Introduction to Algebraic Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

Some Ring Theory

Ring Homomorphisms

Definition

Let R and S be rings. Then $\phi : R \to S$ is a **ring homomorphism** if it preserves the additive and multiplicative structures and the multiplicative identity:

1. For all $a, b \in R$, we have $\phi(a+b) = \phi(a) + \phi(b)$;
2. For all $a, b \in R$, we have $\phi(ab) = \phi(a)\phi(b)$;
3. $\phi(1_R) = 1_S$.

If also ϕ is bijective, then ϕ is an **isomorphism**.
The **kernel** of ϕ is defined as the set

$$\ker\phi = \{r \in R : \phi(r) = 0_S\}.$$

The **image** of ϕ is the set

$$\mathrm{im}\phi = \{s \in S : s = \phi(r), \text{ for some } r \in R\}.$$

Properties of Ring Homomorphisms

- It is easy to check that if $\phi : R \to S$ is a ring homomorphism, then:
  1. $\phi(0_R) = 0_S$;
  2. if $a \in R$, then $\phi(-a) = -\phi(a)$.

1. We have
$$\phi(0_R) = \phi(0_R + 0_R) = \phi(0_R) + \phi(0_R).$$
Therefore, $\phi(0_R) = 0_S$.
2. We have
$$\phi(a) + \phi(-a) = \phi(a + (-a)) = \phi(0_R) = 0_S.$$
So $\phi(-a) = -\phi(a)$.

Inverse Images of Ideals

Lemma

Let $\phi : R \to S$ be a ring homomorphism. Let I be an ideal of S, and let

$$\phi^{-1}(I) = \{a \in R : \phi(a) \in I\}.$$

Then $\phi^{-1}(I)$ is an ideal of R.

- We have to check that:
  1. $0_R \in \phi^{-1}(I)$;
  2. if $a, b \in \phi^{-1}(I)$, then so is $a - b$;
  3. if $i \in \phi^{-1}(I)$ and $a \in R$, then $ai \in \phi^{-1}(I)$.

  We know that $\phi(0_R) = 0_S \in I$. So $0_R \in \phi^{-1}(I)$.

  We also have $\phi(a-b) = \phi(a) - \phi(b)$.

  So, if $\phi(a), \phi(b) \in I$, so is $\phi(a-b)$.

  Equivalently, if $a, b \in \phi^{-1}(I)$, then $a - b \in \phi^{-1}(I)$.

Inverse Images of Ideals (Cont'd)

- Finally, let $i \in \phi^{-1}(I)$ and $a \in R$.
  We have $\phi(ai) = \phi(a)\phi(i)$.
  Since $\phi(i) \in I$, we get $\phi(ai) \in I$.
  So $ai \in \phi^{-1}(I)$.
- Note that $\ker\phi = \phi^{-1}(0_S)$.
- So, if $\phi : R \to S$ is a ring homomorphism, then

$$\ker\phi = \{a \in R : \phi(a) = 0_S\}$$

  is an ideal in R.
- We can also check that $\mathrm{im}\phi$ is a subring of S.

Injectivity and Kernels of Ring Homomorphisms

Lemma

A ring homomorphism $\phi : R \to S$ is injective if and only if its kernel just consists of the zero element.

- Suppose that $\ker\phi = \{0_R\}$. Then

$$\begin{aligned} \phi(r_1) = \phi(r_2) \quad &\Rightarrow \quad \phi(r_1 - r_2) = 0_S \\ &\Rightarrow \quad r_1 - r_2 \in \ker\phi \\ &\Rightarrow \quad r_1 - r_2 = 0_R \\ &\Rightarrow \quad r_1 = r_2. \end{aligned}$$

So ϕ is injective.

Conversely, if ϕ is injective, then its kernel is trivial.

If $\phi(r) = 0_S$, we have $\phi(r) = \phi(0_R)$.

So $r = 0_R$, as ϕ is injective.

Cosets of Ideals in Rings

- Ideals in rings are analogous to normal subgroups of groups.
- Suppose that I is an ideal in a ring R, and that $r \in R$.
- Let
$$r + I = \{r + i : i \in I\}$$
be the coset of I.
- Then
$$r \in I \quad \text{if and only if} \quad r + I = I.$$
- The following is a consequence of this:
$$r + I = r' + I \quad \text{if and only if} \quad r - r' \in I.$$

Quotient Ring by an Ideal

Proposition

Let I be an ideal in the ring R. If $a \in R$, let

$$a + I = \{a + i : i \in I\}$$

be the coset of I. Then the collection of cosets,

$$R/I = \{a + I : a \in R\},$$

may be given the structure of a ring, called the **quotient ring**.

- We define

$$(a + I) + (b + I) = (a + b) + I, \quad (a + I)(b + I) = (ab) + I.$$

We show these are well-defined.

Quotient Ring by an Ideal (Cont'd)

- We must prove that choosing a different coset representative gives the same coset as the answer.

  Suppose $a+I = a'+I$.

  Then $a-a' \in I$.

  Let $i = a-a'$.

  Since $i \in I$, we have $i+I = I$.

  Then

$$(a+I)+(b+I) = (a+b)+I = (a'+i+b)+I = (a'+b)+I = (a'+I)+(b+I).$$

  Moreover,

$$(a+I)(b+I) = ab+I = (a'+i)b+I = a'b+ib+I \overset{ib\in I}{=} a'b+I = (a'+I)(b+I).$$

Quotient Ring by an Ideal (Cont'd)

- Now we check the ring axioms.

  They are straightforward, as they are inherited from R.

  For example, the additive identity is $I = 0_R + I$, because

$$(a + I) + I = (a + I) + (0_R + I) = (a + 0_R) + I = a + I.$$

  In the same way, the multiplicative identity is $1_R + I$.

  For commutativity of addition:

$$(a + I) + (b + I) = (a + b) + I = (b + a) + I = (b + I) + (a + I).$$

  The middle equality holds because of commutativity of addition in R and the others from our definition of addition of cosets.

  Checking the other axioms is similar.

The Integers Modulo n

- Fix the positive integer $n \geq 2$.
- For each integer a, let $\overline{a}$ be the set of all integers congruent to a (mod n),
$$\overline{a} = \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}.$$
- Note that if $a \equiv b \pmod{n}$, then $\overline{a} = \overline{b}$.
- Then the **integers modulo** n are given by $\{\overline{0}, \overline{1}, \ldots \overline{n-1}\}$, with addition and multiplication defined using arithmetic modulo n (which is well defined):
$$\overline{a} + \overline{b} = \overline{a+b}, \quad \overline{a} \cdot \overline{b} = \overline{ab}.$$
- To check any given ring axiom, write down the corresponding axiom for $\mathbb{Z}$, and reduce it modulo n.
- Thus, all the axioms are inherited from those for $\mathbb{Z}$.

The Integers Modulo n (Cont'd)

- Note that
$$\overline{a} = a + n\mathbb{Z}.$$
- So the integers mod n are given by
$$\{a + n\mathbb{Z} : a \in \mathbb{Z}\}.$$
- Thus, they can be viewed as the quotient of the ring $\mathbb{Z}$ by the ideal $n\mathbb{Z}$ of all integers divisible by n, i.e., as $\mathbb{Z}/n\mathbb{Z}$.
- We use the notation $\mathbb{Z}/n\mathbb{Z}$ to denote the integers modulo n.
- We omit the bars on top of the numbers, so that we view $\mathbb{Z}/n\mathbb{Z}$ as the set $\{0, \ldots, n-1\}$, with addition and multiplication taken modulo n.

Quotient Maps

- Let I be an ideal in the ring R.
- Then there is a naturally defined **quotient map**

$$R \to R/I; \quad r \mapsto r + I.$$

- This map is always a homomorphism.
- In the case $R = \mathbb{Z}$, $I = n\mathbb{Z}$, then this is exactly the map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ which takes m to $m \pmod{n}$.

Two Special Cases

1. If $I = R$, then R/I is the trivial ring, with just one element.
   For this, take any element $a + R \in R/R$.
   Since $a \in R$, we have $a + R = R$.
   Thus, the only element of R/R is $0_R + R = R$.
2. If $I = (0_R)$, then R/I is isomorphic to R.
   Every element of R/I is of the form $a + (0_R)$, for some $a \in R$.
   Since these are all distinct, $a + (0_R) = b + (0_R)$ implies that $a = b$.
   So we get an isomorphism.

Example: $\mathbb{Z}[X]/\langle X^2\rangle$

- Let $R=\mathbb{Z}[X]$.
  Let $I=\langle X^2\rangle$ consist of all multiples of X^2.
  A typical element of R/I may be written

$$f(X)+\langle X^2\rangle,$$

  where $f(X)$ is a polynomial with integer coefficients.
  Let $f(X)$ be the polynomial

$$a_0+a_1X+\cdots+a_{d-1}X^{d-1}+a_dX^d.$$

  f may be written $a_0+a_1X+g(X)X^2$, for some polynomial $g(X)$.
  But $g(X)X^2$ is in the ideal $\langle X^2\rangle$.
  It follows that

$$f+\langle X^2\rangle=a_0+a_1X+\langle X^2\rangle.$$

  So elements of $\mathbb{Z}[X]/\langle X^2\rangle$ are parameterized only by their constant and linear terms.

Example: $\mathbb{Z}[X]/\langle X^2\rangle$ (Cont'd)

- The coset corresponding to $a+bX$ is the collection of all polynomials whose constant term is a and whose linear term is b.

  We can add two elements,

$$(a+bX+\langle X^2\rangle)+(c+dX+\langle X^2\rangle)=(a+c)+(b+d)X+\langle X^2\rangle.$$

  We can also multiply them,

$$(a+bX+\langle X^2\rangle)(c+dX+\langle X^2\rangle)=ac+(ad+bc)X+\langle X^2\rangle.$$

  This is done in the usual way, but ignoring all terms X^2 and above.

Example: $\mathbb{Z}[X]/\langle X^2-2\rangle$

- Let $R=\mathbb{Z}[X]$.

  Let $I=\langle X^2-2\rangle$ be the ideal of all multiples of X^2-2.

  Then each $f\in\mathbb{Z}[X]$ can be written as

  $$q(X)(X^2-2)+r(X),$$

  where:
  - $q(X)$ is the quotient after dividing f by X^2-2;
  - $r(X)$ is the remainder after dividing f by X^2-2.

  The degree of $r(X)$ is at most 1.

  So $r(X)=b_0+b_1X$, for some $b_0,b_1\in\mathbb{Z}$.

  Thus, $f+I=r+I$.

  So every coset is parameterized by a linear polynomial as before.

Example: $\mathbb{Z}[X]/\langle X^2-2\rangle$ (Cont'd)

- The addition rule is the same as before,

$$(a+bX+\langle X^2-2\rangle)+(c+dX+\langle X^2-2\rangle) \\ =(a+c)+(b+d)X+\langle X^2-2\rangle.$$

The multiplication rule, however, looks rather different.

$$\begin{aligned}(a+bX+\langle X^2-2\rangle)&(c+dX+\langle X^2-2\rangle)\\ &=ac+(ad+bc)X+bdX^2+\langle X^2-2\rangle\\ &=ac+(ad+bc)X+bd(2+(X^2-2))+\langle X^2-2\rangle\\ &=ac+(ad+bc)X+2bd+bd(X^2-2)+\langle X^2-2\rangle\\ &=(ac+2bd)+(ad+bc)X+\langle X^2-2\rangle.\end{aligned}$$

Example: $\mathbb{Z}[\sqrt{2}]$

- Suppose $\alpha = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ and $\beta = c + d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

  Then

$$\begin{aligned} \alpha + \beta &= (a+c) + (b+d)\sqrt{2}; \\ \alpha\beta &= (ac + 2bd) + (ad + bc)\sqrt{2}. \end{aligned}$$

  These closely resemble the addition and multiplication law for the quotient ring $\mathbb{Z}[X]/\langle X^2 - 2\rangle$.

  Claim: The map

$$\begin{aligned} \mathbb{Z}[X]/\langle X^2 - 2\rangle &\to \mathbb{Z}[\sqrt{2}]; \\ a + bX + \langle X^2 - 2\rangle &\mapsto a + b\sqrt{2}. \end{aligned}$$

  is an isomorphism of rings.

  That it is a homomorphism is verified explicitly using the above calculations.

  One can also check that it is a bijection.

First Isomorphism Theorem

Theorem (First Isomorphism Theorem)

Let $\phi : R \to S$ be a ring homomorphism. Then there is an isomorphism

$$R/\ker\phi \cong \mathrm{im}\phi.$$

- Define a map $\widetilde{\phi} : R/\ker\phi \to \mathrm{im}\phi$ by

$$\widetilde{\phi}(r + \ker\phi) = \phi(r).$$

We need to check that $\widetilde{\phi}$ is well-defined.

Suppose that the coset $r + \ker\phi$ may also be written as $r' + \ker\phi$.

With one definition of $\widetilde{\phi}$ we get $\phi(r)$, and with the other we get $\phi(r')$.

We must check that these are the same.

First Isomorphism Theorem (Well-Defined)

- We have
$$r + \ker\phi = r' + \ker\phi.$$
It follows that the element $r - r' \in \ker\phi$.
In other words, there exists $k \in \ker\phi$, such that $r = r' + k$.
But now
$$\phi(r) = \phi(r' + k) = \phi(r') + \phi(k) = \phi(r') + 0_S = \phi(r').$$
Now we know that the map $\widetilde{\phi}$ exists and makes sense.
Applying $\widetilde{\phi}$ to any coset gives an element which is in the image of ϕ.
So $\widetilde{\phi}$ is valued in $\mathrm{im}\phi$.

First Isomorphism Theorem (Homomorphism)

- Now we check that $\widetilde{\phi}$ is a homomorphism.

  This follows easily from our definition of addition and multiplication of cosets.

  E.g., for addition, we have

$$\begin{aligned}
\widetilde{\phi}((a+\ker\phi)+(b+\ker\phi)) &= \widetilde{\phi}((a+b)+\ker\phi) \\
&= \phi(a+b) \\
&= \phi(a)+\phi(b) \\
&= \widetilde{\phi}(a+\ker\phi)+\widetilde{\phi}(b+\ker\phi).
\end{aligned}$$

First Isomorphism Theorem (Injectivity)

- Next, we check that $\widetilde{\phi}$ is injective.

  Suppose we have an element $r+\ker\phi$ in the kernel.

  Then

  $$\phi(r)=\widetilde{\phi}(r+\ker\phi)=0_S.$$

  So certainly $r\in\ker\phi$.

  So $r+\ker\phi=\ker\phi$, the zero element of the quotient ring $R/\ker\phi$.

  Thus, the kernel just consists of the zero element of the quotient ring.

  So $\widetilde{\phi}$ is injective.

  It is clear that the image of $\widetilde{\phi}$ is exactly the same as the image of ϕ.

  So $\widetilde{\phi}$ is surjective onto $\mathrm{im}\phi$.

  This shows that $\widetilde{\phi}$ is an isomorphism.

First Isomorphism Theorem for Modules

- Let M, N be modules over a ring R.
- A map $\phi : M \to N$ is a **module homomorphism** if, for all $m, m' \in M$ and all $r \in R$,
  - $\phi(m + m') = \phi(m) + \phi(m')$;
  - $\phi(rm) = r\phi(m)$.

First Isomorphism Theorem for Modules

If $\phi : M \to N$ is a homomorphism of modules over a ring R, then the collection $M/\ker\phi$ of cosets $m + \ker\phi$ is isomorphic to $\text{im}\phi$.

- The idea of the proof is similar to that of the preceding theorem.

Quotients of Polynomial Rings and Finite Field Extensions

Lemma

Let K be a field. Suppose that γ is algebraic over K, i.e., it satisfies a polynomial equation with coefficients in K. Suppose that $f \in K[X]$ is the minimal polynomial of γ. Then there is an isomorphism

$$K[X]/\langle f \rangle \cong K(\gamma)$$

got by mapping X to γ.

- Consider the mapping

$$\begin{array}{rccc} \phi_\gamma : & K[X] & \to & K(\gamma); \\ & g(X) & \mapsto & g(\gamma). \end{array}$$

It is a homomorphism. For all $g, h \in K[X]$ and $k \in K$:

- $\phi_\gamma(g+h) = (g+h)(\gamma) = g(\gamma) + h(\gamma) = \phi_\gamma(g) + \phi_\gamma(h)$;
- $k\phi_\gamma(g) = kg(\gamma) = (kg)(\gamma) = \phi_\gamma(kg)$.

Proof of the Lemma (Cont'd)

- The kernel of ϕ_γ consists of all polynomials which have γ as a root.
  This is precisely the set of all multiples of f, namely $\langle f \rangle$.
  Moreover, ϕ_γ is surjective.
  Every element of $K(\gamma)$ is just a polynomial

$$a_d \gamma^d + \cdots + a_0, \quad a_i \in K.$$

  This is the image under ϕ_γ of the polynomial

$$a_d X^d + \cdots + a_0 \in K[X].$$

  By the First Isomorphism Theorem, ϕ_γ gives an isomorphism

$$\widetilde{\phi}_\gamma : K[X]/\langle f \rangle \cong K(\gamma).$$

Example

- Take $K = \mathbb{Q}$ and $\gamma = \sqrt{2}$.

  Then γ has minimal polynomial $X^2 - 2$.

  By the lemma, there is an isomorphism

$$\mathbb{Q}[X]/\langle X^2 - 2\rangle \cong \mathbb{Q}(\sqrt{2}),$$

  given by sending X to $\sqrt{2}$.

  That is, it is defined by

$$a + bX + \langle X^2 - 2\rangle \mapsto a + b\sqrt{2},$$

  just as we saw before for $\mathbb{Z}$.

Subsection 2

Maximal Ideals

Maximal Ideals

- The first definition of a prime number is that it is a natural number p with no divisor other than 1 and itself.
- It is easy to reformulate this in terms of ideals in $\mathbb{Z}$.
  - If a natural number a exists with $a \mid p$, then $\langle p \rangle \subset \langle a \rangle$.
  - If $a \neq p$, then the inclusion $\langle p \rangle \subset \langle a \rangle$ must be strict.
  - If $a \neq 1$, then $\langle a \rangle \subset \mathbb{Z}$ is also a strict inclusion.
- So we have two strict inclusions $\langle p \rangle \subset \langle a \rangle \subset \mathbb{Z}$.
- But if p is prime, there is no natural number a such that we have strict inclusions $\langle p \rangle \subset \langle a \rangle \subset \mathbb{Z}$.
- I.e., there is no proper ideal which is strictly bigger than $\langle p \rangle$.

Definition

Let R be an integral domain. An ideal I of R is said to be **maximal** if:

1. $I \neq R$;
2. There is no ideal $J \neq R$ which strictly contains I.

Maximal Ideals and Irreducible Generators

- We verify that maximal principal ideals are generated by irreducible elements.

Lemma

Let R be an integral domain, and let $p \in R$. If $\langle p \rangle$ is maximal, then p is irreducible.

- Suppose p is not irreducible.

  Then either p is a unit or $p = ab$ for two non-unit elements a and b.
  - Suppose p is a unit.
    Then we would have $\langle p \rangle = R$.
    So $\langle p \rangle$ is not maximal.
  - Suppose $p = ab$ for two non-unit elements a and b.
    Then p is a multiple of a. So $\langle p \rangle \subseteq \langle a \rangle$.
    But a is not a multiple of p, since b is not a unit. So $a \notin \langle p \rangle$.
    Hence, $\langle a \rangle$ strictly contains $\langle p \rangle$.
    Thus, $\langle p \rangle$ is not maximal.

The Converse in PIDs

- If R is a principal ideal domain, the converse of the lemma is also true.
- In particular, maximal ideals exactly correspond to irreducible elements in PIDs (two associate irreducible elements will give the same maximal ideal).
- This suggests that the notion of a maximal ideal might be a suitable generalization to ideals of the notion of an irreducible element.

Maximal Ideals and Fields

Lemma

I is a maximal ideal of R if and only if R/I is a field.

- First suppose that I is a maximal ideal of R.
  Let $a \in R$, but $a \notin I$.
  Then the set $\langle a, I \rangle = aR + I$ is an ideal of R.
  Moreover, it is strictly larger than I as it contains a.
  Thus, we must have $aR + I = R$.
  In particular, $1_R \in aR + I$.
  So, there exists $b \in R$, such that $1_R \in ab + I$.
  It follows that $1_R + I = ab + I = (a + I)(b + I)$.
  So $b + I$ is a multiplicative inverse for $a + I$ in R/I.
  Thus, every non-zero coset is invertible.
  Hence, R/I is a field.

Maximal Ideals and Fields (Cont'd)

- Conversely, suppose R/I is a field.

  Then every non-zero coset is invertible.

  Suppose that J is an ideal of R strictly containing I.

  Let $a \in J - I$.

  Then, there exists $b \in R$, such that

$$(a+I)(b+I) = ab + I = 1_R + I.$$

  As $J \supset I$ and $ab \in J$, we must have $1_R \in J$.

  But any ideal containing a unit must be the whole ring.

  Therefore, $J = R$.

Example: Maximal Ideals in $\mathbb{Z}$

Claim: The maximal ideals of $\mathbb{Z}$ are precisely $\langle p \rangle = p\mathbb{Z}$, where p is prime.

The ideals of $\mathbb{Z}$ are $\langle 0 \rangle$ and $\langle n \rangle = n\mathbb{Z}$, where n is a positive integer.

- $\langle 0 \rangle$ is not maximal because it is contained in any proper ideal, $\langle 2 \rangle$, for example. (Alternatively, $\mathbb{Z}/\langle 0 \rangle \cong \mathbb{Z}$, which is not a field.)
- If n is not prime, it has a divisor d greater than 1.
  Then $n\mathbb{Z}$ is not maximal as it is contained in $d\mathbb{Z}$.
  (Alternatively, d is not invertible in $\mathbb{Z}/n\mathbb{Z}$.)
- However, if $n = p$ is prime, then we know that $\mathbb{Z}/p\mathbb{Z}$ is a field.
  Indeed, any non-zero element $a \in \mathbb{Z}/p\mathbb{Z}$ has an inverse.
  Find b and s, by the Euclidean algorithm, such that $ab + ps = 1$.
  Then $ab \equiv 1 \pmod{p}$.

- Thus, maximal ideals in $\mathbb{Z}$ match up nicely with the prime numbers.

Subsection 3

Prime Ideals

Prime Ideals

- The other possible way to generalize the idea of a prime number to ideals is to recall the property that p is prime if

$$p \mid ab \quad \text{implies} \quad p \mid a \text{ or } p \mid b.$$

- The property says that, if ab is a multiple of p, then either a is a multiple of p or b is a multiple of p, i.e.,

$$ab \in \langle p \rangle \quad \text{implies} \quad a \in \langle p \rangle \text{ or } b \in \langle p \rangle.$$

Definition

Let R be an integral domain. An ideal I of R is said to be **prime** if:

1. $I \neq R$;
2. If $xy \in I$, then $x \in I$ or $y \in I$.

An Equivalent Formulation of Primeness

- Reformulating further: $\langle a\rangle\langle b\rangle \subseteq \langle p\rangle$ implies $\langle a\rangle \subseteq \langle p\rangle$ or $\langle b\rangle \subseteq \langle p\rangle$.

Lemma

I is a prime ideal of R if and only if whenever J_1 and J_2 are ideals of R,

$$J_1 J_2 \subseteq I \quad \text{implies} \quad J_1 \subseteq I \text{ or } J_2 \subseteq I.$$

- Suppose $J_1 \nsubseteq I$, $J_2 \nsubseteq I$, but $J_1 J_2 \subseteq I$.
  Then, there exist $a_1 \in J_1 - I$ and $a_2 \in J_2 - I$.
  But $J_1 J_2 \subseteq I$. So $a_1 a_2 \in I$.
  As I is prime, either a_1 or a_2 must lie in I.
  This contradicts our choices of those elements.

An Equivalent Formulation of Primeness (Cont'd)

- Conversely, suppose I is not prime.

  There exist elements a_1 and a_2 not in I, but with $a_1 a_2 \in I$.

  Let $J_1 = \langle a_1 \rangle$, $J_2 = \langle a_2 \rangle$.

  Then neither J_1 nor J_2 is contained in I.

  On the other hand, $J_1 J_2 = \langle a_1 a_2 \rangle \subseteq I$.
- We will use this formulation when we think about factorization of ideals in rings of integers of number fields into prime ideals.

Prime Ideals and Prime Elements

Lemma

Let R be an integral domain, and let $p \in R$. Then $\langle p \rangle$ is a prime ideal in R if and only if p is a prime element.

- Suppose that $\langle p \rangle$ is a prime ideal.

  We show that p is a prime element.

  Suppose that $p \mid ab$ in R.

  Then $ab \in \langle p \rangle$.

  So either $a \in \langle p \rangle$ or $b \in \langle p \rangle$.

  But this means that $p \mid a$ or $p \mid b$, respectively.

  So p is a prime element.

Prime Ideals and Prime Elements (Cont'd)

- Conversely, suppose that p is a prime element.

  We show that $\langle p \rangle$ is a prime ideal.

  Take a and b with $ab \in \langle p \rangle$.

  Then $ab = cp$, for some $c \in R$.

  So $p \mid ab$.

  By definition, $p \mid a$ or $p \mid b$.

  This means that $a \in \langle p \rangle$ or $b \in \langle p \rangle$.

  Hence, $\langle p \rangle$ is a prime ideal.

- In particular, let R be a ring of integers of some number field, where every ideal is principal.

  Then the prime ideals would correspond exactly to prime elements.

  Of course, two associate prime elements give the same prime ideal.

Prime Ideals and Integral Domains

Lemma

Let R be a ring and I an ideal of R. Then I is a prime ideal if and only if R/I is an integral domain.

- Suppose that I is a prime ideal of R.

  We have to check that R/I has no zero divisors.

  Suppose that $(a+I)(b+I) = 0_R + I = I$.

  But $(a+I)(b+I) = ab+I$, and $ab+I = I$ implies that $ab \in I$.

  As I is prime, either $a \in I$ or $b \in I$.

  If $a \in I$, $a+I = I$.

  If $b \in I$, $b+I = I$.

  So one of $a+I$ and $b+I$ is the zero element $0_R + I$.

  It follows that there are no zero divisors in R/I.

Prime Ideals and Integral Domains (Cont'd)

- Conversely, suppose R/I has no zero divisors.

  Let a and b be elements of R, such that $a \notin I$, and $ab \in I$.

  Then $a+I$ is a non-zero coset such that $(a+I)(b+I) = 0_R + I$.

  But, there are no zero-divisors.

  So we must have $b+I = 0_R + I$.

  So $b \in I$.

  Thus, I is prime.

Maximal Ideals and Prime Ideals

Corollary

Maximal ideals are prime.

- If I is a maximal ideal, then R/I is a field.

  Every field is an integral domain.

  So R/I is an integral domain.

  Therefore, I is prime.

Prime Ideals and Maximal Ideals

- The converse is not quite true.
- The prime ideals of $\mathbb{Z}$ are precisely $\langle p \rangle = p\mathbb{Z}$, where p is prime, and also $\langle 0 \rangle$.
  - $\langle 0 \rangle$ is prime, because $\mathbb{Z}/\langle 0 \rangle \cong \mathbb{Z}$, which is an integral domain.
  - The other ideals are all of the form $n\mathbb{Z}$ for some positive integer n.
    - If n is not prime, then $\mathbb{Z}/n\mathbb{Z}$ has zero divisors.
      So $\langle n \rangle$ is not prime.
    - If $n = p$ is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field.
      So it is certainly an integral domain.
- Therefore $\langle 0 \rangle$ is a prime ideal of $\mathbb{Z}$ which is not maximal.
- All other prime ideals are also maximal.

Inclusion Between Prime Ideals

- The prime ideal $\langle 0 \rangle$ of $\mathbb{Z}$ is contained in all other prime ideals of $\mathbb{Z}$.
- It might seem odd to have one prime ideal contained inside another.
- Of course, $\langle 0 \rangle$ is in some sense a rather exceptional prime ideal.
- Perhaps surprisingly, one can find many examples of rings R in which one prime ideal can contain another, non-trivial, prime ideal.

  Example: Consider the ring $R = K[X, Y]$.

  In R, both $P_1 = \langle X, Y \rangle$ and $P_2 = \langle X \rangle$ are prime, and $P_1 \supseteq P_2$.
- We will see that this sort of example does not occur for rings of integers of number fields.
- In such rings, every non-zero prime ideal is also maximal.

Finite Integral Domains and Fields

- Every maximal ideal is prime.
- The converse is not true (e.g., $\mathbb{Z}$).
- However, finite integral domains are always fields.

Lemma

If R is a finite integral domain, then R is a field.

- We just need to check that every non-zero $r \in R$ is invertible.

  Consider the $\phi : R \to R$ (not a homomorphism), given by $\phi(s) = rs$.

  It is injective. Suppose $\phi(s_1) = \phi(s_2)$. Then $rs_1 = rs_2$.

  So $r(s_1 - s_2) = 0$. Since R is an integral domain, $s_1 - s_2 = 0$.

  But an injective map from a finite set to itself is also surjective.

  So, there is some s, such that $\phi(s) = 1$. So $rs = 1$.

Number Fields and Prime Ideals in Rings of Integers

Lemma

Let K be a number field. If $\mathfrak{p}$ is a non-zero prime ideal in $\mathbb{Z}_K$, then $\mathbb{Z}_K/\mathfrak{p}$ is finite.

- Let $\mathfrak{p}$ be a non-zero prime ideal in $\mathbb{Z}_K$.

  Then there is a non-zero element $\alpha \in \mathfrak{p}$.

  Its norm $N = N_{K/\mathbb{Q}}(\alpha)$ lies in $\mathbb{Z}$.

  It is the product of $\alpha \in \mathfrak{p}$ with all its conjugates.

  So $N \in \mathfrak{p}$.

  Now $\mathbb{Z}_K$ has an integral basis, by a previous result.

  So we can write

$$\mathbb{Z}_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n.$$

Number Fields and Prime Ideals in Rings of Integers

- As $N \in \mathfrak{p}$, by the defining rule of ideals, $N\omega_i \in \mathfrak{p}$, for each i.

  It follows that every element $a_1\omega_1 + \cdots + a_n\omega_n$ is congruent modulo $\mathfrak{p}$ to some element of the form

  $$b_1\omega_1 + \cdots + b_n\omega_n, \quad \text{with } 0 \leq b_i < N.$$

  There are finitely many such elements.

  So $\mathbb{Z}_K/\mathfrak{p}$ is finite.
- It is easy to see that this proof is valid for any non-zero ideal, not just prime ideals.

Nonzero Prime Ideals in Rings of Integers

Proposition

Let K be a number field. Then every non-zero prime ideal $\mathfrak{p}$ in $\mathbb{Z}_K$ is maximal.

- By the lemma, $\mathbb{Z}_K/\mathfrak{p}$ is finite.

  Thus, $\mathbb{Z}_K/\mathfrak{p}$ is a finite integral domain.

  Hence, by the previous lemma, it is also a field.

  Then, by a previous result, $\mathfrak{p}$ must be maximal.

Subsection 4

Unique Factorization into Prime Ideals

Fractional Ideals of $\mathbb{Z}_K$

Definition

A **fractional ideal** of $\mathbb{Z}_K$ is a subset of K which is of the form $\frac{1}{\gamma}\mathfrak{c}$, where $\mathfrak{c}$ is an ideal of $\mathbb{Z}_K$ and γ is a non-zero element of $\mathbb{Z}_K$.
We say that the fractional ideal is **principal** if $\mathfrak{c}$ is principal.

- Notice that fractional ideals are subsets of K, not just of $\mathbb{Z}_K$.
  So (despite the name) they are not generally ideals of $\mathbb{Z}_K$.
- Recall that the product of two ideals is again an ideal.
  So the product of two fractional ideals is again a fractional ideal.

Product of Prime Ideals Included in an Ideal

Lemma

Let $\mathfrak{a}$ be a non-zero ideal of $\mathbb{Z}_K$. Then there exist prime ideals $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$, such that $\mathfrak{p}_1\cdots\mathfrak{p}_r \subseteq \mathfrak{a}$.

- Suppose the statement fails.
  Then we can choose $\mathfrak{a}$ as large as possible subject to the condition that the statement is false.
  That is, we choose $\mathfrak{a}$ so that any larger ideal does have prime ideals $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ as in the statement.
  This is one point where we use the fact that $\mathbb{Z}_K$ is Noetherian.
  Equivalently, $\mathbb{Z}_K$ satisfies the Ascending Chain Condition.
  We consider the set of all ideals such that the statement fails.
  We choose one, $\mathfrak{a}_1$ say.
  If $\mathfrak{a}_1$ is as large as possible, we are done.
  Else, there is a bigger ideal $\mathfrak{a}_2$ contradicting the statement.

Product of Prime Ideals Included in an Ideal (Cont'd)

- We repeat this process.
  The ACC guarantees that this process must eventually produce an ideal which is as large as possible with this property.
  Clearly $\mathfrak{a}$ is not prime (otherwise take $\mathfrak{p}_1 = \mathfrak{a}$).
  So, there exist ideals $\mathfrak{a}_1$ and $\mathfrak{a}_2$ of $\mathbb{Z}_K$, with

$$\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}, \quad \mathfrak{a}_1 \nsubseteq \mathfrak{a}, \quad \mathfrak{a}_2 \nsubseteq \mathfrak{a}.$$

  Write

$$\mathfrak{b}_1 = \mathfrak{a} + \mathfrak{a}_1, \quad \mathfrak{b}_2 = \mathfrak{a} + \mathfrak{a}_2.$$

  Then $\mathfrak{b}_1\mathfrak{b}_2 \subseteq \mathfrak{a}$.
  On the other hand, $\mathfrak{b}_1$ and $\mathfrak{b}_2$ both strictly contain $\mathfrak{a}$.
  By maximality of $\mathfrak{a}$, there exist prime ideals $\mathfrak{p}_i$, such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq \mathfrak{b}_1, \quad \mathfrak{p}_{s+1} \cdots \mathfrak{p}_t \subseteq \mathfrak{b}_2.$$

  Then $\mathfrak{p}_1 \cdots \mathfrak{p}_t \subseteq \mathfrak{b}_1\mathfrak{b}_2 \subseteq \mathfrak{a}$. This contradicts the choice of $\mathfrak{a}$.

The Fractional Ideal $\mathfrak{a}^{-1}$

Lemma

If $\mathfrak{a}$ is an ideal of $\mathbb{Z}_K$, define

$$\mathfrak{a}^{-1} = \{\alpha \in K : \alpha\mathfrak{a} \subseteq \mathbb{Z}_K\}.$$

Then $\mathfrak{a}^{-1}$ is a fractional ideal.

- Take any $\gamma \in \mathfrak{a}$, and put $\mathfrak{c} = \gamma\mathfrak{a}^{-1}$.
  Claim: $\mathfrak{c}$ is an ideal of $\mathbb{Z}_K$.
  Clearly $0 \in \mathfrak{c}$.
  Suppose $i, i' \in \mathfrak{c}$.
  So $i = \gamma\beta$ and $i' = \gamma\beta'$, with $\beta, \beta' \in \mathfrak{a}^{-1}$.
  We must show $i + i' \in \mathfrak{c}$. But $i + i' = \gamma(\beta + \beta')$. So we need $\beta + \beta' \in \mathfrak{a}^{-1}$.
  This follows easily since

$$(\beta + \beta')\mathfrak{a} = \beta\mathfrak{a} + \beta'\mathfrak{a} \subseteq (\mathbb{Z}_K + \mathbb{Z}_K) = \mathbb{Z}_K.$$

The Fractional Ideal $\mathfrak{a}^{-1}$ (Cont'd)

- Finally, suppose $i = \gamma\beta \in \mathfrak{c}$, where $\beta \in \mathfrak{a}^{-1}$, and $r \in \mathbb{Z}_K$.

  We must show $ri \in \mathfrak{c}$.

  It suffices to show that $r\beta \in \mathfrak{a}^{-1}$.

  We have

$$(r\beta)\mathfrak{a} = r(\beta\mathfrak{a}) \subseteq r\mathbb{Z}_K \overset{r \in \mathbb{Z}_K}{\subseteq} \mathbb{Z}_K.$$

  We have shown that $\mathfrak{c} = \gamma\mathfrak{a}^{-1}$ is an ideal.

  So $\mathfrak{a}^{-1} = \frac{1}{\gamma}\mathfrak{c}$ is a fractional ideal.

Property of $\mathfrak{a}^{-1}$

Lemma

If $\mathfrak{a}$ is a proper ideal of $\mathbb{Z}_K$, then $\mathfrak{a}^{-1}$ strictly contains $\mathbb{Z}_K$.

- Suppose $\mathfrak{a}$ is a proper ideal of $\mathbb{Z}_K$.

  Clearly $\mathfrak{a}^{-1}$ contains $\mathbb{Z}_K$.

  We need to check that the inclusion is strict.

  It is easy to see that if $\mathfrak{a} \subseteq \mathfrak{b}$, then $\mathfrak{b}^{-1} \subseteq \mathfrak{a}^{-1}$.

  Now $\mathfrak{a}$ is contained in a maximal ideal $\mathfrak{p}$.

  So it suffices to show that $\mathfrak{p}^{-1}$ strictly contains $\mathbb{Z}_K$.

  We have $\mathfrak{p}^{-1} \supseteq \mathbb{Z}_K$.

  So we must find a non-integer in $\mathfrak{p}^{-1}$.

Property of $\mathfrak{a}^{-1}$ (Cont'd)

- Choose any non-zero $\alpha \in \mathfrak{p}$, so $\langle \alpha \rangle \subseteq \mathfrak{p}$.
  Choose the smallest r such that there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ with

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \langle \alpha \rangle \subseteq \mathfrak{p}.$$

  Such an r exists by a previous lemma.
  As $\mathfrak{p}$ is prime, some $\mathfrak{p}_i \subseteq \mathfrak{p}$.
  After re-ordering, we may suppose it to be $\mathfrak{p}_1$.
  But non-zero prime ideals are maximal.
  Moreover, maximal ideals cannot be properly contained in one another.
  So we have $\mathfrak{p}_1 = \mathfrak{p}$.
  As r is minimal, $\mathfrak{p}_2 \cdots \mathfrak{p}_r \nsubseteq \langle \alpha \rangle$.
  So there is some $\beta \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ not in $\langle \alpha \rangle$.
  Then $\beta \mathfrak{p} \subseteq \langle \alpha \rangle$. So $\beta \alpha^{-1} \mathfrak{p} \subseteq \mathbb{Z}_K$ and $\beta \alpha^{-1} \in \mathfrak{p}^{-1}$.
  As $\beta \alpha^{-1} \notin \mathbb{Z}_K$ $(\beta \notin \alpha \mathbb{Z}_K)$, the result follows.

A Property of Non-Zero Ideals of $\mathbb{Z}_K$

Lemma

If $\mathfrak{a}$ is a non-zero ideal of $\mathbb{Z}_K$, and $\theta \in K$ satisfies $\mathfrak{a}\theta \subseteq \mathfrak{a}$, then $\theta \in \mathbb{Z}_K$.

- As $\mathbb{Z}_K$ is Noetherian, $\mathfrak{a}$ is finitely generated, $\mathfrak{a} = \langle \omega_1, \ldots, \omega_m \rangle$.

  Then

$$\begin{aligned} \omega_1\theta &= a_{11}\omega_1 + \cdots + a_{1m}\omega_m \\ &\vdots \\ \omega_m &= a_{m1}\omega_1 + \cdots + a_{mm}\omega_m \end{aligned}$$

  with $a_{ij} \in \mathbb{Z}$. Thus, θ is an eigenvalue of $A = (a_{ij})$.

  So it is a root of the characteristic polynomial of a matrix of integers.

  It follows that θ is an algebraic integer.

  As $\theta \in K$, it follows that $\theta \in \mathbb{Z}_K$.

Fractional Ideal Inverses of Maximal Ideals

Lemma

If $\mathfrak{p}$ is a maximal ideal of $\mathbb{Z}_K$, then $\mathfrak{p}\mathfrak{p}^{-1} = \mathbb{Z}_K$.

- $\mathfrak{p}^{-1}$ is a fractional ideal.

  $\mathfrak{p}$ is an ideal (therefore, also a fractional ideal).

  So the product $\mathfrak{p}\mathfrak{p}^{-1}$ is a fractional ideal.

  However, by definition of $\mathfrak{p}^{-1}$, $\mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathbb{Z}_K$.

  So the product is an ideal of $\mathbb{Z}_K$.

  Certainly $\mathfrak{p}\mathfrak{p}^{-1} \supseteq \mathfrak{p}$ as $\mathfrak{p}^{-1} \supseteq \mathbb{Z}_K$.

  As $\mathfrak{p}$ is maximal, either $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ or $\mathfrak{p}\mathfrak{p}^{-1} = \mathbb{Z}_K$.

  But $\mathfrak{p}$ contains a non-integer element θ.

  Moreover, by the preceding lemma, $\mathfrak{p}\theta \not\subseteq \mathfrak{p}$.

  So $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ is not possible. The claim follows.

Inverse Property of $\mathfrak{a}^{-1}$

Lemma

If $\mathfrak{a}$ is any non-zero ideal of $\mathbb{Z}_K$, then $\mathfrak{a}\mathfrak{a}^{-1} = \mathbb{Z}_K$.

- Suppose that the assertion fails.

  Let $\mathfrak{a}$ be an ideal such that $\mathfrak{a}\mathfrak{a}^{-1} \neq \mathbb{Z}_K$ which is as large as possible.

  Let $\mathfrak{p}$ be a maximal ideal containing $\mathfrak{a}$.

  Consider $\mathfrak{a}\mathfrak{p}^{-1}$. We have $\mathbb{Z}_K \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$.

  Thus,

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathbb{Z}_K.$$

  So $\mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathbb{Z}_K$.

  So $\mathfrak{a}\mathfrak{p}^{-1}$ is genuinely an ideal (not just a fractional ideal) of $\mathbb{Z}_K$.

  By a previous lemma, $\mathfrak{p}^{-1}$ contains some non-integral θ.

  So we cannot have $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. This contradicts another of our lemmas.

Inverse Property of $\mathfrak{a}^{-1}$ (Cont'd)

- So $\mathfrak{a}$ is strictly contained in $\mathfrak{a}\mathfrak{p}^{-1}$.

  By our choice of $\mathfrak{a}$ as being as large as possible subject to the condition that the statement is false, we have

$$\mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} = \mathbb{Z}_K.$$

  Thus,

$$\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}^{-1}.$$

  So

$$\mathbb{Z}_K = \mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathbb{Z}_K.$$

  The result follows.

Abelian Group of Fractional Ideals

Theorem

The set of fractional ideals form an abelian group.

- We already know how to multiply ideals (and thus fractional ideals).
  - This is clearly associative and commutative.
  - The whole ring $\mathbb{Z}_K$ forms the identity.
  - We show we can define an inverse for any given fractional ideal.
    The preceding lemma gives us the inverse for any ideal.
    A fractional ideal is one of the form

$$\mathfrak{b} = \frac{1}{\gamma}\mathfrak{c},$$

    for some ideal of $\mathbb{Z}_K$ and some non-zero $\gamma \in K$.
    We claim its inverse $\mathfrak{b}^{-1}$ is $\gamma\mathfrak{c}^{-1}$.
    Indeed, we have

$$\mathfrak{b}\mathfrak{b}^{-1} = \frac{1}{\gamma}\mathfrak{c} \cdot \gamma\mathfrak{c}^{-1} = \mathbb{Z}_K.$$

Non-Zero Ideals as Products of Prime Ideals

Lemma

Every non-zero ideal $\mathfrak{a}$ is a product of prime ideals.

- Suppose this is not the case.

  Let $\mathfrak{a}$ be maximal subject to not being a product of prime ideals.

  Then $\mathfrak{a}$ is contained in some maximal ideal $\mathfrak{p}$.

  Now $\mathfrak{a}$ is strictly contained in $\mathfrak{a}\mathfrak{p}^{-1}$.

  So, by maximality of $\mathfrak{a}$, we can write

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

  a product of prime ideals.

  Therefore, $\mathfrak{a} = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_r$.

Uniqueness of the Factorization

Theorem

Factorization of ideals into prime ideals is unique.

- The preceding lemma gives a factorization into ideals.

  We need to show that this decomposition is unique.

  Let r be minimal such that there is an ideal $\mathfrak{a}$ with two different factorizations $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ into prime ideals.

  Then $\mathfrak{p}_1 \supseteq \mathfrak{q}_1 \ldots \mathfrak{q}_s$.

  As $\mathfrak{p}_1$ is a prime ideal, $\mathfrak{p}_1 \supseteq \mathfrak{q}_i$, for some i.

  But both $\mathfrak{p}_1$ and $\mathfrak{q}_i$ are maximal ideals. So $\mathfrak{p}_1 = \mathfrak{q}_i$.

  Multiply by $\mathfrak{p}^{-1}$ to get two different factorizations of an ideal $\mathfrak{a}\mathfrak{p}_1^{-1}$.

  In this, at least one expression is of shorter length than r.

  This contradicts our choice of r.

Subsection 5

Coprimality

Coprimality for Ideals

- In $\mathbb{Z}$, two integers are coprime if their highest common factor is 1.
- Unique factorization shows that this is equivalent to the statement that no prime number divides both.
- Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathbb{Z}_K$, are **coprime** if $\mathfrak{a}+\mathfrak{b}=\mathbb{Z}_K$, that is, if the ideal generated by both $\mathfrak{a}$ and $\mathfrak{b}$ is the whole ring.
- If we factor the two ideals into primes, the ideals will be coprime when no prime ideal occurs in both factorizations.

  Claim: These are equivalent.

  Suppose $\mathfrak{a}$ and $\mathfrak{b}$ both have a prime ideal $\mathfrak{p}$ in their factorization.

  Then $\mathfrak{a}+\mathfrak{b}\subseteq\mathfrak{p}$. So $\mathfrak{a}$ and $\mathfrak{b}$ do not generate the whole ring.

  Conversely, suppose $\mathfrak{a}+\mathfrak{b}$ is strictly contained in $\mathbb{Z}_K$.

  Then $\mathfrak{a}+\mathfrak{b}$ has a prime ideal $\mathfrak{p}$ in its factorization.

  Clearly then $\mathfrak{a}\subseteq\mathfrak{p}$ and $\mathfrak{b}\subseteq\mathfrak{p}$.

  Then $\mathfrak{a}$ and $\mathfrak{b}$ both have $\mathfrak{p}$ in their factorizations.

Highest Common Factor and Chinese Remainder Theorem

- The **highest common factor** of two ideals $\mathfrak{a}$ and $\mathfrak{b}$ is the ideal $\mathfrak{h}$, such that:
  1. $\mathfrak{h} \mid \mathfrak{a}$ and $\mathfrak{h} \mid \mathfrak{b}$;
  2. if $\mathfrak{c} \mid \mathfrak{a}$ and $\mathfrak{c} \mid \mathfrak{b}$, then $\mathfrak{c} \mid \mathfrak{h}$.

Theorem (Chinese Remainder Theorem)

Suppose that K is a number field. Suppose that $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are ideals in $\mathbb{Z}_K$, which are coprime in the sense that $\mathfrak{a}_i + \mathfrak{a}_j = \mathbb{Z}_K$, for all $i \neq j$. Then

$$\mathbb{Z}_K/(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n) \cong \mathbb{Z}_K/\mathfrak{a}_1 \oplus \cdots \oplus \mathbb{Z}_K/\mathfrak{a}_n.$$

- The result is clear for $n = 1$.

  So we assume that $n \geq 2$.

Chinese Remainder Theorem (Cont'd)

- There is a homomorphism

$$\begin{aligned} \theta: \quad \mathbb{Z}_K &\to \mathbb{Z}_K/\mathfrak{a}_1 \oplus \cdots \oplus \mathbb{Z}_K/\mathfrak{a}_n; \\ \alpha &\mapsto (\alpha \pmod{\mathfrak{a}_1}, \ldots, \alpha \pmod{\mathfrak{a}_n}). \end{aligned}$$

The kernel consists of $\alpha \in \mathbb{Z}_K$ mapping to $(0,\ldots,0)$.

I.e., it consists of those α such that $\alpha \in \mathfrak{a}_i$, for each i.

This is the intersection $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$.

We must show that θ is surjective.

We can write $1 = \alpha_i + \beta_i$, where $\alpha_i \in \mathfrak{a}_i$, and $\beta_i \in \mathfrak{a}_j$, for all $j \neq i$.

In the case $i = 1$, $\mathfrak{a}_1 + \mathfrak{a}_i = \mathbb{Z}_K$, for all $i \neq 1$.

So we can write $1 = x_i + y_i$ for $x_i \in \mathfrak{a}_1$, $y_i \in \mathfrak{a}_i$.

Chinese Remainder Theorem (Cont'd)

- Then
$$y_2 y_3 \cdots y_n = (1-x_2)(1-x_3)\cdots(1-x_n).$$
Write, for each $i = 2, \ldots, n$,
$$\beta_1 = y_2 y_3 \cdots y_n \in \mathfrak{a}_i.$$
Expand the right-hand side.
We get an expression $1-\alpha_1$, where all the terms defining α_1 are divisible by some $x_i \in \mathfrak{a}_1$. So $\alpha_1 \in \mathfrak{a}_1$.
Now, let
$$(x_1, \ldots, x_n) \in \mathbb{Z}_K/\mathfrak{a}_1 \oplus \cdots \oplus \mathbb{Z}_K/\mathfrak{a}_n.$$
Then
$$\theta(x_1\beta_1 + \cdots + x_n\beta_n) = (x_1, \ldots, x_n).$$
Hence, θ is surjective.
- We have not used any properties of number fields here.
So this result is valid for any commutative ring.

Subsection 6

Norms of Ideals

Norm of an Ideal

Definition

The **norm** $N_{K/\mathbb{Q}}(\mathfrak{a})$ of a non-zero ideal $\mathfrak{a}$ in $\mathbb{Z}_K$ is the cardinality $|\mathbb{Z}_K/\mathfrak{a}|$. It is finite by a previous lemma.

- We have two notions of norm, one for elements and one for ideals.
- For principal ideals, generated by a single element, these two notions are related.

Norm of a Principal Ideal

Lemma

Let $\alpha \in \mathbb{Z}_K$ be non-zero. Then

$$N_{K/\mathbb{Q}}(\langle \alpha \rangle) = |N_{K/\mathbb{Q}}(\alpha)|.$$

- Let $\mathbb{Z}_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$.
  Then $\langle \alpha \rangle = \mathbb{Z}\alpha\omega_1 + \cdots + \mathbb{Z}\alpha\omega_n$.
  Then $N_{K/\mathbb{Q}}(\langle \alpha \rangle) = |\mathbb{Z}_K/\langle \alpha \rangle|$.
  Write $\alpha\omega_i = \sum_{j=1}^{n} a_{ji}\omega_j$.
  Then the index of $\langle \alpha \rangle$ in $\mathbb{Z}_K$ is just $|\det(a_{ij})|$.
  But we know that $N_{K/\mathbb{Q}}(\alpha) = \det(a_{ij})$.
  So we see that $N_{K/\mathbb{Q}}(\langle \alpha \rangle) = |N_{K/\mathbb{Q}}(\alpha)|$.

The Norm of Prime Ideals

Lemma

Suppose that $\mathfrak{a}$ is a non-zero ideal of $\mathbb{Z}_K$ and that $\mathfrak{p}$ is a non-zero prime ideal of $\mathbb{Z}_K$. Then

$$|\mathbb{Z}_K/\mathfrak{p}| = |\mathfrak{a}/\mathfrak{a}\mathfrak{p}|.$$

- Suppose, for some $\mathfrak{b}$, $\mathfrak{a} \supseteq \mathfrak{b} \supseteq \mathfrak{a}\mathfrak{p}$.

  Then, multiplying through by $\mathfrak{a}^{-1}$ gives $\mathbb{Z}_K \supseteq \mathfrak{a}^{-1}\mathfrak{b} \supseteq \mathfrak{p}$.

  As $\mathfrak{p}$ is a non-zero prime ideal, it is maximal.

  So either $\mathfrak{a}^{-1}\mathfrak{b} = \mathbb{Z}_K$ or $\mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{p}$.

  This shows that $\mathfrak{b} = \mathfrak{a}$ or $\mathfrak{a}\mathfrak{p}$.

The Norm of Prime Ideals (Cont'd)

- Fix $\alpha \in \mathfrak{a}$, but not in $\mathfrak{ap}$.

  Consider the ideal generated by α and $\mathfrak{ap}$.

  It is clearly contained in $\mathfrak{a}$, but is strictly bigger than $\mathfrak{ap}$.

  So it must equal $\mathfrak{a}$.

  Define the map

$$\begin{array}{rccc} \phi: & \mathbb{Z}_K & \to & \mathfrak{a}/\mathfrak{ap}; \\ & x & \mapsto & \alpha x + \mathfrak{ap}. \end{array}$$

  ϕ is a homomorphism of $\mathbb{Z}_K$-modules.

  It is surjective by the above remark.

  The kernel clearly contains $\mathfrak{p}$, since if $x \in \mathfrak{p}$, then $\alpha x \in \mathfrak{ap}$.

  But $1 \notin \ker\phi$, as $\phi(1) = \alpha + \mathfrak{ap}$ and $\alpha \notin \mathfrak{ap}$.

  As $\mathfrak{p}$ is maximal, we see that $\ker\phi = \mathfrak{p}$.

  By the First Isomorphism Theorem for modules, $\mathbb{Z}_K/\mathfrak{p} \cong \mathfrak{a}/\mathfrak{ap}$.

The Norm is Multiplicative

Theorem

Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals of $\mathbb{Z}_K$. Then

$$N_{K/\mathbb{Q}}(\mathfrak{a}\mathfrak{b}) = N_{K/\mathbb{Q}}(\mathfrak{a})N_{K/\mathbb{Q}}(\mathfrak{b}).$$

- By factorizing $\mathfrak{b}$ into prime ideals, it suffices to deal with the case that $\mathfrak{b} = \mathfrak{p}$, a prime ideal, and to show that $N_{K/\mathbb{Q}}(\mathfrak{a}\mathfrak{p}) = N_{K/\mathbb{Q}}(\mathfrak{a})N_{K/\mathbb{Q}}(\mathfrak{p})$.
  Consider the homomorphism

$$\begin{array}{rccc} \phi: & \mathbb{Z}_K/\mathfrak{a}\mathfrak{p} & \to & \mathbb{Z}_K/\mathfrak{a}; \\ & \alpha+\mathfrak{a}\mathfrak{p} & \mapsto & \alpha+\mathfrak{a}. \end{array}$$

  It is clearly surjective.
  Its kernel is the set

$$\mathfrak{a}/\mathfrak{a}\mathfrak{p} = \{\alpha+\mathfrak{a}\mathfrak{p} : \alpha \in \mathfrak{a}\}.$$

The Norm is Multiplicative (Cont'd)

- By applying the First Isomorphism Theorem we see that

$$\left|\frac{\mathbb{Z}_K/\mathfrak{ap}}{\mathfrak{a}/\mathfrak{ap}}\right| = |\mathbb{Z}_K/\mathfrak{a}|.$$

Thus,

$$|\mathbb{Z}_K/\mathfrak{ap}| = |\mathbb{Z}_K/\mathfrak{a}| \cdot |\mathfrak{a}/\mathfrak{ap}|.$$

The previous lemma now gives

$$|\mathbb{Z}_K/\mathfrak{ap}| = |\mathbb{Z}_K/\mathfrak{a}| \cdot |\mathbb{Z}_K/\mathfrak{p}|.$$

The definition of the ideal norm gives

$$N_{K/\mathbb{Q}}(\mathfrak{ap}) = N_{K/\mathbb{Q}}(\mathfrak{a})N_{K/\mathbb{Q}}(\mathfrak{p}).$$

Subsection 7

The Class Group

Summary of Known Results

- We now know several important results:
  - Elements in rings of integers of number fields do not generally factorize uniquely into irreducible elements.
  - Every domain in which all ideals are principal (a principal ideal domain) is one where we do have unique factorization of elements (a unique factorization domain).
  - Ideals in rings of integers of number fields always factorize uniquely into prime ideals.
  - As a consequence, if unique factorization fails, some ideals are not principal.
    This serves as a test for uniqueness or non-uniqueness of factorization.
- We also know that the fractional ideals form a group.
- Using this, we can construct a group which measures the success or failure of uniqueness of factorization.

Test for Unique Factorization

- Suppose that K is a number field, with ring of integers $\mathbb{Z}_K$.
- Form the collection of all ideals,

$$\mathfrak{I}_K = \{\text{ideals in } \mathbb{Z}_K\}.$$

- Every element $\alpha \in \mathbb{Z}_K$ generates a principal ideal, $\langle \alpha \rangle = \alpha \mathbb{Z}_K$.
- So we can form the collection

$$\mathfrak{P}_K = \{\text{principal ideals in } \mathbb{Z}_K\} \subseteq \mathfrak{I}_K.$$

- Unique factorization would follow from the equality $\mathfrak{P}_K = \mathfrak{I}_K$.
- If this does not happen, it can be useful to:
  - Quantify the extent to which it fails;
  - Estimate what proportion of ideals are principal.

The Class Group

- We write

$$\begin{aligned} \mathfrak{F}_K &= \{\text{fractional ideals of } \mathbb{Z}_K\}; \\ \mathfrak{PF}_K &= \{\text{principal fractional ideals of } \mathbb{Z}_K\}. \end{aligned}$$

- Then $\mathfrak{F}_K$ forms a group, as already noted.
- $\mathfrak{PF}_K$ is also a group, since its elements are simply $\alpha\mathbb{Z}_K$, for $\alpha \in K$.
- Since $\mathfrak{F}_K$ is abelian, every subgroup is normal.
- The quotient group

$$C_K = \mathfrak{F}_K/\mathfrak{PF}_K$$

  is called the **class group** of K.
- If C_K is the trivial group, then $\mathfrak{F}_K = \mathfrak{PF}_K$.

  Intersecting with the collection of genuine ideals of $\mathbb{Z}_K$ gives $\mathfrak{I}_K = \mathfrak{P}_K$.

  This implies unique factorization.

The Class Number

- We will prove that the class group

$$C_K = \mathfrak{F}_K / \mathfrak{P}\mathfrak{F}_K$$

  is always finite.
- The **class number** h_K is the number of elements in C_K.
- It measures the proportion of ideals which are principal.
- When the class number is 1, this means that C_K is trivial.

  So every ideal is principal.

  In this case, we have unique factorization.
- When the class number is h_K, the proportion of ideals which are principal is $\frac{1}{h_K}$.

The Canonical Homomorphism Associated With C_K

- There is clearly a surjective group homomorphism

$$\mathfrak{F}_K \to C_K = \frac{\mathfrak{F}_K}{\mathfrak{P}\mathfrak{F}_K},$$

  sending a fractional ideal $\mathfrak{f}$ to its class $[\mathfrak{f}] \in C_K$.
- We will usually just use this in the case where $\mathfrak{f}$ is a genuine ideal.
- Since this is a homomorphism, for all (fractional) ideals $\mathfrak{a}$ and $\mathfrak{b}$,

$$[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}].$$

A Property of C_K

- By Lagrange's Theorem, the order of every element in a group divides the order of the group.
- Suppose $\mathfrak{a}$ is a (fractional) ideal in $\mathbb{Z}_K$.
- $\mathfrak{a}$ belongs to a class $[\mathfrak{a}] \in C_K$.
- Moreover, $[\mathfrak{a}^{h_K}] = [\mathfrak{a}]^{h_K}$ is trivial.
- Thus, $\mathfrak{a}^{h_K}$ is in the class consisting of all principal fractional ideals.
- So $\mathfrak{a}^{h_K}$ is principal for any $\mathfrak{a}$.

Subsection 8

Splitting of Primes

Cardinality of Finite Fields

Clam: Finite fields must have cardinality p^f, for some prime number p and some exponent f.

Suppose k is a finite field.

Consider the sequence

$$1, 1+1, 1+1+1, \ldots.$$

Now k has only finitely many elements.

So eventually the sequence must repeat.

Subtracting the shorter expression from the longer gives a sum

$$1 + \cdots + 1 = 0.$$

That is, for some number n, we must have $n = 0$ in the field.

Cardinality of Finite Fields (Cont'd)

- Let n is the smallest positive integer with this property.

  It is easy to see that n must be prime.

  Suppose $n = rs$ and $n = 0$ in the field.

  Fields have no non-trivial zero-divisors.

  Then either r or s must be 0.

  By the minimality of n, we cannot have $1 < r < n$ or $1 < s < n$.

  Thus, k contains a copy of $\mathbb{F}_p$, the finite field of integers modulo p (sometimes denoted $\mathbb{Z}_p$ or $\mathbb{Z}/p\mathbb{Z}$).

  k can be regarded as a field extension of $\mathbb{F}_p$.

  That is, k is a vector space over $\mathbb{F}_p$.

  But $\mathbb{F}_p$ has p elements.

  So any vector space over it has p^f elements, where $f := [k : \mathbb{F}_p]$.

Prime Ideals and Prime Numbers

- Suppose that K is a number field.
- Let $\mathfrak{p}$ be a non-zero prime ideal in $\mathbb{Z}_K$.
- By a previous lemma, $\mathbb{Z}_K/\mathfrak{p}$ is a finite field.
- So $\mathbb{Z}_K/\mathfrak{p}$ has cardinality p^f, for some prime number p and some exponent f.
- The norm of $\mathfrak{p}$ is p^f.
- We say that $\mathfrak{p}$ **lies above** p, or that p **lies below** $\mathfrak{p}$.

Prime Numbers and Prime Ideals

- Conversely, we can find prime ideals in $\mathbb{Z}_K$ by trying to factor primes $p \in \mathbb{Z}$ in $\mathbb{Z}_K$.

  Example: Suppose $K = \mathbb{Q}(i)$.

  We know that $\mathbb{Z}_K = \mathbb{Z}[i]$.

  We can factor the first few primes as follows:

$$2 = (1+i)(1-i), \quad 3 = 3, \quad 5 = (2+i)(2-i), \quad 7 = 7, \quad \ldots$$

  We notice that some primes can be factorized and some cannot.

Working with Ideals in $\mathbb{Z}[i]$

- Suppose $p = (a+bi)(c+di)$.

  The product has no imaginary part.

  So we need $c+di = a-bi$.

  Hence, $p = a^2 + b^2$.

  So the primes which are the sums of squares (which we know to be $p = 2$ and $p \equiv 1 \pmod 4$) will factor.

  The primes which are not sums of squares (the primes $p \equiv 3 \pmod 4$) will not factor.

Working with Ideals in $\mathbb{Z}[i]$ (Cont'd)

- These representations are not unique.

  We also have $5 = (1+2i)(1-2i)$.

  This is easily seen to be an equivalent to $5 = (2+i)(2-i)$.

  The factors differ by units.

  We know that we can avoid this by working with ideals instead.

  Note that $\langle 1+i \rangle = \langle 1-i \rangle$ (as $1+i = i(1-i)$).

  Set:

  - $\mathfrak{p}_2 = \langle 1+i \rangle$, of norm 2;
  - $\mathfrak{p}_3 = \langle 3 \rangle$, a prime ideal in $\mathbb{Z}[i]$, of norm 9;
  - $\mathfrak{p}_5 = \langle 2+i \rangle$ and $\mathfrak{p}_5' = \langle 2-i \rangle$, prime ideals, of norm 5.

  The factorizations so far become

$$\langle 2 \rangle = \mathfrak{p}_2^2, \quad \langle 3 \rangle = \mathfrak{p}_3, \quad \langle 5 \rangle = \mathfrak{p}_5 \mathfrak{p}_5', \quad \langle 7 \rangle = \mathfrak{p}_7.$$

- These three primes demonstrate the three different sorts of factorization possible in $K = \mathbb{Q}(i)$, or indeed in any quadratic field.

Types of Factorization in Quadratic Fields

- In a quadratic field, the following things can happen.

Definition

Let p a prime, and suppose that K is a quadratic field.

- We say that p **splits** in K if $p\mathbb{Z}_K = \mathfrak{p}\mathfrak{p}'$, for two ideals $\mathfrak{p} \neq \mathfrak{p}'$ of norm p.
- We say that p is **inert** in K if $p\mathbb{Z}_K$ is a prime ideal in $\mathbb{Z}_K$, necessarily of norm p^2.
- We say that p is **ramified** in K if $p\mathbb{Z}_K = \mathfrak{p}^2$, for a prime ideal $\mathfrak{p}$ of norm p.

Arbitrary Number Fields

- There are similar definitions for any number field K.
- However, for arbitrary number fields some combination of these may occur.
- It may be, e.g., that in some higher degree number field,

$$p\mathbb{Z}_K = \mathfrak{p}^2\mathfrak{p}'.$$

This shows aspects of:

- Ramification (because of the exponent of $\mathfrak{p}$);
- Splitting (as there is more than one distinct prime ideal appearing).

In case the norms of $\mathfrak{p}$ or $\mathfrak{p}'$ were greater than p, there would also be aspects of inert behavior.

Ramification Indices and Inertia Degrees

- If p is a prime number in $\mathbb{Z}$, consider $\langle p \rangle = p\mathbb{Z}_K$.
  This is an ideal in $\mathbb{Z}_K$.
  It factorizes uniquely as a product $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ of prime ideals in $\mathbb{Z}_K$.
  In the expression
  $$p\mathbb{Z}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$
  the exponents e_i are called the **ramification indices**.
- As $\mathfrak{p}_i$ is prime in $\mathbb{Z}_K$, the quotient $\mathbb{Z}_K/\mathfrak{p}_i$ is a finite field, for each i.
  $\mathbb{Z}_K/\mathfrak{p}_i$ is a field extension of $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.
  So both fields have the same characteristic.
  We define $f_i = [\mathbb{Z}_K/\mathfrak{p}_i : \mathbb{F}_p]$ to be the **inertia degree**.
- Note that
  $$N_{K/\mathbb{Q}}(\mathfrak{p}_i) = |\mathbb{Z}_K/\mathfrak{p}_i| = p^{f_i}.$$

The Case of Quadratic Fields

- We revisit the case of quadratic fields.
- A prime p *splits* if $\langle p \rangle = \mathfrak{p}\mathfrak{p}'$.

  Both $\mathfrak{p}$ and $\mathfrak{p}'$ have ramification index and inertia degree equal to 1.
- A prime p is *inert* if $\langle p \rangle$ is a prime ideal.

  It has ramification index 1 and inertia degree 2.
- A prime p is *ramified* if $\langle p \rangle = \mathfrak{p}^2$.

  $\mathfrak{p}$ has ramification index 2 and inertia degree 1.

The Degree of a Number Field

Theorem

Let K be a number field of degree n. Suppose that $p\mathbb{Z}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, and that $f_i = [\mathbb{Z}_K/\mathfrak{p}_i : \mathbb{F}_p]$. Then

$$n = \sum_{i=1}^{r} e_i f_i.$$

- By the Chinese Remainder Theorem, we have

$$\mathbb{Z}_K/p\mathbb{Z}_K \cong \bigoplus_{i=1}^{r} \mathbb{Z}_K/\mathfrak{p}_i^{e_i}.$$

All these are vector spaces over $\mathbb{F}_p$.

The Degree of a Number Field (Cont'd)

Claim: We have

$$\dim_{\mathbb{F}_p} \mathbb{Z}_K/p\mathbb{Z}_K = n \quad \text{and} \quad \dim_{\mathbb{F}_p} \mathbb{Z}_K/\mathfrak{p}_i^{e_i} = e_i f_i.$$

Indeed, since $p \in \mathbb{Z}$,

$$|\mathbb{Z}_K/p\mathbb{Z}_K| = p^{[K:\mathbb{Q}]} = p^n.$$

This gives the first claim.

Furthermore, using a previous theorem,

$$|\mathbb{Z}_K/\mathfrak{p}_i^{e_i}| = N_{K/\mathbb{Q}}(\mathfrak{p}_i^{e_i}) = N_{K/\mathbb{Q}}(\mathfrak{p}_i)^{e_i} = (p^{f_i})^{e_i}.$$

This gives the second claim.

Factorization of $p\mathbb{Z}_K$

Proposition

Suppose that K is a number field, and that $\mathbb{Z}_K = \mathbb{Z}[\gamma]$. Write $g(X) \in \mathbb{Z}[X]$ for its minimal polynomial.
Let p be a prime in $\mathbb{Z}$, and let

$$\overline{g}(X) = \overline{g}_1(X)^{e_1} \cdots \overline{g}_r(X)^{e_r}$$

be the factorization of the minimal polynomial g modulo p of γ into irreducibles. Then

$$p\mathbb{Z}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

for certain distinct ideals $\mathfrak{p}_i$ of $\mathbb{Z}_K$. The inertia degree of $\mathfrak{p}_i$ is simply given by the degree of $\overline{g}_i(X)$.

- Let $g_i(X)$ denote any polynomial whose reduction modulo p is $\overline{g}_i(X)$.

Factorization of $p\mathbb{Z}_K$ (Cont'd)

- Define the ideal

$$\mathfrak{p}_i = \langle p, g_i(\gamma) \rangle.$$

Then $\mathbb{Z}_K/\mathfrak{p}_i = \mathbb{Z}[\gamma]/\langle p, g_i(\gamma)\rangle$.
Consider the map $\mathbb{Z}[X] \to \mathbb{Z}[\gamma]$ induced by $X \mapsto \gamma$.
It has kernel $\langle g(X)\rangle$. It induces $\mathbb{Z}[X]/\langle g(X)\rangle \cong \mathbb{Z}[\gamma]$.
Thus,

$$\mathbb{Z}[\gamma]/\langle p, g_i(\gamma)\rangle \cong \mathbb{Z}[X]/\langle g(X), p, g_i(X)\rangle.$$

Consider the homomorphism $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ got by reducing mod p.
It gives an iso

$$\mathbb{Z}[X]/\langle g(X), p, g_i(X)\rangle \cong \mathbb{F}_p[X]/\langle \overline{g}(X), \overline{g}_i(X)\rangle.$$

But $\overline{g}_i(X)$ divides $\overline{g}(X)$.
So the quotient $\mathbb{F}_p[X]/\langle \overline{g}(X), \overline{g}_i(X)\rangle$ is just $\mathbb{F}_p[X]/\langle \overline{g}_i(X)\rangle$.
Combining all these isos, we get $\mathbb{Z}_K/\mathfrak{p}_i \cong \mathbb{F}_p[X]/\langle \overline{g}_i(X)\rangle$.

Factorization of $p\mathbb{Z}_K$ (Cont'd)

- We got $\mathbb{Z}_K/\mathfrak{p}_i \cong \mathbb{F}_p[X]/\langle \overline{g}_i(X)\rangle$.
  As $\overline{g}_i(X)$ is irreducible, the right-hand side is a field.
  So $\mathfrak{p}_i$ is a prime ideal.
  Similarly, there are isomorphisms

$$\mathbb{Z}_K/p\mathbb{Z}_K \cong \mathbb{Z}[\gamma]/p\mathbb{Z}[\gamma] \cong \mathbb{Z}[X]/\langle p, g(X)\rangle \cong \mathbb{F}_p[X]/\langle \overline{g}(X)\rangle.$$

  The Chinese Remainder Theorem implies that

$$\mathbb{F}_p[X]/\langle \overline{g}(X)\rangle \cong \mathbb{F}_p[X]/\langle \overline{g}_1(X)^{e_1}\rangle \times \cdots \times \mathbb{F}_p[X]/\langle \overline{g}_r(X)^{e_r}\rangle.$$

  The map $\mathbb{Z}_K \to \mathbb{Z}_K/p\mathbb{Z}_K$ has kernel $p\mathbb{Z}_K$.
  Using the above isomorphism, we can view this as

$$\mathbb{Z}_K \to \mathbb{F}_p[X]/\langle \overline{g}_1(X)^{e_1}\rangle \times \cdots \times \mathbb{F}_p[X]/\langle \overline{g}_r(X)^{e_r}\rangle.$$

Factorization of $p\mathbb{Z}_K$ (Cont'd)

- The map

$$\mathbb{Z}_K \to \mathbb{F}_p[X]/\langle \overline{g}_1(X)^{e_1}\rangle \times \cdots \times \mathbb{F}_p[X]/\langle \overline{g}_r(X)^{e_r}\rangle$$

has kernel $p\mathbb{Z}_K$.
Unraveling the components above, the map is given by

$$\gamma \mapsto (X,\ldots,X).$$

So the kernel is

$$\langle p, g_1(\gamma)^{e_1}\rangle \cap \cdots \cap \langle p, g_r(\gamma)^{e_r}\rangle.$$

Note that the generators of $\mathfrak{p}_i^{e_i} = \langle p, g_i(\gamma)\rangle^{e_i}$ are all divisible by p except for $g_i(\gamma)^{e_i}$ itself. Therefore, $\mathfrak{p}_i^{e_i} \subseteq \langle p, g_i(\gamma)^{e_i}\rangle$.
Combining, we get

$$p\mathbb{Z}_K = \langle p, g_1(\gamma)^{e_1}\rangle \cap \cdots \cap \langle p, g_r(\gamma)^{e_r}\rangle \supseteq \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}.$$

Factorization of $p\mathbb{Z}_K$ (Cont'd)

- We got

$$p\mathbb{Z}_K = \langle p, g_1(\gamma)^{e_1}\rangle \cap \cdots \cap \langle p, g_r(\gamma)^{e_r}\rangle \supseteq \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}.$$

  The norm of the left-hand side is p^n.

  The norm of the right-hand side is $(p^{f_1})^{e_1}\cdots(p^{f_r})^{e_r}$.

  These two are the same, by the preceding theorem.

  It follows that the inclusion is an equality.

  So $p\mathbb{Z}_K = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$.

- The proof shows that we can take

$$\mathfrak{p}_i = \langle p, g_i(\gamma)\rangle = p\mathbb{Z}_K + g_i(\gamma)\mathbb{Z}_K.$$

(Un)ramified Prime Ideals and Primes

- Let $\mathfrak{p}_i$ be a prime ideal of $\mathbb{Z}_K$ above a prime p.
- Consider the decomposition

$$p\mathbb{Z}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

- $\mathfrak{p}_i$ is **unramified** if its exponent in the decomposition is $e_i = 1$.
- If $e_i > 1$, we say that $\mathfrak{p}_i$ is **ramified**.
- We say that the prime p is **unramified** if

$$e_1 = \cdots = e_r = 1.$$

- Otherwise, p is **ramified**.

Ramified Primes

Proposition

If K is a number field, then there are only finitely many primes p which are ramified in K. Indeed, p is ramified in K if and only if p divides D_K.

- By a previous proposition,

$$p\mathbb{Z}_K = \langle p, f_1(\gamma)\rangle^{e_1} \times \cdots \times \langle p, f_r(\gamma)\rangle^{e_r}.$$

By definition, p ramifies in K if and only if some $e_i > 1$.

Thus, the polynomial $\overline{f}(X)$ does not have distinct roots modulo p.

But these primes are the ones that divide the discriminant of $f(X)$.

Under the assumption that $\mathbb{Z}_K = \mathbb{Z}[\gamma]$, the discriminant of $f(X)$ is equal to D_K, by a previous example.

Remark

- We have seen that it is not always possible to find elements γ such that $\mathbb{Z}_K = \mathbb{Z}[\gamma]$, although they exist when K is a quadratic field.
- We shall see further examples ("cyclotomic fields") later where such elements exist.
- More generally, we can pick any element $\gamma \in \mathbb{Z}_K$, such that $K = \mathbb{Q}(\gamma)$.
- It may be shown that the factorization proposition holds more generally in this setting for the primes p not dividing $|\mathbb{Z}_K/\mathbb{Z}[\gamma]|$.
- The last proposition remains valid:

  p ramifies in the number field K if and only if p divides the discriminant of K.

Example

- We have given a rather complicated proof that $K = \mathbb{Q}(\sqrt{-2}, \sqrt{-5})$ does not have an integral basis of the form $\{1, \gamma, \gamma^2, \gamma^3\}$ (i.e., that K is not monogenic).
- The proof was a less clear version of the following proof.
- Suppose that $\mathbb{Z}_K = \mathbb{Z}[\gamma]$.

  By the Factorization Proposition, the factorization of $\langle 3 \rangle = 3\mathbb{Z}_K$ corresponds to the factorization of the minimal polynomial f of γ modulo 3.

  Recall that, for $K = \mathbb{Q}(\sqrt{-2}, \sqrt{-5})$, $\langle 3 \rangle$ factors as the product of 4 distinct prime ideals in $\mathbb{Z}_K$.

  The proposition implies that f must factor into 4 distinct linear factors modulo 3.

  But there are only 3 irreducible linear polynomials modulo 3, which gives a contradiction.

Subsection 9

Primes in Quadratic Fields

Quadratic Fields

- Consider the case of a quadratic field $K = \mathbb{Q}(\sqrt{d})$, where d is a squarefree integer.
- Quadratic fields are monogenic.
- So they have the property that $\mathbb{Z}_K = \mathbb{Z}[\gamma]$, for some $\gamma \in \mathbb{Z}_K$.
- So all the results of the previous section are valid.
- By the preceding proposition, the primes p which ramify in K are those which divide the discriminant D_K.
- Recall that

$$D_K = \begin{cases} d, & \text{if } d \equiv 1 \pmod 4, \\ 4d, & \text{otherwise.} \end{cases}$$

- We can see how $p\mathbb{Z}_K$ factorizes into prime ideals using a previous proposition, at least for p odd.
- As already noted, p ramifies in K when $p \mid D_K$.

Primes in Quadratic Fields

- For $d \equiv 2,3 \pmod 4$, we know

$$\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}].$$

- Moreover, the minimal polynomial of d is just $X^2 - d$.
- This quadratic has discriminant $4d$.
- Then a prime p factorizes in $\mathbb{Z}_K$ in the same way that $X^2 - d$ factorizes modulo p.
  - p is split in $\mathbb{Z}[\sqrt{d}]$ iff $X^2 - d$ factors into two linear factors mod p. That is, iff $X^2 - d$ has two (distinct) roots modulo p.
    I.e., if $\left(\frac{d}{p}\right) = 1$.
  - p is inert in $\mathbb{Z}[\sqrt{d}]$ if and only if $X^2 - d$ has no root mod p.
    I.e., if $\left(\frac{d}{p}\right) = -1$.

Primes in Quadratic Fields (Cont'd)

- For $d \equiv 1 \pmod 4$,
$$\mathbb{Z}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right].$$
- The minimal polynomial of $\frac{1+\sqrt{d}}{2}$ is $X^2 - X + (\frac{1-d}{4})$.
- This polynomial has discriminant d.
- The results are identical with the previous case.
- A prime p not dividing D_K is:
  - Split if and only if $\left(\frac{d}{p}\right) = 1$;
  - Inert if and only if $\left(\frac{d}{p}\right) = -1$.

Quadratic Reciprocity and Reduction mod D_K

- Using Quadratic Reciprocity, it is not hard to see that these conditions are characterized by congruence conditions modulo D_K.

  Example: In the case $K = \mathbb{Q}(i)$, with $d = -1$, we have $D_K = -4$.

  - A prime p is split if and only if $\left(\frac{-1}{p}\right) = 1$.
    It is well-known that this is equivalent to $p \equiv 1 \pmod 4$.
  - A prime p is inert if and only if $\left(\frac{-1}{p}\right) = -1$.
    This is equivalent to $p \equiv 3 \pmod 4$.

  Example: Let $K = \mathbb{Q}(\sqrt{-3})$, with $D_K = -3$.

  - A prime p is split if and only if $\left(\frac{-3}{p}\right) = 1$.
    This is equivalent to $p \equiv 1 \pmod 3$.
  - It is inert if and only if $\left(\frac{-3}{p}\right) = -1$.
    This is equivalent to $p \equiv 2 \pmod 3$.