Chapter 3

Dedekind Domains

3.1 The Definition and Some Basic Properties

We identify the natural class of integral domains in which unique factorization of ideals is possible.

3.1.1 Definition

A Dedekind domain is an integral domain $A$ satisfying the following three conditions:

1. $A$ is a Noetherian ring;
2. $A$ is integrally closed;
3. Every nonzero prime ideal of $A$ is maximal.

A principal ideal domain satisfies all three conditions, and is therefore a Dedekind domain. We are going to show that in the $AKLB$ setup, if $A$ is a Dedekind domain, then so is $B$, a result that provides many more examples and already suggests that Dedekind domains are important in algebraic number theory.

3.1.2 Proposition

In the $AKLB$ setup, $B$ is integrally closed, regardless of $A$. If $A$ is an integrally closed Noetherian ring, then $B$ is also a Noetherian ring, as well as a finitely generated $A$-module.

Proof. By (1.1.6), $B$ is integrally closed in $L$, which is the fraction field of $B$ by (2.2.8). Therefore $B$ is integrally closed. If $A$ is integrally closed, then by (2.3.8), $B$ is a submodule of a free $A$-module $M$ of rank $n$. If $A$ is Noetherian, then $M$, which is isomorphic to the direct sum of $n$ copies of $A$, is a Noetherian $A$-module, hence so is the submodule $B$. An ideal of $B$ is, in particular, an $A$-submodule of $B$, hence is finitely generated over $A$ and therefore over $B$. It follows that $B$ is a Noetherian ring. ♣

3.1.3 Theorem

In the $AKLB$ setup, if $A$ is a Dedekind domain, then so is $B$. In particular, the ring of algebraic integers in a number field is a Dedekind domain.
CHAPTER 3. DEDEKIND DOMAINS

Proof. In view of (3.1.2), it suffices to show that every nonzero prime ideal $Q$ of $B$ is maximal. Choose any nonzero element $x$ of $Q$. Since $x \in B$, $x$ satisfies a polynomial equation

$$x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0 = 0$$

with the $a_i \in A$. If we take the positive integer $m$ as small as possible, then $a_0 \neq 0$ by minimality of $m$. Solving for $a_0$, we see that $a_0 \in Bx \cap A \subseteq Q \cap A$, so the prime ideal $P = Q \cap A$ is nonzero, hence maximal by hypothesis. By Section 1.1, Problem 6, $Q$ is maximal. ♣

Problems For Section 3.1

This problem set will give the proof of a result to be used later. Let $P_1, P_2, \ldots, P_s$, $s \geq 2$, be ideals in a ring $R$, with $P_1$ and $P_2$ not necessarily prime, but $P_3, \ldots, P_s$ prime (if $s \geq 3$). Let $I$ be any ideal of $R$. The idea is that if we can avoid the $P_j$ individually, in other words, for each $j$ we can find an element in $I$ but not in $P_j$, then we can avoid all the $P_j$ simultaneously, that is, we can find a single element in $I$ that is in none of the $P_j$. The usual statement is the contrapositive of this assertion.

Prime Avoidance Lemma

With $I$ and the $P_i$ as above, if $I \subseteq \cup_{i=1}^s P_i$, then for some $i$ we have $I \subseteq P_i$.

1. Suppose that the result is false. Show that without loss of generality, we can assume the existence of elements $a_i \in I$ with $a_i \in P_i$ but $a_i \notin P_1 \cup \cdots \cup P_{i-1} \cup P_{i+1} \cup \cdots \cup P_s$.

2. Prove the result for $s = 2$.

3. Now assume $s > 2$, and observe that $a_1a_2\cdots a_{s-1} \in P_1 \cap \cdots \cap P_{s-1}$, but $a_s \notin P_1 \cup \cdots \cup P_{s-1}$. Let $a = (a_1 \cdots a_{s-1}) + a_s$, which does not belong to $P_1 \cup \cdots \cup P_{s-1}$, else $a_s$ would belong to this set. Show that $a \in I$ and $a \notin P_1 \cup \cdots \cup P_s$, contradicting the hypothesis.

3.2 Fractional Ideals

Our goal is to establish unique factorization of ideals in a Dedekind domain, and to do this we will need to generalize the notion of ideal. First, some preliminaries.

3.2.1 Products of Ideals

Recall that if $I_1, \ldots, I_n$ are ideals, then their product $I_1 \cdots I_n$ is the set of all finite sums $\sum_i a_{1i}a_{2i} \cdots a_{ni}$, where $a_{ki} \in I_k$, $k = 1, \ldots, n$. It follows from the definition that $I_1 \cdots I_n$ is an ideal contained in each $I_j$. Moreover, if a prime ideal $P$ contains a product $I_1 \cdots I_n$ of ideals, then $P$ contains $I_j$ for some $j$. 
3.2. **FRACTIONAL IDEALS**

3.2.2 **Proposition**

If $I$ is a nonzero ideal of the Noetherian integral domain $R$, then $I$ contains a product of nonzero prime ideals.

**Proof.** Assume the contrary. If $S$ is the collection of all nonzero ideals that do not contain a product of nonzero prime ideals, then, as $R$ is Noetherian, $S$ has a maximal element $J$, and $J$ cannot be prime because it belongs to $S$. Thus there are elements $a, b \in R$ such that $a \notin J$, $b \notin J$, and $ab \in J$. By maximality of $J$, the ideals $J + Ra$ and $J + Rb$ each contain a product of nonzero prime ideals, hence so does $(J + Ra)(J + Rb) \subseteq J + Rab = J$. This is a contradiction. (Notice that we must use the fact that a product of nonzero ideals is nonzero, and this is where the hypothesis that $R$ is an integral domain comes in.) ♣

3.2.3 **Corollary**

If $I$ is an ideal of the Noetherian ring $R$ (not necessarily an integral domain), then $I$ contains a product of prime ideals.

**Proof.** Repeat the proof of (3.2.2), with the word “nonzero” deleted. ♣

Ideals in the ring of integers are of the form $n\mathbb{Z}$, the set of multiples of $n$. A set of the form $(3/2)\mathbb{Z}$ is not an ideal because it is not a subset of $\mathbb{Z}$, yet it behaves in a similar manner. The set is closed under addition and multiplication by an integer, and it becomes an ideal of $\mathbb{Z}$ if we simply multiply all the elements by 2. It will be profitable to study sets of this type.

3.2.4 **Definitions**

Let $R$ be an integral domain with fraction field $K$, and let $I$ be an $R$-submodule of $K$. We say that $I$ is a **fractional ideal** of $R$ if $rI \subseteq R$ for some nonzero $r \in R$. We call $r$ a **denominator** of $I$. An ordinary ideal of $R$ is a fractional ideal (take $r = 1$), and will often be referred to as an **integral ideal**.

3.2.5 **Lemma**

(i) If $I$ is a finitely generated $R$-submodule of $K$, then $I$ is a fractional ideal.

(ii) If $R$ is Noetherian and $I$ is a fractional ideal of $R$, then $I$ is a finitely generated $R$-submodule of $K$.

(iii) If $I$ and $J$ are fractional ideals with denominators $r$ and $s$ respectively, then $I \cap J$, $I + J$ and $IJ$ are fractional ideals with respective denominators $r$ (or $s$), $rs$ and $rs$. [The product of fractional ideals is defined exactly as in (3.2.1).]

**Proof.**

(i) If $x_1 = a_1/b_1, \ldots, x_n = a_n/b_n$ generate $I$ and $b = b_1 \cdots b_n$, then $bI \subseteq R$.

(ii) If $rI \subseteq R$, then $I \subseteq r^{-1}R$. As an $R$-module, $r^{-1}R$ is isomorphic to $R$ and is therefore Noetherian. Consequently, $I$ is finitely generated.

(iii) It follows from the definition (3.2.4) that the intersection, sum and product of fractional ideals are fractional ideals. The assertions about denominators are proved by noting that $r(I \cap J) \subseteq rI \subseteq R$, $rs(I + J) \subseteq rI + sJ \subseteq R$, and $rsIJ = (rI)(sJ) \subseteq R$. ♣
The product of two nonzero fractional ideals is a nonzero fractional ideal, and the multiplication is associative because multiplication in $R$ is associative. There is an identity element, namely $R$, since $RI \subseteq I = 1I \subseteq RI$. We will show that if $R$ is a Dedekind domain, then every nonzero prime ideal has a multiplicative inverse, so the nonzero fractional ideals form a group.

### 3.2.6 Lemma

Let $I$ be a nonzero prime ideal of the Dedekind domain $R$, and let $J$ be the set of all elements $x \in K$ such that $xI \subseteq R$. Then $R \subseteq J$.

**Proof.** Since $RI \subseteq R$, it follows that $R$ is a subset of $J$. Pick a nonzero element $a \in I$, so that $I$ contains the principal ideal $Ra$. Let $n$ be the smallest positive integer such that $Ra$ contains a product $P_1 \cdots P_n$ of $n$ nonzero prime ideals. Since $R$ is Noetherian, there is such an $n$ by (3.2.2), and by (3.2.1), $I$ contains one of the $P_i$, say $P_1$. But in a Dedekind domain, every nonzero prime ideal is maximal, so $I = P_1$. Assuming $n \geq 2$, set $I_1 = P_2 \cdots P_n$, so that $Ra \not\subseteq I_1$ by minimality of $n$. Choose $b \in I_1$ with $b \not\in Ra$. Now $II_1 = P_1 \cdots P_n \subseteq Ra$, in particular, $Ib \subseteq Ra$, hence $Ib^{-1} \subseteq R$. (Note that $a$ has an inverse in $K$ but not necessarily in $R$.) Thus $ba^{-1} \in J$, but $ba^{-1} \not\in R$, for if so, $b \in Ra$, contradicting the choice of $b$.

The case $n = 1$ must be handled separately. In this case, $P_1 = I \supseteq Ra \supseteq P_1$, so $I = Ra$. Thus $Ra$ is a proper ideal, and we can choose $b \in R$ with $b \not\in Ra$. Then $ba^{-1} \not\in R$, but $ba^{-1}I = ba^{-1}Ra = bR \subseteq R$, so $ba^{-1} \in J$. ♠

We now prove that in (3.2.6), $J$ is the inverse of $I$.

### 3.2.7 Proposition

Let $I$ be a nonzero prime ideal of the Dedekind domain $R$, and let $J = \{x \in K : xI \subseteq R\}$. Then $J$ is a fractional ideal and $IJ = R$.

**Proof.** If $r$ is a nonzero element of $I$ and $x \in J$, then $rx \in R$, so $rJ \subseteq R$ and $J$ is a fractional ideal. Now $IJ \subseteq R$ by definition of $J$, so $IJ$ is an integral ideal. Using (3.2.6), we have $I = IR \subseteq IJ \subseteq R$, and maximality of $I$ implies that either $IJ = I$ or $IJ = R$. In the latter case, we are finished, so assume $IJ = I$.

Let $x \in J$, then $xI \subseteq IJ = I$, and by induction, $x^nI \subseteq I$ for all $n = 1, 2, \ldots$. Let $r$ be any nonzero element of $I$. Then $rx^n \in x^nI \subseteq I \subseteq R$, so $R[x]$ is a fractional ideal. Since $R$ is Noetherian, part (ii) of (3.2.5) implies that $R[x]$ is a finitely generated $R$-submodule of $K$. By (1.1.2), $x$ is integral over $R$. But $R$, a Dedekind domain, is integrally closed, so $x \in R$. Therefore $J \subseteq R$, contradicting (3.2.6). ♠

The following basic property of Dedekind domains can be proved directly from the definition, without waiting for the unique factorization of ideals.

### 3.2.8 Theorem

If $R$ is a Dedekind domain, then $R$ is a UFD if and only if $R$ is a PID.

**Proof.** Recall from basic algebra that a (commutative) ring $R$ is a PID iff $R$ is a UFD and every nonzero prime ideal of $R$ is maximal. ♠
Problems For Section 3.2

1. If $I$ and $J$ are relatively prime ideals ($I + J = R$), show that $IJ = I \cap J$. More generally, if $I_1, \ldots, I_n$ are relatively prime in pairs, show that $I_1 \cdots I_n = \cap_{i=1}^n I_i$.

2. Let $P_1$ and $P_2$ be relatively prime ideals in the ring $R$. Show that $P_r^1$ and $P_s^2$ are relatively prime for arbitrary positive integers $r$ and $s$.

3. Let $R$ be an integral domain with fraction field $K$. If $K$ is a fractional ideal of $R$, show that $R = K$.

3.3 Unique Factorization of Ideals

In the previous section, we inverted nonzero prime ideals in a Dedekind domain. We now extend this result to nonzero fractional ideals.

3.3.1 Theorem

If $I$ is a nonzero fractional ideal of the Dedekind domain $R$, then $I$ can be factored uniquely as $P_1^{n_1} P_2^{n_2} \cdots P_r^{n_r}$, where the $n_i$ are integers. Consequently, the nonzero fractional ideals form a group under multiplication.

Proof. First consider the existence of such a factorization. Without loss of generality, we can restrict to integral ideals. [Note that if $r \neq 0$ and $rI \subseteq R$, then $I = (rR)^{-1}(rI)$.] By convention, we regard $R$ as the product of the empty collection of prime ideals, so let $S$ be the set of all nonzero proper ideals of $R$ that cannot be factored in the given form, with all $n_i$ positive integers. (This trick will yield the useful result that the factorization of integral ideals only involves positive exponents.) Since $R$ is Noetherian, $S$, if nonempty, has a maximal element $I_0$, which is contained in a maximal ideal $I$. By (3.2.7), $I$ has an inverse fractional ideal $J$. Thus by (3.2.6) and (3.2.7),

$$I_0 = I_0R \subseteq I_0J \subseteqIJ = R.$$ 

Therefore $I_0J$ is an integral ideal, and we claim that $I_0 \subseteq I_0J$. For if $I_0 = I_0J$, then the last paragraph of the proof of (3.2.7) can be reproduced with $I$ replaced by $I_0$ to reach a contradiction. By maximality of $I_0$, $I_0J$ is a product of prime ideals, say $I_0J = P_1 \cdots P_r$ (with repetition allowed). Multiply both sides by the prime ideal $I$ to conclude that $I_0$ is a product of prime ideals, contradicting $I_0 \in S$. Thus $S$ must be empty, and the existence of the desired factorization is established.

To prove uniqueness, suppose that we have two prime factorizations $P_1^{n_1} \cdots P_r^{n_r} = Q_1^{t_1} \cdots Q_s^{t_s}$ where again we may assume without loss of generality that all exponents are positive. (If $P^{-n}$ appears, multiply both sides by $P^n$.) Now $P_1$ contains the product of the $P_i^{n_i}$, so by (3.2.1), $P_1$ contains $Q_j$ for some $j$. By maximality of $Q_j$, $P_1 = Q_j$, and we may renumber so that $P_1 = Q_1$. Multiply by the inverse of $P_1$ (a fractional ideal, but there is no problem), and continue inductively to complete the proof. ♦
3.3.2 Corollary

A nonzero fractional ideal \( I \) is an integral ideal if and only if all exponents in the prime factorization of \( I \) are nonnegative.

*Proof.* The “only if” part was noted in the proof of (3.3.1). The “if” part follows because a power of an integral ideal is still an integral ideal. ♣

3.3.3 Corollary

Denote by \( n_P(I) \) the exponent of the prime ideal \( P \) in the factorization of \( I \). (If \( P \) does not appear, take \( n_P(I) = 0 \).) If \( I_1 \) and \( I_2 \) are nonzero fractional ideals, then \( I_1 \supseteq I_2 \) if and only if for every prime ideal \( P \) of \( R \), \( n_P(I_1) \leq n_P(I_2) \).

*Proof.* We have \( I_2 \subseteq I_1 \) iff \( I_2I_1^{-1} \subseteq R \), and by (3.3.2), this happens iff for every \( P \), \( n_P(I_2) - n_P(I_1) \geq 0 \). ♣

3.3.4 Definition

Let \( I_1 \) and \( I_2 \) be nonzero integral ideals. We say that \( I_1 \) divides \( I_2 \) if \( I_2 = JI_1 \) for some integral ideal \( J \). Just as with integers, an equivalent statement is that each prime factor of \( I_1 \) is a factor of \( I_2 \).

3.3.5 Corollary

If \( I_1 \) and \( I_2 \) are nonzero integral ideals, then \( I_1 \) divides \( I_2 \) if and only if \( I_1 \supseteq I_2 \). In other words, for these ideals,

\[
\text{DIVIDES MEANS CONTAINS.}
\]

*Proof.* By (3.3.4), \( I_1 \) divides \( I_2 \) iff \( n_P(I_1) \leq n_P(I_2) \) for every prime ideal \( P \). By (3.3.3), this is equivalent to \( I_1 \supseteq I_2 \). ♣

3.3.6 GCD’s and LCM’s

As a nice application of the principle that divides means contains, we can use the prime factorization of ideals in a Dedekind domain to compute the greatest common divisor and least common multiple of two nonzero ideals \( I \) and \( J \), exactly as with integers. The greatest common divisor is the smallest ideal containing both \( I \) and \( J \), that is, \( I + J \). The least common multiple is the largest ideal contained in both \( I \) and \( J \), which is \( I \cap J \).

A Dedekind domain comes close to being a principal ideal domain in the sense that every nonzero integral ideal, in fact every nonzero fractional ideal, divides some principal ideal.
3.3.7 Proposition

Let $I$ be a nonzero fractional ideal of the Dedekind domain $R$. Then there is a nonzero integral ideal $J$ such that $IJ$ is a principal ideal of $R$.

**Proof.** By (3.3.1), there is a nonzero fractional ideal $I'$ such that $II' = R$. By definition of fractional ideal, there is a nonzero element $r \in R$ such that $rI'$ is an integral ideal. If $J = rI'$, then $IJ = Rr$, a principal ideal of $R$. ♣

Problems For Section 3.3

By (2.3.11), the ring $B$ of algebraic integers in $Q(\sqrt{-5})$ is $\mathbb{Z}[\sqrt{-5}]$. In Problems 1-3, we will show that $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain by considering the factorization

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \times 3.$$ 

1. By computing norms, verify that all four of the above factors are irreducible.
2. Show that the only units of $B$ are $±1$.
3. Show that no factor on one side of the above equation is an associate of a factor on the other side, so unique factorization fails.
4. Show that the ring of algebraic integers in $Q(\sqrt{-17})$ is not a unique factorization domain.
5. In $\mathbb{Z}[\sqrt{-5}]$ and $\mathbb{Z}[\sqrt{-17}]$, the only algebraic integers of norm 1 are $±1$. Show that this property does not hold for the algebraic integers in $Q(\sqrt{-3})$.

3.4 Some Arithmetic in Dedekind Domains

Unique factorization of ideals in a Dedekind domain permits calculations that are analogous to familiar manipulations involving ordinary integers. In this section, we illustrate some of the ideas.

Let $P_1, \ldots, P_n$ be distinct nonzero prime ideals of the Dedekind domain $R$, and let $J = P_1 \cdots P_n$. Let $Q_i$ be the product of the $P_j$ with $P_i$ omitted, that is,

$$Q_i = P_1 \cdots P_{i-1}P_{i+1} \cdots P_n.$$ 

(If $n = 1$, we take $Q_1 = R$.) If $I$ is any nonzero ideal of $R$, then by unique factorization, $IQ_i \supseteq IJ$. For each $i = 1, \ldots, n$, choose an element $a_i$ belonging to $IQ_i$, but not to $IJ$, and let $a = \sum_{i=1}^n a_i$.

3.4.1 Lemma

The element $a$ belongs to $I$, but for each $i$, $a \notin IP_i$. (In particular, $a \neq 0$.)

**Proof.** Since each $a_i$ belongs to $IQ_i \subseteq I$, we have $a \in I$. Now $a_i$ cannot belong to $IP_i$, for if so, $a_i \in IP_i \cap IQ_i$, which is the least common multiple of $IP_i$ and $IQ_i$ [see (3.3.6)]. But by definition of $Q_i$, the least common multiple is simply $IJ$, which contradicts the choice of $a_i$. We break up the sum defining $a$ as follows:

$$a = (a_1 + \cdots + a_{i-1}) + a_i + (a_{i+1} + \cdots + a_n).$$ (1)
If \( j \neq i \), then \( a_j \in IQ_j \subseteq IP_i \), so the first and third terms of the right side of (1) belong to \( IP_i \). Since \( a_i \notin IP_i \), as found above, we have \( a_i \notin IP_i \). ♣

In (3.3.7), we found that any nonzero ideal is a factor of a principal ideal. We can sharpen this result as follows.

### 3.4.2 Proposition

Let \( I \) be a nonzero ideal of the Dedekind domain \( R \). Then there is a nonzero ideal \( I' \) such that \( II' \) is a principal ideal \((a)\). Moreover, if \( J \) is an arbitrary nonzero ideal of \( R \), then \( I' \) can be chosen to be relatively prime to \( J \).

**Proof.** Let \( P_1, \ldots, P_n \) be the distinct prime divisors of \( J \), and choose \( a \) as in (3.4.1). Then \( a \in I \), so \((a) \subseteq I \). Since divides means contains [see (3.3.5)], \( I \) divides \((a)\), so \((a) = II' \) for some nonzero ideal \( I' \). If \( I' \) is divisible by \( P_i \), then \( I' = P_i I_0 \) for some nonzero ideal \( I_0 \), and \((a) = IP_i I_0 \). Consequently, \( a \in IP_i \), contradicting (3.4.1). ♣

### 3.4.3 Corollary

A Dedekind domain with only finitely many prime ideals is a PID.

**Proof.** Let \( J \) be the product of all the nonzero prime ideals. If \( I \) is any nonzero ideal, then by (3.4.2) there is a nonzero ideal \( I' \) such that \( II' \) is a principal ideal \((a)\), with \( I' \) relatively prime to \( J \). But then the set of prime factors of \( I' \) is empty, so \( I' = R \). Thus \((a) = II' = IR = I \). ♣

The next result reinforces the idea that a Dedekind domain is not too far away from a principal ideal domain.

### 3.4.4 Corollary

Let \( I \) be a nonzero ideal of the Dedekind domain \( R \), and let \( a \) be any nonzero element of \( I \). Then \( I \) can be generated by two elements, one of which is \( a \).

**Proof.** Since \( a \in I \), we have \((a) \subseteq I \), so \( I \) divides \((a)\), say \((a) = IJ \). By (3.4.2), there is a nonzero ideal \( I' \) such that \( II' \) is a principal ideal \((b)\) and \( I' \) is relatively prime to \( J \). If \( \gcd \) stands for greatest common divisor, then the ideal generated by \( a \) and \( b \) is

\[
gcd((a), (b)) = \gcd(IJ, II') = I
\]

because \( \gcd(J, I') = (1) \). ♣

### 3.4.5 The Ideal Class Group

Let \( I(R) \) be the group of nonzero fractional ideals of a Dedekind domain \( R \). If \( P(R) \) is the subset of \( I(R) \) consisting of all nonzero principal fractional ideals \( Rx, x \in K \), then \( P(R) \) is a subgroup of \( I(R) \). To see this, note that \((Rx)(Ry)^{-1} = (Rx)(Ry^{-1}) = Rxy^{-1} \), which belongs to \( P(R) \). The quotient group \( C(R) = I(R)/P(R) \) is called the ideal class group of \( R \). Since \( R \) is commutative, \( C(R) \) is abelian, and we will show later that in the number field case, \( C(R) \) is finite.
Let us verify that $C(R)$ is trivial if and only if $R$ is a PID. If $C(R)$ is trivial, then every integral ideal $I$ of $R$ is a principal fractional ideal $Rx, x \in K$. But $I \subseteq R$, so $x = 1x$ must belong to $R$, proving that $R$ is a PID. Conversely, if $R$ is a PID and $I$ is a nonzero fractional ideal, then $rI \subseteq R$ for some nonzero $r \in R$. By hypothesis, the integral ideal $rI$ must be principal, so $rI = Ra$ for some $a \in R$. Thus $I = R(a/r)$ with $a/r \in K$, and we conclude that every nonzero fractional ideal of $R$ is a principal fractional ideal.

Problems For Section 3.4

We will now go through the factorization of an ideal in a number field. In the next chapter, we will begin to develop the necessary background, but some of the manipulations are accessible to us now. By (2.3.11), the ring $B$ of algebraic integers of the number field $\mathbb{Q}(\sqrt{-5})$ is $\mathbb{Z}[\sqrt{-5}]$. (Note that $-5 \equiv 3 \mod 4$.) If we wish to factor the ideal $(2) = 2B$ of $B$, the idea is to factor $x^2 + 5 \mod 2$, and the result is $x^2 + 5 \equiv (x + 1)^2 \mod 2$. Identifying $x$ with $\sqrt{-5}$, we form the ideal $P_2 = (2, 1 + \sqrt{-5})$, which turns out to be prime. The desired factorization is $(2) = P_2^2$. This technique works if $B = \mathbb{Z}[\alpha]$, where the number field $L$ is $\mathbb{Q}(\sqrt{\alpha})$.

1. Show that $1 - \sqrt{-5} \in P_2$, and conclude that $6 \in P_2^2$.
2. Show that $2 \in P_2^2$, hence $(2) \subseteq P_2^2$.
3. Expand $P_2^2 = (2, 1 + \sqrt{-5})(2, 1 + \sqrt{-5})$, and conclude that $P_2^2 \subseteq (2)$.
4. Following the technique suggested in the above problems, factor $x^2 + 5 \mod 3$, and conjecture that the prime factorization of $(3)$ in the ring of algebraic integers of $\mathbb{Q}(\sqrt{-5})$ is $(3) = P_3P_3'$ for appropriate $P_3$ and $P_3'$.
5. With $P_3$ and $P_3'$ as found in Problem 4, verify that $(3) = P_3P_3'$. 