to Example 2.1.1, half of the primes in $\mathbb{Q}$ are inert in $\mathbb{Q}(i)$, the ones $\equiv 3 \bmod 4$, i.e., the primes not sums of 2 squares. One way to differentiate the case of inert and "split" primes in this example is the following. For split primes ($p \equiv 1 \bmod 4$), we have $\mathfrak{p}\mathcal{O}_L = p\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2$, then $[\mathcal{O}_L : \mathfrak{P}_i] = N(\mathfrak{P}_i) = p$ (this also holds for the ramified case of $p = 2$), but for inert primes ($p \equiv 1 \bmod 3$), then $\mathfrak{P} = \mathfrak{p}\mathcal{O}_L = p\mathcal{O}_L$ is prime in L and we have $[\mathcal{O}_L : \mathfrak{P}] = N(\mathfrak{P}) = N_{L/K}(p) = p^2$.

Hence, if we think of the exponent of p in $N(\mathfrak{P}) = [\mathcal{O}_L : \mathfrak{P}]$ as the "weight" of $\mathfrak{P}$, then we can say the weighted sum of the primes above $\mathfrak{p}$ (with multiplicity) is always 2, at least in Example 2.1.1. In general, when the base field $K \neq \mathbb{Q}$, this definition of weight needs to be appropriately modified, and we give the formal definitions of the appropriate multiplicity (ramification index) and weight (inertial degree) below.

Exercise 2.5. *Suppose $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. Show the ring embedding $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ yields a field embedding $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{P}$. In other words, the finite field $\mathcal{O}_L/\mathfrak{P}$ is an extension of $\mathcal{O}_K/\mathfrak{p}$.*

Definition 2.1.5. *Let $\mathfrak{p}$ be a prime of K. Suppose the prime ideal factorization of $\mathfrak{p}\mathcal{O}_L$ is $\mathfrak{p} = \prod \mathfrak{P}_i^{e_i}$ where each $\mathfrak{P}_i$ is distinct. The* **ramification index** *of $\mathfrak{P}_i$ over $\mathfrak{p}$ is $e(\mathfrak{P}_i|\mathfrak{p}) = e_i$ and the* **inertial degree** *of $\mathfrak{P}_i$ over $\mathfrak{p}$ is $f(\mathfrak{P}_i|\mathfrak{p}) = f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$.*

This definition of inertial degree is really the natural generalization of the "weight" of $\mathfrak{P}$ we suggested in the case of $\mathbb{Q}(i)/\mathbb{Q}$ (see also lemma below). The previous exercise guarantees it makes sense. For instance, if $K = \mathbb{Q}$, then and $\mathfrak{P} = p\mathcal{O}_L$ is prime in L, then $f(\mathfrak{P}|(p)) = [\mathcal{O}_L/p\mathcal{O}_L : \mathbb{Z}/p\mathbb{Z}]$. Now $\mathcal{O}_L/p\mathcal{O}_L$ must be the finite field of order $N(p\mathcal{O}_L) = N_{L/\mathbb{Q}}(p) = p^n$ where $n = [L : K]$, which has degree n over $\mathbb{Z}/p\mathbb{Z}$, so the inertial degree is $f(\mathfrak{P}|(p)) = n$.

The above definition of inertial degree, is the standard one, but it is clearly equivalent to the following form, which will be useful to us.

Lemma 2.1.6. *The inertial degree $f_i = f(\mathfrak{P}_i|\mathfrak{p})$ satisfies $N(\mathfrak{P}_i) = N(\mathfrak{p})^{f_i}$.*

Proof. We know $\mathcal{O}_K/\mathfrak{p}$ is a finite field of some order, say $q = N(\mathfrak{p})$. By the exercise above $\mathcal{O}_L/\mathfrak{P}$ is an extension of $\mathcal{O}_K/\mathfrak{p}$, and the order of this extension field is $q^{f_i} = N(\mathfrak{P}_i)$ by the definition of the inertial degree. Hence $N(\mathfrak{p})^{f_i} = N(\mathfrak{P})$. □

Theorem 2.1.7. (The fundamental identity) *With the notation in the definition,*

$$\sum e_i f_i = n = [L : K].$$

For simplicity, we will omit some details of the proof when $K \neq \mathbb{Q}$.

Proof. Note

$$N(\mathfrak{p}\mathcal{O}_L) = \prod N(\mathfrak{P}_i)^{e_i} = \prod N(\mathfrak{p})^{e_i f_i},$$

by the previous lemma. Then the theorem follows from the statement that $N(\mathfrak{p}\mathcal{O}_L) = N(\mathfrak{p})^n$.

This is true but not entirely obvious—one must check some details. However in our main case of interest, which is $K = \mathbb{Q}$, it is particularly simple, and in the interest of time and simplicity we will restrict to when $K = \mathbb{Q}$. Then $\mathfrak{p} = (p)$ for some $p \in \mathbb{N}$ and $N(\mathfrak{p}\mathcal{O}_L) = N(p\mathcal{O}_L) = N_{L/K}(p) = p^n$. □

Hence if $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{P}_i^{e_i}$ (with each $\mathfrak{P}_i$ distinct), the number of $\mathfrak{P}_i$ lying above $\mathfrak{p}$ is at most $n = [L : K]$, and is exactly n if we count multiplicities e_i's and "weights" f_i's. Now let's give a couple names for different ways in which $\mathfrak{p}$ (i.e., $\mathfrak{p}\mathcal{O}_L$) can factor in $\mathcal{O}_L$.

Definition 2.1.8. *Write $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$ (with each $\mathfrak{P}_i$ distinct). If $e_i > 1$ for some i, we say $\mathfrak{p}$* **ramifies** *in L. Otherwise, we say $\mathfrak{p}$ is* **unramified** *in L.*

If $g > 1$, i.e. there is more than one prime of L above $\mathfrak{p}$, then we say $\mathfrak{p}$ is **split** *in L. If $g = 1$, i.e. there is only one prime of L above $\mathfrak{p}$, we say $\mathfrak{p}$ is* **nonsplit** *in L.*

If $g = n$, i.e. $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_n$, then we say $\mathfrak{p}$ is **totally split** *(or* **splits completely***) in L. If $g = 1$ and $e_1 = 1$, i.e. if $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1$, then we say $\mathfrak{p}$ is* **inert** *(or* **remains prime***) in L.*

Note by the fundamental identity, if $\mathfrak{p}$ is totally split in L, then $e_i = f_i = 1$ for each i. Similarly if $\mathfrak{p}$ is inert in L then $f(\mathfrak{P}|\mathfrak{p}) = n$ where $\mathfrak{P} = \mathfrak{p}\mathcal{O}_L$. In particular if $\mathfrak{p}$ is totally split or inert in L, then it is unramified. We will see shortly that ramification is a special phenomenon which only happens for finitely many primes.

We now give a couple of simple consequences of the lemma and fundamental identity.

Corollary 2.1.9. *Let $\mathfrak{p}$ be a prime ideal of K which lies above a prime $p \in \mathbb{N}$. Then $N(\mathfrak{p}) = p^k$ for some $1 \leq k \leq [K : \mathbb{Q}]$.*

Proof. It follows from the lemma above (or the argument before with the base field being $\mathbb{Q}$), that $N(\mathfrak{p}) = p^{f(\mathfrak{p}|(p))}$. We know $k = f(\mathfrak{p}|(p)) \leq n$ by the fundamental identity. □

Knowing this is useful in determining whether an ideal is prime or not, and in determining how a prime of $\mathbb{Q}$ splits in K. A consequence of this (without requiring the bound on k) is the fact that an ideal of K divides (the ideal generated by) its norm. Recall we mentioned this result can be used to prove that the class number of K is finite (see Lemma 1.6.6.

Corollary 2.1.10. *Let $\mathcal{I}$ be an ideal of K and $m = N(\mathcal{I})$. Then $\mathcal{I}|m\mathcal{O}_K$.*

Proof. Write $\mathcal{I} = \prod \mathfrak{p}_i$ where the $\mathfrak{p}_i$'s are (not necessarily distinct) prime ideals of K. Then $m = N(\mathcal{I}) = \prod N(\mathfrak{p}_i)$. By the previous corollary, we can write $N(\mathfrak{p}_i) = p_i^{f_i}$ for some f_i where $\mathfrak{p}_i|p_i$. In particular $\mathfrak{p}_i \supseteq p_i\mathcal{O}_K \supseteq p_i^{f_i}\mathcal{O}_K$. Hence

$$\mathcal{I} = \prod \mathfrak{p}_i \supseteq \prod \mathfrak{p}_i^{f_i}\mathcal{O}_K = m\mathcal{O}_K.$$

□

Now one might ask if all primes of L above $\mathfrak{p}$ have the same ramification index and inertial degree. This is not true in general, but it is true if we pass to the Galois closure of L. Precisely, we have the following.

Theorem 2.1.11. *Suppose L/K is Galois and write $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ where the $\mathfrak{P}_i$'s are distinct prime ideals of L. Then $\mathrm{Gal}(L/K)$ acts transitively on $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$. In particular $e_1 = e_2 = \cdots = e_g$ and $f_1 = f_2 = \cdots = f_g$. In this case, if we set $e = e_1$ and $f = f_1$, we have*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^e\mathfrak{P}_2^e \cdots \mathfrak{P}_g^e$$

and the fundamental identity becomes

$$n = efg.$$

Proof. Let $\sigma \in \mathrm{Gal}(L/K)$ and $\mathfrak{P}|\mathfrak{p}$. Since L/K is Galois, $\sigma(\mathfrak{P}) \subseteq \mathcal{O}_L$. It follows immediately from the definitions that $\sigma(\mathfrak{P})$ is an ideal of $\mathcal{O}_L$ and $\sigma(\mathfrak{P})$ is prime. Note if $x \in \mathfrak{p}$, then $\sigma(x) = x$ since $x \in \mathcal{O}_L$. Thus $\mathfrak{P} \supseteq \mathfrak{p}$ implies $\sigma(\mathfrak{P}) \supseteq \mathfrak{p}$, i.e., $\sigma(\mathfrak{P})|\mathfrak{p}$. This implies $\mathrm{Gal}(L/K)$ acts on $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$.

Now we want to show this action is transitive. Suppose it is not, i.e., suppose $\mathfrak{P}, \mathfrak{P}'|\mathfrak{p}$ but $\mathfrak{P}' \neq \sigma(\mathfrak{P})$ for any $\sigma \in \mathrm{Gal}(L/K)$. By the Chinese Remainder Theorem (for general rings) there is an $x \in \mathcal{O}_L$ such that

$$x \equiv 0 \bmod \mathfrak{P}',\ x \equiv 1 \bmod \sigma(\mathfrak{P}) \text{ for all } \sigma \in \mathrm{Gal}(L/K).$$

Now $y = N_{L/K}(x) = \prod \sigma(x) \in \mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p}$. On the other hand $\mathfrak{P} \nmid (y) = \prod(\sigma(x))$ since no $\sigma(x) \in \mathfrak{P}$. But this means $y \notin \mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$, a contradiction.

This shows $\mathrm{Gal}(L/K)$ acts transitively on $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$. On the other hand, $\mathrm{Gal}(L/K)$ fixes $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_g^{e_g}$, so all the ramification indices e_i are the same by uniqueness of prime ideal factorization. Also, because $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ are Galois conjugates of each other, they all have the same norm. Hence the all the inertial degrees f_i are the same. The restatement of the fundamental identity is immediate. □

When L/K is Galois, we say the ideals $\sigma(\mathfrak{P})$ are **conjugates** of $\mathfrak{P}$.

We remark that just like one can define the norm of elements from L to K, one can define the norm of ideals from L to K. Precisely, if $\mathfrak{A}$ is an ideal of L, then the norm from L to K of $\mathfrak{A}$ is

$$N_{L/K}(\mathfrak{A}) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\mathfrak{A}) \cap \mathcal{O}_K.$$

Of course, this norm is an ideal, not a number, but remember that ideals are a sort of generalization of numbers. One can show this satisfies various nice properties, and thus it can be useful like the usual norm is useful.

Exercise 2.6. *Suppose L/K is Galois.*

(a) Suppose $\mathfrak{P}$ is a prime of L lying above $\mathfrak{p}$, a prime of K. Let $f = f(\mathfrak{P}|\mathfrak{p})$. Show $N_{L/K}(\mathfrak{P}) = \mathfrak{p}^f$.

(b) Show $N_{L/K}(\mathfrak{AB}) = N_{L/K}(\mathfrak{A})N_{L/K}(\mathfrak{B})$ for any ideals $\mathfrak{A}, \mathfrak{B}$ of $\mathcal{O}_L$.

(c) Let $\mathfrak{A}$ be an ideal of L with norm $n = N(\mathfrak{A}) = |\mathcal{O}_L/\mathfrak{A}|$. Show $N_{L/\mathbb{Q}}(\mathfrak{A}) = (n)$. In other words, the notion of an "ideal-valued norm" from L to K agrees with the original definition of the integer-valued norm when $K = \mathbb{Q}$ (identifying the principal ideal (n) with the integer n).

2.2 Splitting in quadratic fields

In this section, we will let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field. As usual we will assume $d \neq 1$ is squarefree. Further p will denote a prime (element) of $\mathbb{Z}$ and $\mathfrak{p}$ will denote a prime (ideal) of $\mathcal{O}_K$.

In this case, the splitting of p (i.e., of $p\mathbb{Z}$) in K is particularly simple. By the fundamental identity there are at most 2 prime ideals of K lying above p (i.e., $p\mathbb{Z}$), counting multiplicity. Hence either p is inert in K, i.e., $p\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$, or $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime ideals of $\mathcal{O}_K$. When $\mathfrak{p}_1 = \mathfrak{p}_2$, p is ramified in $\mathcal{O}_K$, and when $\mathfrak{p}_1 \neq \mathfrak{p}_2$, p splits in $\mathcal{O}_K$. Note that since K is quadratic, p splitting and p splitting completely are one and the same.

Let $\Delta = \Delta_K$ be the discriminant of K. Recall $\Delta = d$ if $d \equiv 1 \bmod 4$ and $\Delta = 4d$ if $d \equiv 2, 3 \bmod 4$.

Let $\left(\frac{a}{p}\right)$ denote the **Kronecker symbol** mod p. If p is odd, $\left(\frac{a}{p}\right)$ is the ordinary Legendre symbol define for any $a \in \mathbb{Z}$, i.e., $\left(\frac{a}{p}\right) = 1$ when $\gcd(a, p) = 1$ and a is a square mod p, $\left(\frac{a}{p}\right) = -1$ when $\gcd(a, p) = 1$ and a is a nonsquare mod p, and $\left(\frac{a}{p}\right) = 0$ when $p|a$. If $p = 2$, we set

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & 4|a \\ 1 & a \equiv 1 \bmod 8 \\ -1 & a \equiv 5 \bmod 8 \\ \text{undefined} & a \not\equiv 0, 1 \bmod 4. \end{cases}$$

This is an extension of the Legendre symbol where we have allowed $p = 2$ on the bottom, and $p|a$ for p odd. Note the definition for $p = 2$ satisfies

$$\left(\frac{a}{2}\right) = \left(\frac{2}{a}\right)$$

whenever $a \equiv 0, 1 \bmod 4$. Since the squares mod 8 are $0, 1, 4$, the Kronecker symbol mod 2 detects whether an $a \equiv 0, 1, \bmod 4$ is a square mod 8. The problem with $a \not\equiv 0, 1 \bmod 4$, is one cannot extend the Kronecker symbol to integer values for such a so that it is multiplicative in a. However, this is fine for us, since we only want that $\left(\frac{\Delta}{p}\right)$ is defined for any prime $p \in \mathbb{N}$, which it is since $\Delta \equiv 0, 1 \bmod 4$. The utility of this definition is apparent from the following result on the splitting of p in K.

Theorem 2.2.1. *Let $p \in \mathbb{N}$ be prime.*

(i) If $\left(\frac{\Delta}{p}\right) = 0$ then p is ramified in K.

(ii) If $\left(\frac{\Delta}{p}\right) = 1$ *then* p *is split in* K*.*
(iii) If $\left(\frac{\Delta}{p}\right) = -1$ *then* p *is inert in* K*.*

Note this say the primes with ramify in K are precisely the ones dividing Δ. In particular, there are finitely many.

Proof. Let $\mathfrak{p}$ be a prime of K lying above p. Then $\mathfrak{p}$ is a subgroup of $\mathcal{O}_K$ which is free of rank 2 over $\mathbb{Z}$. In particular, $\mathfrak{p}$ is generated (as an ideal) by at most 2 elements of $\mathcal{O}_K$. We may take one of them to be p, and write $\mathfrak{p} = (p, \pi)$ for some $\pi \in \mathcal{O}_K$. Write $\pi = \frac{a+b\sqrt{d}}{2}$. Further, since $N(\mathfrak{p})|N_{K/\mathbb{Q}}(\pi)$ we have $p|N_{K/\mathbb{Q}}(\pi) = \frac{a^2-db^2}{4}$, so $a^2 \equiv db^2 \bmod p$ (in fact, mod $4p$).

We first prove the contrapositive of (iii). Suppose $p\mathcal{O}_K$ is not inert and p is odd. Then $\mathfrak{p} \neq p\mathcal{O}_K$, so $p \nmid \pi$, i.e., a and b are not both divisible by p. This implies $b \not\equiv 0 \bmod p$. Let b^{-1} such that $b^{-1}b \equiv 1 \bmod p$. Then $a^2 \equiv db^2 \bmod p$ implies $(ab^{-1})^2 \equiv d \bmod p$, i.e., d is a square mod p so either $\left(\frac{d}{p}\right) = 1$ or 0, according to whether $p \nmid d$ or $p|d$. Since $\Delta = d$ or $\Delta = 4d$, $\left(\frac{d}{p}\right) \neq -1$ implies $\left(\frac{\Delta}{p}\right) \neq -1$. This proves (iii).

A similar argument works for $p = 2$.

Now suppose $\left(\frac{\Delta}{p}\right) = 0$ and p odd. Then $\left(\frac{\Delta}{p}\right) = \left(\frac{d}{p}\right)$, so $p|d$. In this case, we can take $\mathfrak{p} = (p, \sqrt{d})$. To see this, observe that any element of $\mathfrak{p}$ looks like

$$\frac{1}{2}((x + y\sqrt{d})p + (z + w\sqrt{d})\sqrt{d}) = \frac{1}{2}(px + dw + (z + py)\sqrt{d})$$

for some $x, y, z, w \in \mathbb{Z}$. Since $p|d$, this means

$$\mathcal{O}_K \supsetneq (p, \sqrt{d}) = \left\{\frac{1}{2}(px + y\sqrt{d}) : x, y \in \mathbb{Z}\right\} \cap \mathcal{O}_K \supsetneq p\mathcal{O}_K.$$

Hence $\mathfrak{p} = (p, \sqrt{d})$ lies above p. Thus $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ where $\overline{\mathfrak{p}}$ is the conjugate ideal of $\mathfrak{p}$ in K, but $\overline{\mathfrak{p}} = (p, -\sqrt{d}) = \mathfrak{p}$, so p is ramified in K.

The case of $\left(\frac{\Delta}{p}\right) = 0$ and $p = 2$ is an exercise below.

Now assume $\left(\frac{\Delta}{p}\right) = 1$ and p odd, so that $\left(\frac{\Delta}{p}\right) = \left(\frac{d}{p}\right) = 1$. Let $a \in \mathbb{Z}$ be such that $a^2 \equiv d \bmod p$. Note $p \nmid a$ since $p \nmid d$. We claim we can take $\overline{p} = (p, a + \sqrt{d})$. Then the conjugate ideal is $\overline{\mathfrak{p}} = (p, a - \sqrt{d})$. It is clear that$\mathfrak{p}, \overline{\mathfrak{p}} \supsetneq p\mathcal{O}_K$, so it suffices to show $\mathfrak{p} \neq \mathcal{O}_K$. To see this, observe that

$$\mathfrak{p}\overline{\mathfrak{p}} = (p^2, pa + p\sqrt{d}, pa - p\sqrt{d}, a^2 - d) \subseteq p\mathcal{O}_K.$$

Hence $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ (and $\mathfrak{p}, \overline{\mathfrak{p}}$ are primes of K). It remains to show $\mathfrak{p} \neq \overline{\mathfrak{p}}$. If $\mathfrak{p} = \overline{\mathfrak{p}}$, then we would have $2a = a + \sqrt{d} - a - \sqrt{d} \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, which is impossible since $p \nmid 2a$. This shows p splits in K.

Suppose $\left(\frac{\Delta}{p}\right) = 1$ and $p = 2$. Then $\Delta \equiv 1 \bmod 8$. Then as in the p odd case one shows one can take $\mathfrak{p} = (2, \frac{1+\sqrt{d}}{2})$, $\overline{\mathfrak{p}} \neq \mathfrak{p}$ and $\mathfrak{p}\overline{\mathfrak{p}} = 2\mathcal{O}_K$. □

Exercise 2.7. *Suppose* $\left(\frac{\Delta}{2}\right) = 0$*. Show* $\mathfrak{p} = (2, \pi)$ *is a proper ideal of* K *containing* $2\mathcal{O}_K$*, where* $\pi = \sqrt{d}$ *or* $1 + \sqrt{d}$ *according to whether* d *is even or odd. Use this to verify (i) in the above theorem for* $p = 2$*.*

Exercise 2.8. *Let* $K = \mathbb{Q}(\sqrt{-5})$*. Determine which primes of* $\mathbb{Q}$ *ramify in* K *and which are unramified. Then determine which primes of* $\mathbb{Q}$ *split completely in* K *and which are inert.*

Note that in the course of the proof of the above theorem, we were able to explicitly describe the prime ideals of K lying above p. For convenient reference, we summarize this below.

Corollary 2.2.2. *If $p \neq 2$ is ramified in K, then $\mathfrak{p} = (p, \sqrt{d})$ is a prime of K lying above p. (For $p = 2$ ramified in K, see Exercise 2.7 above.) If $p \neq 2$ splits in K, then $\mathfrak{p} = (p, a + \sqrt{d})$ is a prime of K lying above p for any a such that $a^2 \equiv d \bmod p$. If 2 splits in K, then $d \equiv 1 \bmod 4$ and $\mathfrak{p} = (2, \frac{1+\sqrt{d}}{2})$ is a prime of K lying above 2.*

The above theorem is very useful for many things. One application is to determining class numbers and class groups of quadratic fields.

Example 2.2.3. *Let $K = \mathbb{Q}(\sqrt{-19})$. This has determinant $\Delta = -19$. By Lemma 1.6.4 (or Minkowski's bound, which is the same in this case), every ideal of $\mathcal{O}_K$ is equivalent to one of norm at most $\frac{2}{\pi}\sqrt{19} \approx 2.85$. There is only ideal of norm one, namely $\mathcal{O}_K$, which is principal. Any ideal of norm 2 must lie above 2 (Corollary 2.1.9), but $\left(\frac{\Delta}{2}\right) = -1$ since $\Delta = -19 \equiv 5 \bmod 8$, i.e., 2 is inert in K. Hence there is no ideal of norm 2, which means the class number $h_K = 1$.*

Exercise 2.9. *Show $K = \mathbb{Q}(\sqrt{-15})$ has class number 2.*

Exercise 2.10. *Show $K = \mathbb{Q}(\sqrt{-43})$ has class number 1.*

Another application of the above theorem is to determining primes of the form $x^2 + ny^2$, which we consider next.

2.3 Primes of the form $x^2 + ny^2$

Recall that one of our motivating questions, both this semester and last semester, was to study numbers of the form $x^2 + ny^2$. Any two number of the form $x^2 + ny^2$ have a product which is also of the form $x^2 + ny^2$ by Brahmagupta's composition law, so this question largely reduces to the question of which primes p are of the form $x^2 + ny^2$.

It is clear that $p = x^2 + ny^2$ means p is reducible in the ring of integers of $K = \mathbb{Q}(\sqrt{-n})$. For simplicity, we assume n is a square free integer, and put $d = -n$, so $K = \mathbb{Q}(\sqrt{d})$ which coincides with the notation in the previous section. For the result below we will allow n to be negative, because it is no extra work (it just involves including a $\pm$ sign), though our main interest is in $n > 0$.

We will also assume $n \neq -1$, because then $K = \mathbb{Q}$. So the case of $n = -1$ is particularly simple, as our question is: which primes are of the form $p = x^2 - y^2 = (x-y)(x+y)$. But this factorization means (say for $p > 0$) that $x - y = 1$ so $p = 2y + 1$, i.e., all odd $p > 0$ are of the form $x^2 - y^2$. Interchanging x and y also shows that any odd $p < 0$ is of the form $x^2 - y^2$.

Proposition 2.3.1. *Let p be a prime of $\mathbb{Z}$. If $p = x^2 + ny^2$ for some $x, y \in \mathbb{Z}$, then $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are (not necessarily distinct) principal prime ideals of $\mathcal{O}_K$. Conversely, if $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are principal prime ideals of $\mathcal{O}_K$, then*

(i) $\pm p$ is of the form $x^2 + ny^2$ if $n \equiv 1, 2 \bmod 4$;

(ii) $\pm 4p$ is of the form $x^2 + ny^2$ if $n \equiv 3 \bmod 4$.

Proof. ($\Rightarrow$) As above, set $d = -n$ to match with notation from the previous section. Suppose $p = x^2 + ny^2 = x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d})$. Since p is squarefree, both x and y must be nonzero so $\alpha = x + y\sqrt{d}$ and $\beta = x - y\sqrt{-d}$ are nonzero nonunits of $\mathcal{O}_K$. Thus $p\mathcal{O}_K = (\alpha)(\beta)$

is the prime ideal factorization of $p\mathcal{O}_K$. (The ideals (α) and (β) are prime either by the argument that $N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\beta) = \pm p$ or using the fundamental identity to count the prime ideals in the factorization of $p\mathcal{O}_K$).

($\Leftarrow$) Suppose $p\mathcal{O}_K$ is a product of two principal prime ideals $\mathfrak{p}_1 = (\alpha)$ and $\mathfrak{p}_2 = (\beta)$. Since the ideals (α) and (β) are conjugate, we may assume α and β are conjugate, i.e., $\alpha = x + y\sqrt{d}$, $\beta = x - y\sqrt{d}$ for some $x, y \in \mathbb{Q}$. Then $N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\beta) = p$, and the factorization $p\mathcal{O}_K = (\alpha)(\beta)$ implies $p = u\alpha\beta = u(x^2 - dy^2)$ for some unit u of $\mathcal{O}_K$. Since $x^2 - dy^2 \in \mathbb{Z}$, we must have $u = \pm 1$.

If $d \equiv 2, 3 \bmod 4$, then we may assume $x, y \in \mathbb{Z}$ so we have shown (i). If $d \equiv 1 \bmod 4$, then $x, y \in \frac{1}{2}\mathbb{Z}$ and (ii) follows. □

Note that we can rephrase the $n \equiv 1, 2 \bmod 4$ case as follows: $\pm p = x^2 + ny^2$ if and only if $p\mathcal{O}_K$ is a product of 2 (not necessarily distinct) principal ideals in $\mathcal{O}_K$.

When $n > 0$, the $\pm$ sign here is moot: negative p are never of the form $x^2 + ny^2$, but for $n < 0$ the distinction of whether p or $-p$ is of the form $x^2 + ny^2$ is somewhat more subtle. Our main focus is when $n > 0$, so we will not worry about this now, but it can be treated via the general theory of binary quadratic forms. We will discuss binary quadratic forms in Part II, but again our focus there will be mostly on the "positive" cases.

One can make a similar if and only if statement when $n \equiv 3 \bmod 4$.

Exercise 2.11. *Suppose $n \equiv 3 \bmod 4$. Show $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ for two (not necessarily distinct) prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$ of $\mathcal{O}_K$ if and only if $\pm 4p = x^2 + ny^2$ for some $x, y \in \mathbb{Z}$.*

To see that these two cases are necessary, look at $K = \mathbb{Q}(\sqrt{-11})$. Then $p = 3 = \frac{1+\sqrt{-11}}{2}\frac{1-\sqrt{-11}}{2}$ so p splits in $\mathcal{O}_K$, but $3 \neq x^2 + 11y^2$ for $x, y \in \mathbb{Z}$. Of course $12 = 4 \cdot 3 = 1^2 + 11 \cdot 1^2$.

We remark that one could treat the $n \equiv 3 \bmod 4$ and the $n \equiv 1, 2 \bmod 4$ uniformly as follows: $\pm p = x^2 + ny^2$ if and only if $p\mathbb{Z}[\sqrt{-n}]$ is a product of two proper principal ideals of $\mathbb{Z}[\sqrt{-n}]$. However the issue with this is that the ideals of $\mathbb{Z}[\sqrt{-n}]$ (when $n \equiv 3 \bmod 4$) are more difficult to study than $\mathcal{O}_K$, e.g., the prime ideal factorization theorem does not hold for $\mathbb{Z}[\sqrt{-n}]$.

Now let's see how we can use this to give alternative (simpler) proofs of some of our main results from last semester. New cases are contained in the exercises. Below p denotes a prime number in $\mathbb{N}$ and $x, y \in \mathbb{Z}$.

Corollary 2.3.2. (Fermat's two square theorem) *We can write $p = x^2 + y^2$ if and only if $p = 2$ or $p \equiv 1 \bmod 4$.*

Proof. By the proposition, $p = x^2 + y^2$ if and only if p is a product of two (not necessarily distinct) principal ideals in $\mathbb{Q}(i)$. ($-p$ cannot be a sum of 2 squares so the $\pm$ in the proposition is not an issue here.) Since we know the class number of $\mathbb{Q}(i)$ is 1, we in fact have $p = x^2 + y^2$ if and only if p splits or ramifies in $\mathbb{Q}(i)$.

Here $\Delta = \Delta_{\mathbb{Q}(i)} = -4$, so by Theorem 2.2.1, $p = x^2 + y^2$ if and only if $p = 2$ (the ramified case) or $\left(\frac{\Delta}{p}\right) = \left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right) = 1$. But the first supplementary law to quadratic reciprocity tells us $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \bmod 4$. □

Exercise 2.12. *We have $p = x^2 + 2y^2$ if and only if $p = 2$ or $p \equiv 1, 3 \bmod 8$.*

We proved this in Chapter 9 last semester, but you should give a simpler argument using the above results. Then we left the case of $x^2 + 3y^2$ as an exercise in Chapter 9, which you may recall was considerably more challenging than the $x^2 + 2y^2$ case. In fact, we still haven't made things any

easier on ourselves for this case since this corresponds to $d \equiv 1 \bmod 4$ above. It may be worthwhile to see what the issue is, so let's go through this.

Suppose $p = x^2 + 3y^2$. Then by the above proposition $p\mathcal{O}_K$ is a product of two principal ideals of $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{-3})$. In this case $h_K = 1$, so every ideal is principal. Hence p either splits or ramifies in $\mathcal{O}_K$ which means $\left(\frac{\Delta}{p}\right) = \left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = 0$ or 1, i.e., $p = 3$ or $p \equiv 1 \bmod 3$. Clearly $p = 3$ is of the form $x^2 + 3y^2$. It remains to show if $p \equiv 1 \bmod 3$, then $p = x^2 + 3y^2$. By this same computation of $\left(\frac{\Delta}{p}\right)$, if $p \equiv 1 \bmod 3$, the p splits into two (prinicipal) ideals of K. However since $d = -n \equiv 1 \bmod 4$, the above proposition only tells us that $4p = x^2 + 3y^2$. For instance $4 \cdot 7 = 5^2 + 3 \cdot 1^2$. It is not clear how to conclude that we must have $p = (x')^2 + 3(y')^2$ for some x', y', though it is true. Roughly, one might like to use Brahmagupta's composition law (the product of two numbers of the form $x^2 + ny^2$ is again of this form—this is simple, but not pretty, computation) in reverse: $4 = 1^2 + 3 \cdot 1^2$ and $4p$ are both of the form $x^2 + 3y^2$, so their *quotient* $p = 4p/4$ should be. We will see that one can more or less do just this using Gauss's theory of binary quadratic forms in Part II. Hence for now, we will forget about the case $n \equiv 3 \bmod 4$ (i.e., $d \equiv 1 \bmod 4$).

Corollary 2.3.3. *We have $p = x^2 + 5y^2$ if and only if $p = 5$ or $p \equiv 1, 9 \bmod 20$.*

Proof. Let $K = \mathbb{Q}(\sqrt{-5})$ so $\Delta = \Delta_K = -20$. Only two primes p ramify in K, $p = 2$ and $p = 5$. Clearly $2 \neq x^2 + 5y^2$ and $5 = x^2 + 5y^2$, so from now on, assume p is unramified. (By the proposition above, this corresponds to the fact that $2\mathcal{O}_K$ is the square of the nonprincipal ideal $(2, 1 + \sqrt{-5})$ and $5\mathcal{O}_K$ is the square of the principal ideal $(\sqrt{-5})$.)

Note that p is split in K if and only if $\left(\frac{\Delta}{p}\right) = \left(\frac{-5}{p}\right) = 1$, i.e., if and only if $p \equiv 1, 3, 7, 9 \bmod 20$.

($\Rightarrow$) If $p = x^2 + 5y^2$, then p splits in K by the proposition, so $p \equiv 1, 3, 7, 9 \bmod 20$. On the other hand, $x^2 + 5y^2 \equiv x^2 + y^2 \equiv 0, 1, 2 \bmod 4$ so $p \not\equiv 3, 7 \bmod 20$. (Alternatively, one can look at the squares mod 20.)

($\Leftarrow$) Suppose $p \equiv 1, 9 \bmod 20$ but $p \neq x^2 + 5y^2$. The congruence conditions imply $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ where $\mathfrak{p}$ is a prime ideal of K, and $p \neq x^2 + 5y^2$ means $\mathfrak{p}$ is nonprincipal. Since $h_K = 2$, this means $\mathfrak{p} \sim (2, 1 + \sqrt{-5})$, i.e., $\mathfrak{p} = \alpha(2, 1 + \sqrt{-5})$ for some $\alpha \in K$.

Write $\alpha = \frac{a}{c} + \frac{b}{d}\sqrt{-5}$ for some $a, b, c, d \in \mathbb{Z}$. Note that 2α and $(1 + \sqrt{-5})\alpha$ must lie in $\mathcal{O}_K$. Since $2\alpha \in \mathcal{O}_K$, $c|2$ and $d|2$ so we can write $\alpha = \frac{a + b\sqrt{-5}}{2}$ (replacing a and b with $2a$ and $2b$ if necessary). Then one has

$$(2)\mathfrak{p} = (a + b\sqrt{-5})(2, 1 + \sqrt{-5}).$$

Taking norms yields

$$2p = a^2 + 5b^2.$$

Reducing this equation mod 5 yields $a^2 \equiv 2, 3 \bmod 5$ (since $p \equiv 1, 4 \bmod 5$), which is a contradiction.* □

For a slightly different argument, see last semester's Chapter 12 Notes. One could simplify this proof if we knew we could use Brahmagupta's composition law in reverse (see above remarks on x^2+3y^2). In particular, for the argument in the ($\Leftarrow$) direction, $\mathfrak{p} \sim (2, 1+\sqrt{-5})$ means $(a+b\sqrt{-5})\mathfrak{p} = (c + d\sqrt{-5})(2, 1 + \sqrt{-5})$ for some $a, b, c, d \in \mathbb{Z}[\sqrt{-5}]$. Taking norms gives $p(a^2 + 5b^2) = 2(c^2 + 5d^2)$. Since 2 is not of the form $x^2 + 5y^2$, one would like to conclude p is not either, but it is not obvious how to make this argument work. We will essentially be able to via genus theory in Part II.

*Thanks to Victor Flynn for correcting an earlier argument.

Before moving on, let us observe there is another interesting characterization of which primes are of the form x^2+5y^2. Suppose $n>0$ and $n \equiv 1,2, \mod 3$. As before, set $K=\mathbb{Q}(\sqrt{-n})$. When $h_K=1$, the above proposition and the theorem if that a prime p is of the form x^2+ny^2 if and only if $\left(\frac{\Delta}{p}\right)=0$ or 1. By quadratic reciprocity, one can then essentially say an prime p is of the form x^2+ny^2 if and only if p is a square mod Δ. (One can formalize this with a different extension of the Legendre symbol called the Jacobi symbol—we won't go through the details, but you can observe it in the simplest case: $p \neq 2$ is of the form x^2+y^2 if and only if p is a square mod $\Delta_{\mathbb{Q}(i)}=-4$.)

When $h_K=2$ (or larger), the problem is the quadratic residue symbol can essentially only detect 2 things—whether p is split or inert (or ramified). But we need to distinguish when a p splits into principal ideals and when p splits into nonprincipal ideals. Check the following criterion for x^2+5y^2.

Exercise 2.13. *Let $K=\mathbb{Q}(\sqrt{-5})$, and $p \in \mathbb{N}$ be a rational prime. Show $p=x^2+5y^2$ if and only if $\left(\frac{\Delta}{p}\right)=1$ and p is a square mod Δ.*

One can treat other forms x^2+ny^2 similar to x^2+5y^2 when the class number of $\mathbb{Q}(\sqrt{-n})$ is 2.

Exercise 2.14. *Determine all primes of the form x^2+6y^2.*

When the class number of $K=\mathbb{Q}(\sqrt{-n})$ is larger than 2, determining the primes of the form x^2+ny^2 can get considerably more complicated, and the solution will depend upon the structure of the class group $\mathcal{C}l_K$. In general, primes of the form x^2+ny^2 are not characterized just by simple congruence conditions (though it always will be if $\mathcal{C}l_K \simeq (\mathbb{Z}/2\mathbb{Z})^r$). We will explore some of the issues involved in Part II.

2.4 General splitting results

In this section, let L/K be an extension of number fields, let $\mathfrak{p}$ denote a prime of K and $\mathfrak{P}$ denote a prime of L. If $\mathfrak{p}\mathcal{O}_L=\prod \mathfrak{P}_i^{e_i}$ with the $\mathfrak{P}_i$'s distinct prime ideals of L, then f_i denotes the inertial degree $f_i=f(\mathfrak{P}_i|\mathfrak{p})$.

In Section 2.2, we saw that it is simple to understand completely the way a prime $\mathfrak{p}$ splits in L when $K=\mathbb{Q}$ and L is quadratic. (It is also not much harder when K is arbitrary and L/K is quadratic.) In general things are not so simple, but there are some general fundamental results which describe the splitting of primes in L/K. We will not give complete proofs in both the interest of time and simplicity.

Note that $\mathcal{O}_K[\alpha]$ is a free $\mathcal{O}_K$-module of rank $n=[L:K]$, so it has finite index (either as an abelian group or $\mathcal{O}_K$-module) in $\mathcal{O}_L$. Thus $\mathcal{O}_L/\mathcal{O}_K[\alpha]$ is a finite abelian group.

Theorem 2.4.1. *Write $L=K(\alpha)$ and let $q(x) \in \mathcal{O}_K[x]$ be the minimum polynomial for α over K. Suppose p is a prime of $\mathbb{Z}$ such that $p \nmid |\mathcal{O}_L/\mathcal{O}_K[\alpha]|$ and $\mathfrak{p}$ is a prime ideal of K lying above p. Write*

$$q(x) \equiv q_1(x)^{e_1} q_2(x)^{e_2} \cdots q_g(x)^{e_g} \mod \mathfrak{p}$$

where the q_i's are distinct irreducible polynomials (of positive degree) in the finite field $\mathcal{O}_K/\mathfrak{p}$. Then

$$\mathfrak{p}\mathcal{O}_L=\mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}$$

for distinct prime ideals $\mathfrak{P}_1,\ldots,\mathfrak{P}_g$ of $\mathcal{O}_L$ such that $f_i=f(\mathfrak{P}_i|\mathfrak{p})=\deg q_i(x)$.

This theorem provides a way to determine how prime ideals $\mathfrak{p}$ of K split in L. For technical reasons, a finite number of primes $\mathfrak{p}$ are excluded from this result.

Proof. (Sketch.) One first shows

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \simeq (\mathcal{O}_K[\alpha])/(\mathfrak{p}\mathcal{O}_K[\alpha]) \simeq (\mathcal{O}_K/\mathfrak{p})[x]/(\overline{q}(x)),$$

where $\overline{q}(x)$ is the image of $q(x)$ in $(\mathcal{O}_K/\mathfrak{p})[x]$. The first isomorphism requires that $\mathfrak{p}\mathcal{O}_L + \mathfrak{F} = \mathcal{O}_L$ where the *conductor* $\mathfrak{F}$ is the largest ideal of $\mathcal{O}_L$ contained in $\mathcal{O}_K[\alpha]$. This is where the technicality that $p \nmid |\mathcal{O}_L/\mathcal{O}_K[\alpha]|$ comes in. The second isomorphism is straightforward.

Then one can use the Chinese Remainder Theorem (for general rings, whose proof is essentially the same as for $\mathbb{Z}$),

$$(\mathcal{O}_K/\mathfrak{p})[x]/(\overline{q}(x)) \simeq \bigoplus_{i=1}^{g} (\mathcal{O}_K/\mathfrak{p})[x]/(\overline{q}_i(x)^{e_i}),$$

where $\overline{q}_i(x)$ is the image of $q_i(x)$ in $(\mathcal{O}_K/\mathfrak{p})[x]$. □

Exercise 2.15. *Suppose $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{-5})$. Determine $|\mathcal{O}_L/\mathcal{O}_K[\alpha]|$ where $\alpha = \sqrt{-5}$. Verify the above theorem in this case.*

Theorem 2.4.2. *Consider the extension $K/\mathbb{Q}$. Then a prime (p) of $\mathbb{Q}$ ramifies in K if and only if $p|\Delta_K$.*

In particular, only finitely many primes of $\mathbb{Q}$ ramify in K.

Corollary 2.4.3. *Let L/K be an extension of number fields. If a prime $\mathfrak{p}$ of K ramifies in L, then $\mathfrak{p}$ lies above a prime of $\mathbb{N}$ dividing Δ_L. In particular, only finitely many primes $\mathfrak{p}$ of K ramify in L.*

Exercise 2.16. *Deduce this corollary from the previous theorem.*