12 Prime ideals

Again, the presentation here is somewhat different than the text. In particular, the sections do not match up. (In fact we have done some of the Chapter 12 material in the text in our Chapter 11 notes.)

Our goal is to prove that $\mathcal{O}_K$ has unique factorization into prime ideals for any number field K. We will use this to determine which primes are of the form $x^2 + 5y^2$.

12.1 The ideal factorization theorems

We are still missing one main ingredient to prove the *existence* of factorization into prime ideals. The ingredient we need is the following result.

Proposition 12.1. *Let K be a number field and $\mathcal{I}, \mathcal{J}$ be nonzero proper ideals of $\mathcal{O}_K$. If $\mathcal{J}|\mathcal{I}$ and $\mathcal{I} \neq \mathcal{J}$, then $\mathcal{I} = \mathcal{J}\mathcal{J}'$ for some nonzero proper ideal $\mathcal{J}'$ of $\mathcal{O}_K$.*

In other words, this notion of $\mathcal{J}|\mathcal{I}$ for ideals, means $\mathcal{I}$ really factors as a product $\mathcal{I} = \mathcal{J}\mathcal{J}'$. This is an immediate consequence of Corollary 12.6 below. Stillwell gives what is perhaps a simpler argument for this in Section 12.5 when K is an imaginary quadratic field. For the moment, let's take it for granted and see how it implies existence of prime factorization for ideals.

Theorem 12.2. (Existence of factorization into prime ideals) *Let K be a number field and $\mathcal{I}$ be a nonzero proper ideal of $\mathcal{O}_K$. Then $\mathcal{I} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ where $\mathfrak{p}_i$'s are prime ideals of $\mathcal{O}_K$.*

Proof. Either $\mathcal{I}$ is maximal (and therefore prime) or not. If so we're done, so suppose not. Then there is some prime ideal $\mathfrak{p}_1$ which contains $\mathcal{I}$ by Prop 11.15 and Cor 11.19. By the above proposition, we can write $\mathcal{I} = \mathfrak{p}_1\mathcal{J}_1$ for some ideal nonzero proper ideal $\mathcal{J}_1$. Further $\mathcal{J}_1 \supseteq \mathcal{I}$. We repeat this argument so that at each stage we get $\mathcal{I} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n\mathcal{J}_n$ and $\mathcal{I} \subseteq \mathcal{J}_1 \subseteq J_2 \subseteq \cdots \subseteq \mathcal{J}_n \subseteq \mathcal{O}_K$. This has to terminate at some point because we can only nest in a finite number of ideals in between $\mathcal{I}$ and $\mathcal{O}_K$ (since $\mathcal{O}_K$ is finitely generated—we used this also in Prop. 11.15), i.e., at some point we have $\mathcal{J}_k = \mathfrak{p}_k$ is prime. □

Theorem 12.3. (Uniqueness of prime ideal factorization) *Let $\mathcal{I}$ be a nonzero proper ideal of $\mathcal{O}_K$ and suppose*

$$\mathcal{I} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s$$

where each $\mathfrak{p}_i$ and $\mathfrak{q}_j$ is a prime ideal of $\mathcal{O}_K$. Then $r = s$ and, up to reordering the $\mathfrak{q}_j$'s, $\mathfrak{p}_i = \mathfrak{q}_i$ for $1 \leq i \leq r$.

Stillwell gives a simple argument for this, but just like his argument for unique prime factorization in $\mathbb{Z}$, it is lacking when some of the prime ideals are repeated in the factorization.

For a complete proof, we would like to make the following argument. Suppose

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s$$

for some prime ideals $\mathfrak{p}_i$, $\mathfrak{q}_j$. By the prime divisor property, i.e., the definition of prime ideals, $\mathfrak{p}_1|\mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s$ implies $\mathfrak{p}_1$ divides one of the $\mathfrak{q}_j$'s, say $\mathfrak{q}_1$. Since $\mathfrak{p}_1$ and $\mathfrak{q}_1$ are maximal (prime), $\mathfrak{p}_1$ divides (contains) $\mathfrak{q}_1$ implies $\mathfrak{p}_1 = \mathfrak{q}_1$. Now we would like to be able to multiply both sides by the "inverse" of $\mathfrak{p}_1$, some $\mathfrak{p}_1^{-1}$, to conclude

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

Repeating this argument would show $r = s$ and $\mathfrak{p}_i = \mathfrak{q}_i$ for each i, giving uniqueness of prime ideal factorizations.

Now if we think about ideals in $\mathbb{Z}$, prime ideals are of the form $\mathfrak{p} = (p)$. Such a $\mathfrak{p}^{-1}$ would have to be something like the ideal generated by p^{-1}, which is not an element of $\mathbb{Z}$. Nevertheless, we can formally construct such ideals, which will be called *fractional ideals*, to apply the above argument. Precisely what we need is given below in Corollary 12.7. It turns out that the theory of fractional ideals will also provide the proof of Proposition 12.1.

12.2 Fractional ideals and the class group

Definition 12.4. *Let K be a number field, and $\mathcal{I} \subseteq K$. If $a\mathcal{I} = \{ai : i \in \mathcal{I}\}$ is an ideal of $\mathcal{O}_K$ for some nonzero $a \in \mathcal{O}_K$, we say $\mathcal{I}$ is a* **fractional ideal** *of $\mathcal{O}_K$. Further if $a\mathcal{I}$ is principal, we say $\mathcal{I}$ is* **principal**. *Denote the set of nonzero fractional ideals of $\mathcal{O}_K$ by $\mathrm{Frac}(\mathcal{O}_K)$, and the set of nonzero principal ideals by $\mathrm{Prin}(\mathcal{O}_K)$.*

Put another way, the fractional ideals of $\mathcal{O}_K$ are just subsets of the form $a^{-1}\mathcal{I}$ where $a \in \mathcal{O}_K$, $a \neq 0$ (possibly $a = 1$, so this includes the case of usual ideals). It is clear that fractional ideals still satisfy the two defining properties of ideals: (i) closed under addition, and (ii) closed under multiplication by elements of $\mathcal{O}_K$. The only thing they don't satisfy in the definition of ideals is that they may not be contained in $\mathcal{O}_K$.

Note on terminology: whenever I say an ideal of $\mathcal{O}_K$, I will mean an honest ideal in $\mathcal{O}_K$. If I mean fractional ideal, I will always say fractional. However, sometimes I will say ordinary ideal to stress that we are talking about honest ideals contained in $\mathcal{O}_K$.

Example. *The fractional ideals of $\mathbb{Z} = \mathcal{O}_{\mathbb{Q}}$ are $\frac{1}{n}(m) = \left\{k\frac{m}{n} : k \in \mathbb{Z}\right\}$ where $m \in \mathbb{N} \cup \{0\}$, $n \in \mathbb{N}$ and $\gcd(m, n) = 1$. To see this, it is clear from the definition, together with the classification of ideals of $\mathbb{Z}$, that they are subsets of $\mathbb{Q}$ of the form $\frac{a}{n}(m)$ for some $\frac{a}{n} \in \mathbb{Q}$ and $m \in \mathbb{N} \cup \{0\}$, i.e., all integer multiples of the rational number $\frac{an}{m}$. Renaming am to m, we see get all multiples of $\frac{m}{n}$. It is clear we may take $\gcd(m, n) = 1$ and $n > 0$ to give the claim.*

Hence the fractional ideals of $\mathbb{Z}$ are in 1-to-1 correspondence with $\mathbb{Q}_{\geq 0}$, the set of nonnegative rational numbers. Precisely, the correspondence is a nonnegative rational number corresponds to the fractional ideal which is all integral multiples of that number.

Example. *Let K be a number field. Any ideal of $\mathcal{O}_K$ is a fractional ideal. If $a \in K$, then $a\mathcal{O}_K$ is also a fractional ideal.*

Example. *Let K be a number field. Then K is* not *a fractional ideal of $\mathcal{O}_K$, even though it satisfies the properties of being closed under addition and multiplication by elements of $\mathcal{O}_K$, because there is no element a of $\mathcal{O}_K$ such that $aK \subseteq \mathcal{O}_K$. A similar non-example (for the same reason), but perhaps less trivial, is the ring $\mathbb{Z}[\frac{1}{2}] = \left\{\frac{a}{2^k} : a, k \in \mathbb{Z}\right\}$.*

One formally defines the product of fractional ideals in the same way as for ideals: $\mathcal{I}\mathcal{J} = \{i_1j_1 + i_2j_2 + \cdots i_kj_k : i_m \in \mathcal{I}, j_n \in \mathcal{J}\}$. The point is every (non-zero) fractional ideal is invertible.

Exercise 12.1. *Let $\mathcal{I} = (n)$ be a non-zero ideal of $\mathbb{Z}$. Check the fractional ideal $\mathcal{I}^{-1} = \frac{1}{n}\mathbb{Z}$ is indeed the inverse of $\mathcal{I}$, i.e., $\mathcal{I}\mathcal{I}^{-1} = (1) = \mathbb{Z}$. Similarly, for any number field K and any non-zero principal ideal $\mathcal{I} = (\alpha)$ of $\mathcal{O}_K$, show $\alpha^{-1}\mathcal{O}_K$ is the inverse of $\mathcal{I}$, i.e., $\mathcal{I}\mathcal{I}^{-1} = (1) = \mathcal{O}_K$.*

Exercise 12.2. *Let K be a number field. Show the principal fractional ideals of $\mathcal{O}_K$ correspond to the elements of K, up to units.*

In fact, the product of principal (fractional) ideals corresponds to the product of elements of K (up to units). In the case $K = \mathbb{Q}$, $\mathrm{Frac}(\mathcal{O}_K)$ is essentially $\mathbb{Q}_{>0}$ the positive rational numbers, which forms a group under multiplication. More generally we have the following.

Theorem 12.5. $\mathrm{Frac}(\mathcal{O}_K)$ *is an abelian group under multiplication, and $\mathcal{O}_K$ is the identity element.*

Exercise 12.3. *Check that $\mathcal{O}_K$ is the identity element of* $\mathrm{Frac}(\mathcal{O}_K)$*, i.e., if $\mathcal{I} \in \mathrm{Frac}(\mathcal{O}_K)$, show $\mathcal{O}_K \cdot \mathcal{I} = \mathcal{I}$.*

Proof. First note that the product of two fractional ideals $\mathcal{I}$ and $\mathcal{J}$ is again a fractional ideal. This is because there exist $a, b \in \mathcal{O}_K$ such that $a\mathcal{I}$ and $b\mathcal{J}$ are ideals of $\mathcal{O}_K$. Then $ab\mathcal{I}\mathcal{J}$ is just the product of two ordinary ideals $a\mathcal{I}$ and $b\mathcal{J}$ of $\mathcal{O}_K$, and thus itself an ideal of $\mathcal{O}_K$. Hence multiplication is a binary operation on $\mathrm{Frac}(\mathcal{O}_K)$.

One formally checks from the definition that multiplication is associative and commutative. This is straightforward and I will not write it down.

The exercise above shows $\mathcal{O}_K$ is a multiplicative identity, so it suffices to show every element has an inverse. Let $\mathcal{I}$ be an (ordinary) ideal of $\mathcal{O}_K$. Define $\mathcal{I}^{-1} = \{a \in K : a\mathcal{I} \subseteq \mathcal{O}_K\}$. Then it is easy to see that $\mathcal{I}^{-1}\mathcal{I} \subseteq \mathcal{O}_K$. It takes a little more work to show $\mathcal{I}^{-1}\mathcal{I} = \mathcal{O}_K$, and in the interest of time I will omit it, though it is nothing too difficult (the proof is about 1–1$\frac{1}{2}$ pages, see any text on Algebraic Number Theory). Roughly, one can use a descent-type argument to reduce the proof to the case where $\mathcal{I}$ maximal. It easy to see $\mathcal{I}^{-1} \not\subseteq \mathcal{O}_K$ (exercise below), and therefore $\mathcal{I}^{-1}\mathcal{I}$ is strictly larger than $\mathcal{I}$. But then the maximality of I implies $\mathcal{I}^{-1}\mathcal{I}$ must be $\mathcal{O}_K$. □

Corollary 12.6. *Let $\mathcal{I}$, $\mathcal{J}$ be ideals of $\mathcal{O}_K$. Then $\mathcal{J}|\mathcal{I} \iff \mathcal{I} = \mathcal{J}\mathcal{J}'$ for some (ordinary) ideal $\mathcal{J}'$ of $\mathcal{O}_K$.*

Proof. Let $\mathcal{J}'$ be the fractional ideal $\mathcal{J}' = \mathcal{J}^{-1}\mathcal{I}$. Then $\mathcal{I} = \mathcal{J}\mathcal{J}'$, and the corollary then reads $\mathcal{J}|\mathcal{I} \iff \mathcal{J}'$ is an ordinary ideal of $\mathcal{O}_K$, i.e., if and only if $\mathcal{J}' = \mathcal{J}^{-1}\mathcal{I} \subseteq \mathcal{O}_K$. Multiplying both sides by $\mathcal{J}$, this is true if and only if $\mathcal{I} \subseteq \mathcal{J}\mathcal{O}_K = \mathcal{J}$, which was the definition of $\mathcal{J}|\mathcal{I}$. □

This completes the proof of Proposition 12.1, and hence Theorem 12.2.

Corollary 12.7. *Let $\mathcal{I}, \mathcal{J}, \mathcal{J}'$ be ideals of $\mathcal{O}_K$. If $\mathcal{I}\mathcal{J} = \mathcal{I}\mathcal{J}'$, then $\mathcal{J} = \mathcal{J}'$.*

Proof. Multiply by $\mathcal{I}^{-1}$. □

This completes the proof of Theorem 12.3.

Exercise 12.4. *Let $\mathcal{I}, \mathcal{J}$ be ideals of $\mathcal{O}_K$. Then $\mathcal{J}|\mathcal{I} \iff \mathcal{J} \supseteq \mathcal{I} \iff \mathcal{J}^{-1} \subseteq \mathcal{I}^{-1}$. (Hint: it's easy if you use Theorem 12.5 to multiply by inverses like in the corollary above.) Note when $\mathcal{J} = \mathcal{O}_K$, this says $\mathcal{I}^{-1} \supseteq \mathcal{O}_K$.*

Corollary 12.8. $\mathrm{Prin}(\mathcal{O}_K)$ *is a subgroup of* $\mathrm{Frac}(\mathcal{O}_K)$.

Proof. Since it's a subset of $\mathrm{Frac}(\mathcal{O}_K)$ is suffices to check it's closed under multiplication and inverses. Suppose $\mathcal{I}, \mathcal{J} \in \mathrm{Prin}(\mathcal{O}_K)$. Then $a\mathcal{I} = (b)$ and $c\mathcal{J} = (d)$ for some $a, b, c, d \in \mathcal{O}_K$ where $a, c \neq 0$. In other words, $\mathcal{I}$ is all integer $(\mathcal{O}_K)$ multiples of $\frac{b}{a}$ and $\mathcal{J}$ is the integer multiples of $\frac{d}{c}$. Hence their product is the integer multiples of $\frac{bd}{ac}$, which is again a principal fractional ideal.

It is closed under inverses, because $\mathcal{I}^{-1}$ is just the set of all integer multiples of $\frac{a}{b}$ (proof same as for Exercise 12.1), which is again a prinicipal fractional ideal. □

It is simple result from group theory that if A is an abelian group and B is a subgroup, the set of cosets A/B forms an abelian group, called the quotient group. I will assume that you know this, or are willing to take it for granted. We won't really use the group structure anyway, but we will use the term group.

Definition 12.9. *Let K be a number field. The* **class group** *of K (or of $\mathcal{O}_K$) is defined to be the quotient group* $\mathrm{Frac}(\mathcal{O}_k)/\mathrm{Prin}(\mathcal{O}_K)$*, and denoted $\mathcal{C}l_K$ or $\mathcal{C}l(\mathcal{O}_K)$, or possibly $\mathcal{C}l(K)$ or $\mathcal{C}l_{\mathcal{O}_K}$, or maybe even H_K or $H(K)$. The* **class number** *of K (or of $\mathcal{O}_K$) is $h(K) = h_K = \#\mathcal{C}l_K$.*

The class group has been one of the fundamental objects of study in number theory since Gauss developed the theory of binary quadratic forms. Note that the class group is trivial, i.e., the class number is 1, if and only if every fractional ideal of $\mathcal{O}_K$ is principal. It is easy to see that this happens if and only if every ideal of $\mathcal{O}_K$ is principal, since the inverses of prinicipal ideals are principal fractional ideals, and the inverses of nonprincipal ideals are nonprincipal fractional ideals. Hence $h_K = 1$ if and only if $\mathcal{O}_K$ has unique factorization.

In fact the class group measures in a very precise way, exactly just how much unique factorization can fail in $\mathcal{O}_K$, and these notions have been studied over the past 50 years. For instance, in 1960 Carlitz showed that every irreducible factorization of an element α in $\mathcal{O}_K$ has the same length (number of irreducible factors, with multiplicity) if and only if $h_K \leq 2$. The quantitative study of the relation with the class group of $\mathcal{O}_K$ and the non-uniqueness of factorization in $\mathcal{O}_K$ for some reason is not addressed in most number theory texts, but for a good account of this theory, see Chapter 9 of Narkiewicz's *Elementary and Analytic Theory of Algebraic Numbers*.

One of the major problems of algebraic number theory is understanding the class group of a number field. In particular, using Minkowski's theorem (see Chapter 8, the second proof) one can provide a bound on the class number, which is sufficient to determine the class number in special cases, but not in general. On the other hand, Dirichlet proved an exact formula for the class number of quadratic fields in terms of his L-functions, but again this is not always computationally feasible enough to use to pin down the class number exactly. Indeed if one looks at a table of class numbers just for imaginary quadratic fields, there is no apparent pattern, so one can not hope for an elementary formula.

I briefly discussed the problem of determining which quadratic fields have class number 1 in the section on PIDs, since these notions are equivalent, so this should give you some idea of the state of things. Recall in particular that there are 9 imaginary quadratic fields $K = \mathbb{Q}(\sqrt{-d})$ such that $\mathcal{O}_K$ is a PID, i.e., has class number 1. Using Minkowski's bound it is easy to check that these 9 fields found by Gauss all have class number 1, but it is much harder to show that there are no others. In fact these questions are related to difficult problems in the theory of elliptic curves. In 2004, Watkins determined all imaginary quadratic fields with class number n for $n \leq 100$ (there are finitely many). However, a s mentioned before, it is not even known if there are infinitely many real quadratic fields with class number 1, but it is conjectured that about 75% do.

12.3 Equivalence classes

Definition 12.10. *Let K be a number field and $\mathcal{I}, \mathcal{I}' \in \mathrm{Frac}(\mathcal{O}_K)$. We say $\mathcal{I}$ and $\mathcal{I}'$ are* **equivalent**, *and write $\mathcal{I} \sim \mathcal{I}'$, if $\mathcal{I}' = \mathcal{J}\mathcal{I}$ for some $\mathcal{J} \in \mathrm{Prin}(\mathcal{O}_K)$.*

In other words, with this notion of equivalence, the class group is the group of equivalence classes in $\mathrm{Frac}(\mathcal{O}_K)$. In other words, $\mathcal{I}' \sim \mathcal{I}$ means $\mathcal{I}' = \alpha\mathcal{I}$ for some $\alpha \in K$ (by Exercise 12.2), i.e., equivalent fractional ideals just differ by scalars.

Now we can relate this notion with the book's geometric notion of the "shape" of an ideal. If $K = \mathbb{Q}(\sqrt{-d})$ is an imaginary quadratic field, then $\mathcal{O}_K$ is a lattice in $\mathbb{C}$. Similarly, any fractional or ordinary ideal of $\mathcal{O}_K$ will be a lattice in $\mathbb{C}$, and two of them will have the same shape if an only if they differ by scalars (remember, a real number scalars would just scale a lattice symmetrically by a certain amount, and a complex number scalar will involve a rotation). Hence two (fractional or ordinary) ideals if and only if they are equivalent.

The following is an immediate consequence of the definition of fractional ideals and equivalence, but worth pointing out.

Lemma 12.11. *Let K be a number field. If $\mathcal{I} \in \mathrm{Frac}(\mathcal{O}_K)$, then $\mathcal{I} \sim \mathcal{I}'$ where $\mathcal{I}'$ is an ordinary ideal of $\mathcal{O}_K$.*

Proof. By definition $\mathcal{I}' = a\mathcal{I}$ is an ordinary ideal of $\mathcal{O}_K$ for some $a \in \mathcal{O}_K$. Since $\mathcal{I}' = (a)\mathcal{I}$, $\mathcal{I}' \sim \mathcal{I}$. □

12.4 Primes of the form $x^2 + 5y^2$

One of our motivating questions this semester was: which numbers are of the form $x^2 + ny^2$? By Brahmagupta's composition law, this essentially reduces to the question of which primes are of the form $x^2 + ny^2$, which has a much cleaner answer (cf. Chapter 6 for $n = 1$). We have dealt with the cases $n = 1, 2, 3$ by using unique factorization in the rings $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\zeta_3] = \mathcal{O}_{\mathbb{Q}(\sqrt{-3}}$. By the exercise below, we can reduce the $n = 4$ case to the $n = 1$ case because $x^2 + 4y^2 = x^2 + (2y)^2$.

Exercise 12.5. *Use Fermat's 2 square theorem to determine the primes of the form $x^2 + 4y^2$ (Exercise 12.8.1).*

Hence the next logical case is $n = 5$. Unfortunately, the same approach does not work because $\mathbb{Z}[\sqrt{-5}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ does not have unique factorization.

Lemma 12.12. *The class number $h_{\mathbb{Q}(\sqrt{-5})} = 2$, and representatives for the class group are* (1) *and* $(2, 1 + \sqrt{-5})$.

Proof. First note the class number is not 1, i.e., $\mathbb{Z}[\sqrt{-5}]$ is not a PID, since $\mathfrak{p} = (2, 1 + \sqrt{-5})$ is not a principal ideal. The argument is the same as for the ideal $(2, 1 + \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-3}]$. Here is one argument.

Let α be an non-zero element of $\mathfrak{p}$ of smallest possible norm. Recall the $N(a+b\sqrt{-5}) = a^2+5b^2$, so the only elements of norm less than $4 = N(2)$ in $\mathbb{Z}[\sqrt{-5}]$ are ± 1. Note $1 \in \mathfrak{p}$ (which is equivalent to $-1 \in \mathfrak{p}$) means

$$1 = 2(a + b\sqrt{-5}) + (1 + \sqrt{-5})(c + d\sqrt{-5}) = 2a + 2b\sqrt{-5} + c - 5d + (c + d)\sqrt{-5}$$

Looking at real and imaginary parts we have $1 = 2a + c - 5d$ and $0 = 2b + c + d$, but the first means $c \not\equiv d \bmod 2$ and the second means $c \equiv d \bmod 2$ which is impossible. Hence $\alpha = \pm 2$. If $\mathfrak{p}$ were principal, it would have to be generated by α, which it is not, since $1 + \sqrt{-5} \notin (\alpha)$.

Hence the class number is at least 2. To show it equals 2, we want to show that if $\mathcal{I}$ is any non-principal fractional ideal of $\mathbb{Z}[\sqrt{-5}]$ is equivalent to $(2, \sqrt{-5})$. It in fact suffices to show this for $\mathcal{I}$ an ordinary non-prinicpal ideal, since $\mathcal{I}$ is equivalent to an ordinary ideal by the previous lemma.

Let α be a non-zero element of $\mathcal{I}$ of minimal norm. Since $\mathcal{I}$ is not principal, there exists an element $\beta \in \mathcal{I}$ such that $\beta \notin (\alpha)$. Consider the rectangle (p. 232 of Stillwell) with corners 0, α,

$\sqrt{-5}\alpha$ and $(1+\sqrt{-5})\alpha$. By adding appropriate an appropriate multiple of α to β, we may assume β lies in this rectangle. In fact, by replacing β with $\alpha-\beta$ if necessary, we may assume β is in the "left half" of the rectangle. Similarly, replacing β with $(1+\sqrt{-5})\alpha-\beta$ if necessary, we may assume β is in the "lower left quadrant" of the rectangle. This means 2β will still be contained in the rectangle. In particular $N(2\beta) \leq N((1+\sqrt{-5})\alpha)$, since the norm is just the square of the distance from the origin. But this means $N(\beta) \leq N(\alpha)$ since $N(2) = N(1+\sqrt{-5}) = 4$. Then by the assumption that $N(\alpha)$ is minimal, we conclude $N(\alpha) = N(\beta)$. Then the only possibility for β is $\beta = \frac{1+\sqrt{-5}}{2}\alpha$ (any other point in the "lower left quadrant" of the rectangle has smaller norm).

Now we claim $\mathcal{I} = (\alpha, \beta)$. If not, take $\gamma \in \mathcal{I}$ but not in (α, β). Applying the same argument above for γ in place of β, we may assume γ is in the lower left quadrant, and conclude that $\gamma = \beta = \frac{1+\sqrt{-5}}{2}$, a contradiction. Hence

$$\mathcal{I} = (\alpha, \beta) = (\alpha, \frac{1+\sqrt{-5}}{2}\alpha) \sim 2(\alpha, \frac{1+\sqrt{-5}}{2}\alpha) = (2\alpha, (1+\sqrt{-5})\alpha) \sim (2, 1+\sqrt{-5}).$$

□

Example. *Let* $\mathfrak{q} = (3, 1+\sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}]$. *As above, one may show* $\mathfrak{q}$ *is not principal. Thus* $\mathfrak{q} \sim \mathfrak{p} = (2, 1+\sqrt{-5})$. *To see this directly, note that*

$$(1+\sqrt{-5})\mathfrak{p} = (2(1+\sqrt{-5}), -4+2\sqrt{-5}) = (2(1+\sqrt{-5}), 6) \sim (1+\sqrt{-5}, 3).$$

The only non-obvious equality is the middle one, but this is true because $6 = 2(1+\sqrt{-5}) - (-4+\sqrt{-5}) \in (2(1+\sqrt{-5}), -4+2\sqrt{-5})$. *Hence* $(2(1+\sqrt{-5}), -4+2\sqrt{-5}) \supseteq (2(1+\sqrt{-5}), 6)$. *Writing* $-4+\sqrt{-5} = 2(1+\sqrt{-5}) - 6$, *we see that* $(2(1+\sqrt{-5}), -4+2\sqrt{-5}) \subseteq (2(1+\sqrt{-5}), 6)$ *also holds.*

Let us take for granted the following basic facts on norms of ideals, which I may prove formally next semester.

Proposition 12.13. *Let* K *be a number field and* $\mathcal{I}, \mathcal{J}$ *be ideals of* $\mathcal{O}_K$. *Then* $N(\mathcal{I}\mathcal{J}) = N(\mathcal{I})N(\mathcal{J})$. *Further if* $K = \mathbb{Q}(\sqrt{d})$ *is a quadratic field (real or imaginary) and* $a \in \mathcal{O}_K$, *then* $N(a) = N((a))$, *i.e., the norm of the element* a *(as previously defined* $N(a) = a\overline{a}$*) equals the norm of principal ideal* (a).

The multiplicativity is essentially just a standard ring isomorphism theorem, which says $(\mathcal{O}_K/\mathcal{I}) \simeq (\mathcal{O}_K/\mathcal{I}\mathcal{J})/(\mathcal{I}/\mathcal{I}\mathcal{J})$. The cardinality of the quotient on the left is $N(\mathcal{I})$, while that on the right is $N(\mathcal{I}\mathcal{J})/N(\mathcal{J})$.

Theorem 12.14. *Let* $p \in \mathbb{N}$ *be prime. Then* $p = x^2+5y^2$ *for some* $x, y \in \mathbb{Z} \iff p \equiv 1, 9 \bmod 20$.

Proof. ($\Rightarrow$) Suppose $p = x^2+5y^2$. It is clear $p \neq 2, 5$, so p mod 20 must be relatively prime to 2 and 5. The squares mod 20 are $0, 1, 4, 5, 9, 16$. Thus the only values of x^2+5y^2 that are relatively prime to 2 and 5 are 1 and 9.

($\Leftarrow$) Suppose $p \equiv 1, 9 \bmod 20$. By quadratic reciprocity, we see that $\left(\frac{-5}{p}\right) = 1$, i.e., $p | m^2+5 = (m+\sqrt{-5})(m-\sqrt{-5})$ for some $m \in \mathbb{Z}$. On the other hand $p \nmid m \pm \sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$ since $\frac{m}{p} \pm \frac{\sqrt{-5}}{p} \notin \mathbb{Z}[\sqrt{-5}]$. In other word, the principal ideal $(p) | (m+\sqrt{-5})(m-\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$ but $(p) \nmid (m+\sqrt{-5})$ and $(p) \nmid (m-\sqrt{-5})$ (these are denote principal ideals). Hence (p) is not a prime ideal of $\mathbb{Z}[\sqrt{-5}]$.

Now by the prime ideal factorization theorem, (p) factors into prime ideals $(p) = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$. Looking at norms, we see $N(\mathfrak{p}_1)N(\mathfrak{p}_2)\cdots N(\mathfrak{p}_r) = N((p)) = N(p) = p^2$. Since each $N(\mathfrak{p}_i) > 1$ (otherwise $\mathfrak{p}_i = \mathcal{O}_K$), we must have $r = 2$ and $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$.

Consider $\mathfrak{p}_1$. Either it is principal or not. If it is, say $\mathfrak{p}_1 = (a + b\sqrt{-5})$. Then $N(\mathfrak{p}_1) = p$ means $N(a + b\sqrt{-5}) = a^2 + 5b^2 = p$, and we are done.

If not, then $\mathfrak{p}_1 \sim (2, 1 + \sqrt{-5})$ so $\mathfrak{p}_1 = \alpha(2, 1 + \sqrt{-5})$ for some $\alpha \in K$. Writing $\alpha = \frac{a}{b} + \frac{c}{d}\sqrt{-5}$ with $a, b, c, d \in \mathbb{Z}$, we see $2\alpha, (1 + \sqrt{-5})\alpha \in \mathcal{O}_K$ implies either $\alpha \in \mathcal{O}_K$ ($b = d = 1$) or $\alpha = \frac{1+\sqrt{-5}}{2}\mathcal{O}_K$ ($b = d = 2$ and $a \equiv c \bmod 2$). However one easily checks that $\frac{1+\sqrt{-5}}{2}(2, 1 + \sqrt{-5}) = (1 + \sqrt{-5}, -4 + 2\sqrt{-5}) = (1 + \sqrt{-5}, 2)$, so without loss of generality we may assume $\alpha \in \mathcal{O}_K$. But then $\mathfrak{p}_1 = (\alpha)(2, 1+\sqrt{-5})$ is a factorization of $\mathfrak{p}_1$ into ideals of $\mathcal{O}_K$. Since $\mathfrak{p}_1$ is prime (maximal), this factorization must be trivial, i.e., we must have $(\alpha) = \mathbb{Z}[\sqrt{-5}]$. But then $N(\mathfrak{p}_1) = N((2, 1+\sqrt{-5})) = 2$ (as computed in your homework), which is not $\equiv 1, 9 \bmod 20$. Hence $\mathfrak{p}_1$ must be principal. □

Remarks.

(1) While we did not explicitly use *uniqueness* of prime factorization, we used the *existence*, together with the explicit structure of the class group of $\mathbb{Z}[\sqrt{-5}]$. Both of these inputs rely on the fact that $\mathrm{Frac}(\mathcal{O}_K)$ is a group, which was our key to proving the uniqueness. Additionally, one may want to use uniqueness in to prove the fact that the norm is multiplicative.

(2) An alternative proof that does not rely on the unproven norm facts is in the last section of Stillwell. However, I opted for the above proof because (i) it is much simpler, (ii) it illustrates the usefulness of norms of ideals, (iii) it is more typical and enlightening of the applications of ideal factorization, and (iv) it is much more similar to the arguments we made before for $\mathbb{Z}$, $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$.

(3) Here is an alternative way to compute $N((2, 1 + \sqrt{-5}))$. Since $(2, 1 + \sqrt{-5})$ divides (2), we must have $(2) = (2, 1 + \sqrt{-5})\mathfrak{p}$ for some proper ideal $\mathfrak{p}$ (in fact $\mathfrak{p} = (2, 1 + \sqrt{-5})$. Then $4 = N((2)) = N((2, 1 + \sqrt{-5}))N(\mathfrak{p})$ which implies $N((2, 1 + \sqrt{-5})) = N(\mathfrak{p}) = 2$. You are free to use the multiplicativity of the norm on the final exam.

To close, let us revisit the example of the non-unique factorization

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

in $\mathbb{Z}[\sqrt{-5}]$. In terms of principal ideals, this says

$$\overset{36}{(6)} = \overset{4}{(2)}\overset{9}{(3)} = (1 + \overset{6}{\sqrt{-5}})(1 - \overset{6}{\sqrt{-5}}) \, .$$

Here the numbers above the ideals are the norms of each ideal. So in some sense, this non-unique factorization is like the non-unique factorization of 36 into two non-irreducibles of $\mathbb{Z}$.

Let $\mathfrak{p} = (2, 1 + \sqrt{-5})$, $\mathfrak{q} = (3, 1 + \sqrt{-5})$ and $\overline{\mathfrak{q}} = (3, 1 - \sqrt{-5})$. We have already computed that $N(\mathfrak{p}) = 2$. Similarly one computes $N(\mathfrak{q}) = N(\overline{\mathfrak{q}}) = 3$. If the norm of an ideal is prime in $\mathbb{Z}$, that means the ideal itself must be a prime ideal (by multiplicativity), so $\mathfrak{p}, \mathfrak{q}, \overline{\mathfrak{q}}$ are all prime ideals. Note that $1 - \sqrt{-5} = 2 - (1 + \sqrt{-5}) \in \mathfrak{p}$ (this is why we don't consider $\overline{\mathfrak{p}}$, since $\overline{\mathfrak{p}} = \mathfrak{p}$), so $\mathfrak{p}|(2)$, $\mathfrak{p}|(1 + \sqrt{-5})$ and $\mathfrak{p}|(1 - \sqrt{-5})$. Similarly, $\mathfrak{q}|(3)$, $\mathfrak{q}|(1 + \sqrt{-5})$, and $\overline{\mathfrak{q}}|(3)$, $\overline{\mathfrak{q}}|(1 - \sqrt{-5})$. One can easily check that $\mathfrak{q} \neq \overline{\mathfrak{q}}$, so we have 2 divisors of the ideal (3). Since $N(\mathfrak{q})N(\overline{\mathfrak{q}}) = N((3))$, there can't be any other divisors. This proves

$$(3) = \mathfrak{q}\overline{\mathfrak{q}}$$

(without explicitly doing the calculation of the product on the right, though one could obviously also do that). Similarly we have

$$(1+\sqrt{-5}) = \mathfrak{p}\mathfrak{q}, \;\; (1-\sqrt{-5}) = \mathfrak{p}\overline{\mathfrak{q}}.$$

Finally, to check

$$(2) = \mathfrak{p}^2$$

we can do the same argument of norms, ones we check that $2 \in \mathfrak{p}^2$ so we know that $\mathfrak{p}^2|(2)$. An alternative argument is the following—since $\mathcal{C}l(\mathbb{Z}[\sqrt{-5}])$ has order 2, any ideal squared must be equivalent to (1), i.e., the square of any ideal is principal. In particular $\mathfrak{p}^2$ is principal, and since it has norm 4 it must be generated by an element of $\mathbb{Z}[\sqrt{-5}]$ of norm 4—but the only such elements are ± 2. Thus the non-unique factorization is resolved in terms of ideals as

$$(6) = (2)(3) = \mathfrak{p}^2\mathfrak{q}\overline{\mathfrak{q}} = (\mathfrak{p}\mathfrak{q})(\mathfrak{p}\overline{\mathfrak{q}}) = (1+\sqrt{-5})(1-\sqrt{-5}).$$

Another way to look at this example, more in line with Kummer's original ideas of adding ideal numbers to the ring, is the following. Somehow $\mathfrak{p}$ should be correspond to the "ideal number" $\alpha = \frac{1+\sqrt{-5}}{3}$. The reason for this, is that if $\mathfrak{p}$ were a principal ideal (α), both 2 and $1+\sqrt{-5}$ would have to be multiples of α. Since $\mathfrak{p} \neq \mathbb{Z}[\sqrt{-5}]$, $\alpha \neq 1$, and a reasonable choice would be $\alpha = \frac{1+\sqrt{-5}}{3}$. Then $\alpha(1-\sqrt{-5}) = 2$ and $3\alpha = 1+\sqrt{-5}$. Similarly, we see that $\mathfrak{q}$ is like the "ideal number" $\beta = \frac{1+\sqrt{-5}}{2}$ and $\overline{\mathfrak{q}}$ is like the "ideal number" $\overline{\beta} = \frac{1-\sqrt{-5}}{2}$. In terms of $\alpha, \beta, \overline{\beta}$, we can resolve the factorization

$$\begin{aligned} 2 \cdot 3 &= \frac{1+\sqrt{-5}}{3}(1-\sqrt{-5}) \cdot (1+\sqrt{-5})\frac{1-\sqrt{-5}}{2} \\ &= \frac{1+\sqrt{-5}}{3}\frac{1-\sqrt{-5}}{2}(1+\sqrt{-5}) \cdot (1-\sqrt{-5}) = (1+\sqrt{-5}) \cdot (1-\sqrt{-5}) \end{aligned}$$

in the ring $\mathbb{Z}[\alpha, \beta, \overline{\beta}]$. The technical problem is that $\alpha, \beta, \overline{\beta}$ are not algebraic integers—for instance $\beta - \beta^2 = \frac{1}{2}$. This this ring has infinite degree over $\mathbb{Z}$ (a $\mathbb{Z}$-basis for the ring is infinite) and this factorization, while resolved, is in fact made trivial, because 2, 3 and 6 are all units in this ring.

There are, however, ways to recover unique factorization in $\mathbb{Z}[\sqrt{-5}]$ (without trivializing the problems) by passing to the ring of integers of a larger number field. For instance every element of $\mathbb{Z}[\sqrt{-5}]$ factors uniquely into irreducibles in the ring of integers of $K = \mathbb{Q}(\sqrt{-5}, \sqrt{2})$. However, other difficulties arise with this approach, which I've alluded to before: (1) in general, how do you find the appropriate number field K to work in, (2) how do you determine its ring of integers $\mathcal{O}_K$ and irreducible elements of $\mathcal{O}_K$, (3) this ring $\mathcal{O}_K$ itself may not have unique factorization. (While we can guarantee any element of the smaller ring factors uniquely into irreducibles in $\mathcal{O}_K$, this may not be true for every element of $\mathcal{O}_K$). Thus the approach via Dedekind's ideal theory is generally the most satisfactory.