Introduction to Algebraic Number Theory 2020 Note, Ross Program

Scott Xu

Contents

0 Introduction

This course is hosted by professor Paul Pollack during the 2020 Ross Mathematics Program. The organization of the whole course and the problems in this note is taken from his lectures, problem sets and problem sessions.

The two-week course after the usual analytic number theory sessions aims to give a short introduction on algebraic number theory, and particularly, how ideas in the algebraic number theory applies to the quadratic fields. (The content of the course will be updated after the course is finished as the note is updated.)

I studied the style of the LaTeX note by Evan Chen's *An Infinitely Large Napkin*, which is open-source on Github.

1 Introduction to Algebraic Number Theory, Ross Program 2020

§1.1 Lecture 1, July 29

Definition 1.1.1 (Algebraic Number)
$\alpha \in \mathbb{C}$ is called an algebraic number iff it's a root of some nonzero polynomial in $\mathbb{Q}[x]$. We denote the set of all algebraic numbers as $\bar{\mathbb{Q}}$.

Definition 1.1.2 (Algebraic Integer)
An algebraic integer $\alpha \in \mathbb{C}$ is the root of some monic polynomial in $\mathbb{Z}[x]$. We denote the set of all algebraic integers as $\bar{\mathbb{Z}}$.

In summary, we have $\bar{\mathbb{Z}} \subset \bar{\mathbb{Q}} \subset \mathbb{C}$. We can also check that $\bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. This leads us to the general discussions about number fields.

Definition 1.1.3 (Number Field)
A number field is a field of the form $\mathbb{Q}[\theta]$ where $\theta \in \bar{\mathbb{Q}}$.

For example, $\mathbb{Z}[i], \mathbb{Q}[i], \mathbb{Q}[\omega]$ are all number fields.

Definition 1.1.4
If K is a number field, the ring of integers of K is defined to be $\bar{\mathbb{Z}} \cap K$. For example, the ring of integers of $\mathbb{Q}$ is just $\mathbb{Z}$.

The reason why we want to study the ring of integers instead of all algebraic integers is that there are "too many" numbers to be studied. One observation is that $\bar{\mathbb{Z}}$ has no irreducible, because for any non-unit $\alpha \in \bar{\mathbb{Z}}$, $\sqrt{\alpha}$ is also in $\bar{\mathbb{Z}}$. (Definition of units and irreducibles will be given in Lecture 2.)

§1.2 Problem Session 1, July 30

Problem 1.2.1
$\bar{\mathbb{Z}}$ is a ring and $\bar{\mathbb{Q}}$ is a field.

Proof. We want to borrow the **Fundamental Theorem of Symmetrical Functions** here.

Lemma 1.2.2 (Fundamental Theorem of Symmetrical Functions)
Let R be a ring and let $P(x_1, x_2, \cdots, x_n) \in R[x_1, x_2, \cdots, x_n]$ be a symemtric polynomial. Then $P(x_1, x_2, \cdots, x_n) = G(s_1, s_2, \cdots, s_n)$ for some polynomial G with coefficients from R. s_i denotes the i-th elementary symmetrical function in $x_1, x_2, \cdots, x_n$, i.e., the sum of all products of i terms in $x_1, x_2, \cdots, x_n$.

Now we prove that $\mathbb{Z}$ is closed under addition and multiplication. The closure of $\mathbb{Q}$ can be proved in a similar way. Suppose that α_1 and β_1 are roots of $P(x)$ and $Q(x)$, respectively. And suppose that $P(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_t)$ and $Q(x) = (x-\beta_1)(x-\beta_2)\cdot(x-\beta_s)$. We now find the polynomial $S(x)$ where

$$S(x) = \prod_{1\le i\le t, 1\le j\le s} (x - (\alpha_i + \beta_j))$$

and its coefficients should lie in $\mathbb{Z}$ using Lemma 1.2.2 twice. Similarly we can construct

$$T(x) = \prod_{1\le i\le t, 1\le j\le s} (x - \alpha_i\beta_j)$$

to prove the multiplicative closure. □

Problem 1.2.3
It's known that the sum $1 + \sqrt{2} + \sqrt[3]{3} + \cdots + \sqrt[100]{100}$ lies strictly between 111 and 112. Explain how we can quickly deduce that the sum is irrational. (From what we've already known)

Proof. Because $\bar{\mathbb{Z}}$ is a ring, and each of the elements in the sum is in $\bar{\mathbb{Z}}$, the number is also in $\bar{\mathbb{Z}}$. Suppose by contradiction that it's in $\mathbb{Q}$, then it's in $\bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$, which is impossible because it lies between two integers. Thus, the sum is irrational. □

Problem 1.2.4

Exhibit a monic polynomial in $\mathbb{Q}[x]$ which has $\sin(2\pi/7)$ as a root.
Exhibit a monic polynomial in $\mathbb{Z}[x]$ which has $2\cos(2\pi/9)$ as a root.

Proof. For the first problem, notice that

$$(\cos\frac{2\pi}{7}+\sin\frac{2\pi}{7}i)^7=e^{2\pi i}=1$$

$$\sum_{j=0}^{7}\binom{7}{j}\cos^j\frac{2\pi}{7}(\sin^{7-j}\frac{2\pi}{7})i^{7-j}=1$$

Because both sides represent a real number, the term when j is even can be treated as 0. When j is odd, $7-j$ is even, so we can represent $\cos^2(2\pi/7)$ by $1-\sin^2(2\pi/7)$. This generates a monic polynomial in $\mathbb{Q}[x]$ which has $\sin(2\pi/7)$ as a root.
For the second problem, let $\zeta=e^{2\pi i/9}$ denote the ninth root of unity. Then

$$2\cos\frac{2\pi}{9}=\zeta+\bar{\zeta}=\zeta+\zeta^{-1}$$

As $\zeta^9=1$ and $\zeta\neq 1$, we also have

$$\zeta^8+\zeta^7+\cdots+\zeta+1=0$$

$$(\zeta^4+\zeta^{-4})+(\zeta^3+\zeta^{-3})+\cdots+1=0$$

Because each $\zeta^k+\zeta^{-k}$ can be represented by a polynomial of $\zeta+\zeta^{-1}$, we have now found a monic polynomial for our $\zeta+\zeta^{-1}$, which is $2\cos(2\pi/9)$. □

Problem 1.2.5

Show that $\sin 1^\circ$ is an algebraic number.

Proof. The proof is similar to Problem 1.2.4. □

Problem 1.2.6

Show that $\bar{\mathbb{Q}}$ is a fraction field of $\bar{\mathbb{Z}}$. That is (it remains to show that), every number in $\bar{\mathbb{Q}}$ can be represented as the fraction of two numbers in $\bar{\mathbb{Z}}$.

Proof. For any $\alpha\in\bar{\mathbb{Q}}$, it's a root to the polynomial $P(x)=a_nx^n+\cdots+a_1x+a_0$ (we can let $a_n=1$ so that the polynomial is monic). Let L denotes the least common multiplier of the denominators of a_i's written in their reduced form. Now, $P(L\alpha)=L^n(P(\alpha))=0$ gives Lx is a root of the monic polynomial $L^nP(x)$ in $\mathbb{Z}[x]$. Therefore, $L\alpha\in\bar{\mathbb{Z}}$. Because L is trivially in $\bar{\mathbb{Z}}$, we have $\alpha=L\alpha/L$ as the desired form. □

Problem 1.2.7
Is $1/(3+\sqrt{2})$ an algebraic integer? How to characterize the units in $\bar{\mathbb{Z}}$?

Proof. For the first problem, if $\alpha = 1/(3+\sqrt{2})$ is an algebraic integer, then $\bar{\alpha} = 1/(3-\sqrt{2})$ is also an algebraic integer. (This can be easily checked by the knowledge of polynomial and "conjugate" roots, or viewing the map from one root to its conjugate as a ring automorphism). Because $\bar{\mathbb{Z}}$ is a ring, we know that $\alpha\bar{\alpha} = 1/7$ is also in $\bar{\mathbb{Z}}$, contradiction.
For the second problem, the units in $\bar{\mathbb{Z}}$ can be characterize as "those α with minimal polynomial ending with constant term ± 1". (Equivalently, the product of all its conjugates should be ± 1). □

§1.3 Lecture 2, July 31

Recall that the study of algebraic integers focuses on $\bar{\mathbb{Z}} \cap K := \mathbb{Z}_K$, called the ring of integers of K, where $K = \mathbb{Q}[\theta]$ for some $\theta \in \bar{\mathbb{Q}}$. Now we restrict our discussion on those K such that θ is a root of a degree-two polynomial.

Definition 1.3.1 (Quadratic Number Field)
A quadratic number field is of the form $\mathbb{Q}[\theta]$ where θ is a root of a degree-two polynomial in $\mathbb{Q}[x]$ and $\theta \notin \mathbb{Q}$.

If the polynomial given in the definition is $P(x) = ax^2 + bx + c$, then we can express θ as $\dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ where $D := b^2 - 4ac$ is a non-square. Then actually $\mathbb{Q}[\theta] = \mathbb{Q}[\sqrt{D}]$. Moreover, we can uniquely determine $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{D'}]$ where D' is not only non-square but also square-free. (Given as exercise)
Another remark is on the convention of $\sqrt{d}$: when $d < 0$, this represents $i \cdot \sqrt{|d|}$.
Now let $\alpha \in \mathbb{Q}[\sqrt{d}]$ with $d \neq 1$ being square-free. Then $\alpha = x + y\sqrt{d}$ with x, y uniquely determined. Define $\bar{\alpha} = x - y\sqrt{d}$.

Remark 1.3.2. $\alpha \in \bar{\mathbb{Z}} \Leftrightarrow \alpha + \bar{\alpha} \in \mathbb{Z}, \alpha\bar{\alpha} \in \mathbb{Z}$.

Proof. ($\Rightarrow$) $\alpha \in \bar{\mathbb{Z}}$ implies $\bar{\alpha} \in \bar{\mathbb{Z}}$, $\alpha + \bar{\alpha} \in \bar{\mathbb{Z}}$. On the other hand, $\alpha + \bar{\alpha} \in \mathbb{Q}$. Therefore, $\alpha + \bar{\alpha} \in \bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. By the same argument, $\alpha\bar{\alpha} \in \mathbb{Z}$.
($\Leftarrow$) α is the root of the polynomial $P(x) = (x - \alpha)(x - \bar{\alpha})$ and $P(x) \in \mathbb{Z}[x]$. Thus, $\alpha \in \bar{\mathbb{Z}}$. □

Remark 1.3.3 (Traces and Norms in quadratic field)**.** $\mathrm{Tr}(\alpha) = \alpha + \bar{\alpha}$, $N(\alpha) = \alpha\bar{\alpha}$.

Definition 1.3.4 (Unit)
An $\alpha \in \mathbb{Z}_K$ is called a unit if there exists $\beta \in \mathbb{Z}_K$ such that $\alpha\beta = 1$.

Definition 1.3.5 (Irreducible)
A $\pi \in \mathbb{Z}_K$ is irreducible (an irreducible) if π is a non-zero, non-unit element and if $\pi = \alpha\beta, \alpha, \beta \in \mathbb{Z}_K$ implies either α or β is a unit.

Definition 1.3.6 (Unique Factorization Domain, UFD)
Let R be an integral domain (a commutative ring with no zero divisors.) R is a UFD if $\forall \alpha \in R$, α being a non-zero and non-unit, α can be uniquely expressible as $\alpha = \pi_1\pi_2\cdots\pi_k$ where the π_i's are irreducibles.

Example 1.3.7 (A classical example of a non-UFD)
$\mathbb{Z}[\sqrt{-5}]$ is not a UFD, as $6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

Some exercises that characterize the quadratic field, its units and the unique factorization will be included in next section as exercises.

The problem with the non-UFD domains is that "there are not enough numbers". For example, a famous "four-number theorem" is valid in $\mathbb{Z}$: if $ab = cd$ and $\gcd(a,b,c,d) = 1$, then we can write $a = (a,c)(a,d)$, $b = (b,c)(b,d)$, $c = (a,c)(b,c)$, $d = (a,d)(b,d)$, where (m,n) denotes the $\gcd(m,n)$. However, the theorem is not true in $\mathbb{Z}[\sqrt{-5}]$ for the four irreducible factors in Example 1.3.7 because $\gcd(2, 1+\sqrt{-5})$ doesn't exist.
The way that we "restore" the unique factorization in these fields is to introduce new "numbers" that play the role of "$(2, 1+\sqrt{-5})$", etc.

§1.4 Problem Session 2, August 1

Problem 1.4.1
Prove the Four Numbers Theorem: Suppose a, b, c, d are positive integers with $ab = cd$ and $\gcd(a,b,c,d) = 1$. Then:

$$a = (a,c)(a,d), b = (b,c)(b,d), c = (a,c)(b,c), d = (a,d)(b,d).$$

Proof. Let $a = (a,c)m, c = (a,c)n$ where $(m,n) = 1$. Let $b = (b,d)t, d = (b,d)s$ where $(t,s) = 1$. Then $ab = cd$ gives $mt = ns$, which gives $m = s, n = t$.

Now we have $a = (a,c)m, d = (b,d)m$. $m \mid a, d$ gives $m \mid (a,d)$. On the other hand, $(a,d) \mid a$ and $(a,d) \mid d$ gives $(a,d) \mid m(a,c)$ and $(a,d) \mid m(b,d)$. Therefore, $(a,d) \mid \gcd((a,c),(b,d)) = m$. Together we get $m = (a,d)$. Similarly, $n = (b,c)$ and we are done. □

Problem 1.4.2

Show that if K is a quadratic field, then $K = \mathbb{Q}[\sqrt{d}]$ for some squarefree integer d. Show further that d is uniquely determined.

Problem 1.4.3

Suppose $K = \mathbb{Q}[\sqrt{d}]$ where $d \neq 1$ is a squarefree integer. Show that if $d \equiv 2, 3 \pmod 4$, then

$$\mathbb{Z}_K = \left\{ a + b\sqrt{d} : a, b \in \mathbb{Z} \right\} = \mathbb{Z}[\sqrt{d}]$$

while if $d \equiv 1 \pmod 4$, then

$$\mathbb{Z}_K = \left\{ \frac{a + b\sqrt{d}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod 2 \right\} = \mathbb{Z}\left[\frac{1 + \sqrt{d}}{2} \right]$$

Proof. Recall Remark 1.3.2: $\alpha \in \bar{\mathbb{Z}} \Leftrightarrow \alpha + \bar{\alpha} \in \mathbb{Z}, \alpha\bar{\alpha} \in \mathbb{Z}$. It suffices to check the latter claim. Let $\alpha = m + n\sqrt{d}$ where $m, n \in \mathbb{Q}$, then for $\alpha \in \mathbb{Z}_K$, we need

$$2m \in \mathbb{Z}, m^2 - dn^2 \in \mathbb{Z}$$

Thus, we write $m = t/2, n = p/q$ where $t, p, q \in \mathbb{Z}, \gcd(p,q) = 1$. This reduces to

$$\frac{t^2}{4} - \frac{p^2 d}{q^2} \in \mathbb{Z}$$

If $q = 1$, then $2 \mid t$. If $q = 2$, then $4 \mid t^2 - p^2 d$. When $d \equiv 1 \pmod 4$, we now that t and p can have the same parity (the second case in the problem). Otherwise, both t and q should be even. If $q > 2$, the number above cannot be in $\mathbb{Z}$.
The argument shows that for α to be in $\mathbb{Z}_K$, it has to satisfy $m, n \in \mathbb{Z}$ when $d \equiv 2, 3 \pmod 4$ and $2m, 2n \in \mathbb{Z}$ where $2m \equiv 2n \pmod 2$. We now check that for all number that satisfy the condition, it's really in $\mathbb{Z}_K$. This can be check by

$$(x - \alpha)(x - \bar{\alpha}) \in \mathbb{Z}[x]$$

in either case. □

Problem 1.4.4 (Units when $d < 0$)

Let $K = \mathbb{Q}[\sqrt{d}]$ where $d < 0$ and d squarefree. Show that:

- When $d \neq -1, -3$, the (only) units of $\mathbb{Z}_K$ are ± 1.
- When $d = -1$, the units are $\pm 1, \pm i$.
- When $d = -3$, the units are $\pm 1, \pm\omega, \pm\omega^2$ where $\omega = e^{2\pi i/3}$.

This is easily checked by the above problem and consider the fact that the norm of the unit is 1.

Problem 1.4.5 (Units when $d > 1$)

Let $K = \mathbb{Q}[\sqrt{d}]$ where $d > 1$ and d squarefree. Show that:

- If $\epsilon = x + y\sqrt{d} > 1$ is a unit, then $x, y > 0$.
- The set of units of $\mathbb{Z}_K$ that are larger than 1 has a smallest element.
- Let ϵ_0 be the unit you found in part (b). Show that every unit of $\mathbb{Z}_K$ has a unique expression in the form $\pm\epsilon_0^n$. ϵ_0 is called the "fundamental unit".

Proof. First, $x^2 - dy^2 = \pm 1$ gives $\epsilon|\bar{\epsilon}| = 1$. We know that $|\bar{\epsilon}| < 1/\epsilon < \epsilon$

$$x = \frac{\epsilon + \bar{\epsilon}}{2} > \frac{1}{2}(1 - 1) = 0$$

$$y = \frac{\epsilon - \bar{\epsilon}}{2\sqrt{d}} > \frac{1}{2\sqrt{d}}(\epsilon - \epsilon) = 0$$

The second claim is similar to the Well-Ordering principal by noticing we have to compare the pair $(x, y) \in \mathbb{Z}^2$ or $(2x, 2y) \in \mathbb{Z}^2$. We can first pick the smallest y by considering $\{2y\} \subset \mathbb{Z}$ and then argue that the corresponding x should also be the smallest.
The third claim is a direct consequnce of the second one by noticing that the units are multiplicative. If there are some unit $u > 1$ and $u \in (\epsilon_0^k, \epsilon_0^{k+1})$, then $u\epsilon_0^{-k}$ is a unit in $(1, \epsilon_0)$, contradiction. □

Example 1.4.6

The fundamental units in $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Z}[\sqrt{5}]$ and $\mathbb{Z}[\sqrt{7}]$ are $1 + \sqrt{2}, 2 + \sqrt{3}, (1 + \sqrt{5})/2, 8 + 3\sqrt{7}$, respectively.

Remark 1.4.7. A better procedure to calculate the units of these quadratic fields is to use the continued fractions.

Problem 1.4.8

Suppose that $d \equiv 1 \pmod 4$is squarefree, $d \neq 1$. Show that the ring $\mathbb{Z}[\sqrt{d}]$ does not have unique factorization.

Proof. Let $d = 4t + 1$ where $t \in \mathbb{Z}$.

$$(\sqrt{d}+1)(\sqrt{d}-1) = d - 1 = 2 \cdot (2t)$$

but $2 \nmid (\sqrt{d}+1)$, $2 \nmid (\sqrt{d}-1)$ and 2 is an irreducible (there is no solution to $x^2 - y^2 d = 2$ in this case). □

Problem 1.4.9

Let K be a field and let R be a subring of K having K as its fraction field. (This means that every element of K is a quotient of two elements of R.) Suppose that R is a unique factorization domain. Prove that if $a \in K$ is a root of a monic polynomial in $R[x]$, then $a \in R$. What does this have to do with the last exercise?

Proof. The proof is analogous to the "rational root theorem" where $\mathbb{Q}$ and $\mathbb{Z}$ are used instead of K and R. With this hindsight, we let $R = \mathbb{Z}[\sqrt{d}]$ and $K = \mathbb{Q}[\sqrt{d}]$. When $d \equiv 1 \pmod 4$, $\dfrac{1+\sqrt{d}}{2}$ doesn't belong to R, but it is a root of the polynomial

$$\left(x - \frac{1+\sqrt{d}}{2}\right)\left(x - \frac{1-\sqrt{d}}{2}\right) = x^2 - x + \frac{1-d}{4} \in R[x]$$

Thus, $\mathbb{Z}[\sqrt{d}]$ is not a UFD. □

Remark 1.4.10. This explains why $\mathbb{Z}_K$ is the right to study for it better ensures unique factorization.

§1.5 Lecture 3, August 3

The goal of today's lecture is to find out the "missing numbers" that can take the place of the gcd.

Definition 1.5.1
Let R be an integral domian. For each $\alpha \in R$, denote $\langle \alpha \rangle = \{\alpha\beta : \beta \in R\}$.

We can easily check that $\langle \alpha_1 \rangle = \langle \alpha_2 \rangle$ if and only if $\alpha_1 = \alpha_2 u$ for some unit $u \in R$. Therefore, we can treat the $\langle \alpha_i \rangle$'s as a partition of R under the equivalence relation.

Definition 1.5.2 (Ideal)
Let R be any commutative ring. A subset I of R is called an ideal if I satifies the following properties:

- $0 \in I$.
- I is closed under addition.
- I "absorbs" multiplication from R. For all $\gamma \in I$, $r \in R$, we have $\gamma r \in I$.

We can also replace the first condition by $I \neq \varnothing$ to insure that there really is some element in I for the third properties to make sense.

Example 1.5.3
The ideals in $\mathbb{Z}$ are of the form $\langle a \rangle = a\mathbb{Z}$.

Definition 1.5.4 (principal Ideal, principal Ideal Domain (PID))
If there is an ideal $\langle a \rangle = R$ in the domain R, we call the ideal a "principal ideal" and the domain a "principal Ideal Domain" (PID).

Example 1.5.5 (Non-principal ideals)
Let $R = \mathbb{Z}[x]$ and let $I = \{f(x) \in \mathbb{Z}[x] : 2 \mid f(0)\}$. This is an ideal of $\mathbb{Z}[x]$ as we can check, but $1 \notin I$.
Let $R = \mathbb{Z}[\sqrt{-5}]$ and $I = \langle 2, 1+\sqrt{-5} \rangle$. I is not principal. If $I = \langle \alpha \rangle$ for some $\alpha \in R$, then $2 \in I \Rightarrow \alpha \mid 2$. Similarly, $\alpha \mid 1 + \sqrt{-5}$. But this gives $N(\alpha) | \gcd(4, 6) = 2$, making $N(\alpha) = 1$ and α is a unit. Then $I = R$. However, $1 \notin I$ (as we can check that the elements in I have even norms), contradiction.

Here, I can also be described as $\{xf(x) + 2g(x) : f(x), g(x) \in \mathbb{Z}[x]\} = \langle 2, x \rangle$. This lead us to the definition below and a harder question: how many elements we need to generate an ideal in $\mathbb{Z}[x]$?

Definition 1.5.6 (Ideal generated by a set of elements)
Let R be a ring and $\alpha_1, \alpha_2, \cdots, \alpha_n \in R$. Define $\langle \alpha_1, \alpha_2, \cdots, \alpha_n \rangle = \{\alpha_1\beta_1 + \cdots + \alpha_n\beta_n : \text{all } \beta_i \in R\}$. As we can check, this is also an ideal.

Definition 1.5.7 (Quotient Ring)
If R is a ring, define $\mathrm{Id}(R) = \{\text{nonzero ideals of } R\}$. If I, J are ideals of R, define $I + J = \{\alpha + \beta : \alpha \in I, \beta \in J\}$ and $IJ = \{\text{finite sums } \alpha_1\beta_1 + \cdots + \alpha_n\beta_n : \forall \alpha_i \in I, \beta_j \in J\}$. $\mathrm{Id}(R)$ is then called the quotient ring of R over I and is also denoted as R/I.

It can really be checked that $\mathrm{Id}(R)$ is a ring, and we will explore more of its properties through exercises after the lecture. Now, we are well equipped to replace the gcd's in our Four Number Theorem by the ideal generated by each of the two elements. And the theorem is now true for the ideals. For example, we can check that $\langle 3 \rangle = \langle 3, 1 + \sqrt{-5} \rangle \langle 3, 1 - \sqrt{-5} \rangle$.

$$\begin{aligned}
\text{RHS} &= \left\langle 3, 1 + \sqrt{-5} \right\rangle \left\langle 3, 1 - \sqrt{-5} \right\rangle \\
&= \left\langle 3 \times 3, 3 \times (1 - \sqrt{-5}), 3 \times (1 + \sqrt{-5}), (1 - \sqrt{-5})(1 + \sqrt{-5}) \right\rangle \\
&= \langle 3 \rangle \left\langle 3, 1 - \sqrt{-5}, 1 + \sqrt{-5}, 2 \right\rangle \\
&= \langle 3, 1 \rangle \\
&= \langle 3 \rangle
\end{aligned}$$

§1.6 Problem Session 3, August 4

Problem 1.6.1
Let R be a domain. Show that if R has a division algorithm, then every ideal of R has the form $\langle \alpha \rangle$ for some $\alpha \in R$. An ideal of this form is called principal.

Proof. Recall that we can continue the division algorithm until it terminates with a remainder ρ_k of the smallest possible norm before it becomes 0 (Euclidean Algorithm). It's easily checked that $R = \langle \rho_k \rangle$ in this case and R is a PID. □

Problem 1.6.2
Let I be the ideal of $\mathbb{Z}[x]$ described by $I = \{f(x) \in \mathbb{Z}[x] : f(0) \text{ is even } \}$. Prove that $I = \langle 2, x \rangle$.

Proof. For all $f(x)$ where $f(0)$ is even, we can do the division algorithm of monic polynomial in $\mathbb{Z}[x]$ to get $f(x) = xq(x) + r$ where $q(x) \in \mathbb{Z}[x]$ and r a constant. Then $r = 2k$ for some $k \in \mathbb{Z}$, and $f(x) = xq(x) + 2 \cdot k \in \langle 2, k \rangle$. On the other hand, any element in $\langle 2, k \rangle$ has an even constant term. □

Problem 1.6.3

Let R be a ring. Let S be any subset of R. Recall that $\langle \alpha \rangle_{\alpha \in S}$ is defined by $\{\text{all finite sums } c_1\alpha_1 + \cdots + c_k\alpha_k : c_1, \ldots, c_k \in R \text{ and } \alpha_1, \ldots, \alpha_k \in S\}$.
Show that $\langle \alpha \rangle_{\alpha \in S}$ is an ideal of R.

Problem 1.6.4

Let R be a ring. Recall that if I, J are ideals of R, we defined $I + J = \{\alpha + \beta : \alpha \in I, \beta \in J\}$, $IJ = \left\{ \text{finite sums } \sum_i \alpha_i\beta_i, \text{ where } \alpha_i \in I, \beta_i \in J \right\}$. Show that $I + J$ and IJ are ideals of R.

We can quickly check these two problems by chasing the definition of ideals.

Problem 1.6.5

Let $R = \mathbb{Z}[\sqrt{-5}]$ and let $I = \langle 2, 1 + \sqrt{-5} \rangle$. Show that $N(\alpha)$ is even for each $\alpha \in I$. Here $N(\cdot)$ is the norm function on $\mathbb{Q}[\sqrt{-5}]$.

Proof. Let $\alpha = 2s + (1 + \sqrt{-5})t \in I$. Then

$$\alpha = (2s + t) + t\sqrt{-5}$$

$$N(\alpha) = (2s + t)^2 + 5t^2$$

is even. □

Problem 1.6.6

Check the following basic properties of ideal operations in a ring R :

- Addition and multiplication are associative and commutative.
- $\langle 0 \rangle$ is the additive identity and $\langle 1 \rangle$ is the multiplicative identity.
- Multiplication distributes over addition: $I(J+K) = IJ + IK$.
- $IJ \subseteq I \cap J$.
- If $I = \langle \alpha_1, \ldots, \alpha_k \rangle, J = \langle \beta_1, \ldots, \beta_\ell \rangle$, then
$$IJ = \langle \alpha_1\beta_1, \ldots \alpha_1\beta_\ell, \ldots, \alpha_k\beta_1, \ldots, \alpha_k\beta_\ell \rangle$$
- If R is a domain and $I, J \neq \langle 0 \rangle$, then $IJ \neq \langle 0 \rangle$

For the fifth claim, we notice that the left hand side is a subset to the right hand side and vice versa, which proves that these two sets are equal.

Problem 1.6.7

Complete the verification that in $\mathbb{Z}[\sqrt{-5}]$, we have

$$\langle 2 \rangle = \langle 2, 1+\sqrt{-5} \rangle \langle 2, 1-\sqrt{-5} \rangle, \quad \langle 1+\sqrt{-5} \rangle = \langle 2, 1+\sqrt{-5} \rangle \langle 3, 1+\sqrt{-5} \rangle$$
$$\langle 3 \rangle = \langle 3, 1+\sqrt{-5} \rangle \langle 3, 1-\sqrt{-5} \rangle, \quad \langle 1-\sqrt{-5} \rangle = \langle 2, 1-\sqrt{-5} \rangle \langle 3, 1-\sqrt{-5} \rangle$$

One verification is done in the note for Lecture 3. The others are similar.

Problem 1.6.8

Now let $K = \mathbb{Q}[\sqrt{d}]$, where $d \in \mathbb{Z}$ is squarefree, $d \neq 1$. Put $\tau = \sqrt{d}$ when $d \neq 1 \pmod 4$, and put $\tau = \dfrac{1+\sqrt{d}}{2}$ when $d \equiv 1 \pmod 4$. Recall that every element of $\mathbb{Z}_K$ has a unique expression in the form $u + v\tau$ with $u, v \in \mathbb{Z}$. Let I be a nonzero ideal of $\mathbb{Z}_K$. Check that:

- Put $I_0 = I \cap \mathbb{Z}$. Show that I_0 is a nonzero ideal of $\mathbb{Z}$. It follows that $I_0 = n\mathbb{Z}$.
- Put $I_1 = \{b \in \mathbb{Z} : a + b\tau \in I \text{ for some } a \in \mathbb{Z}\}$. Show that I_1 is a nonzero ideal of $\mathbb{Z}$. Thus, $I_1 = B\mathbb{Z}$ for some positive integer B.
- since $B \in B\mathbb{Z} = I_1$, we can choose $A \in \mathbb{Z}$ with $A + B\tau \in I$. Show that $n, A + B\tau$ form a $\mathbb{Z}$-basis for I. That is, every element of I can be written uniquely in the form $un + v(A + B\tau)$ for integers u, v for some integer n, which can be chosen to be positive.

Proof. The first claim is easy to check by looking at the definition of ideals and the fact that all the ideals in $\mathbb{Z}$ are of the form $n\mathbb{Z}$. Plus, because I is not empty, there is some $\alpha \in I$ and $\alpha\bar{\alpha} \in I \cap \mathbb{Z}$. Therefore, I_0 is a non-zero ideal.

Now we prove the second claim. $0 \in I_1$ because I is non-empty. The addition closure and the multiplication "absorbing" property is also easy to check. Now Suppose that $I_1 = 0$, but we can pick $b \in I$ and $b\tau \in I_1$ with $b \neq 0$, giving the contradiction.

For the third claim, start from any $a + b\tau \in I$, but then $B \mid b$ because $b \in I_1$. Then, we can write $b = Bv$ where $v \in \mathbb{Z}$. Notice that $a + b\tau - v(A + B\tau) \in I$ gives $a - vA \in I$. So $a - vA \in I \cap \mathbb{Z} = n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Therefore, $a - vA = nu$ for some $u \in \mathbb{Z}$. Together this gives $a + b\tau = un + v(A + B\tau)$. □

Corollary 1.6.9

Let K be a quadratic field, and let I be a nonzero ideal of $\mathbb{Z}_K$ with standard basis $n, A + B\tau$. Show that $I = \langle n, A + B\tau \rangle$.

Actually, we can prove that every ideal of $\mathbb{Z}_K$ can be generated by two elements in any number fields K (but by a very different way).

Problem 1.6.10

How many elements does the ring $\mathbb{Z}[\sqrt{-5}]/\langle 3 \rangle$ have? Same question for $\mathbb{Z}[\sqrt{-5}]/\langle 3, 1+\sqrt{-5} \rangle$

Proof. We can show that in the first ring, $a + b\tau = c + d\tau$ implies $a \equiv c, b \equiv d \pmod 3$. This gives 9 elements in total. In the second ring by a similar argument, there are 3 elements. The second ring is isomorphic to $\mathbb{Z}_3$. □

§1.7 Lecture 4, August 4

The goal of today's lecture is to restore the Unique Factorization Theorem in any quadratic field $\mathbb{Z}_K$. The following lemma characterize a way to construct a principal ideal in $\mathbb{Z}_K$.

Lemma 1.7.1

For any $I \in \mathrm{Id}(\mathbb{Z}_K)$, $I\bar{I}$ is a principal ideal of $\mathbb{Z}_K$, where $\bar{I} = \{\bar{\alpha} : \alpha \in \mathbb{Z}_K\}$.

Proof. Recall in Problem Set 3 that I can be represented as $I = \langle \alpha, \beta \rangle$. Then

$$\begin{aligned} I\bar{I} &= \langle \alpha, \beta \rangle \langle \bar{\alpha}, \bar{\beta} \rangle \\ &= \langle N(\alpha), \alpha\bar{\beta}, \beta\bar{\alpha}, N(\beta) \rangle \end{aligned}$$

Observe that $I\bar{I}$ contains $N(\alpha), \mathrm{Tr}(\alpha\bar{\beta}), N(\beta)$, all of which are elements in $\mathbb{Z}$. We can let $n = \gcd(N(\alpha), \mathrm{Tr}(\alpha\bar{\beta}), N(\beta)$, and by the Euclidean algorithm, $I\bar{I} \subseteq \langle n \rangle$.
Now we show that $\langle n \rangle \subseteq I\bar{I}$. It suffices to check that $n \mid \alpha\bar{\beta}$ and $n \mid \beta\bar{\alpha}$. Let's check the first one and the second one will be similar.
It then suffices to show that $\dfrac{\alpha\bar{\beta}}{n} \in \mathbb{Z}_K$. Hence, we check the trace and norm of this number.

$$\mathrm{Tr}\left(\frac{\alpha\bar{\beta}}{n}\right) = \frac{\alpha\bar{\beta} + \bar{\alpha}\beta}{n} \in \mathbb{Z}$$

$$N\left(\frac{\alpha\bar{\beta}}{n}\right) = \frac{N(\alpha)N(\bar{\beta})}{n^2} \in \mathbb{Z}$$

And we are done by Remark 1.3.2.
To conclude, we proved that $I\bar{I} = \langle n \rangle$ where $n \in \mathbb{Z}$. □

Definition 1.7.2 (Irreducible Ideal)
An $P \in \mathrm{Id}(\mathbb{Z}_K)$ is irreducible if $P \neq \langle 1 \rangle$, and if whenever $P = AB$, either A or B is $\langle 1 \rangle$.

Now we can start to prove that there is UFT in $\mathrm{Id}(\mathbb{Z}_K)$. The existence is easy by using the WOP, and now we want to construct the "uniqueness" proof.

Lemma 1.7.3 (To Contain is to Divide)
Let $A, B \in \mathrm{Id}(\mathbb{Z}_K)$, then $A \mid B \Leftrightarrow A \supseteq B$.

Proof. ($\Rightarrow$) If $A \mid B$, then $B = AC$ for some $C \in \mathrm{Id}(\mathbb{Z}_K)$. Now $B = AC \subset A \cap C \subset A$.
($\Leftarrow$) Now suppose that $B \subset A$. We know that $A\bar{A} = \langle \alpha \rangle$ is a principal ideal. (If by chance $B = AC$, then we have $\bar{A}B = \langle \alpha \rangle C = \alpha C$, which is called a "dilation" of C. Then C should be $\alpha^{-1}\bar{A}B$.) We check that $A(\alpha^{-1}\bar{A}B) = B$, so $A \mid B$ ($\alpha^{-1}\bar{A}B$ is also an ideal). □

Now we want to fix the "Bezout's Theorem" so that we can prove the "Fundamental Lemma" on our ideal ring.

Theorem 1.7.4
Assume $P, A \in \mathrm{Id}(\mathbb{Z}_K)$ where $P \nmid A$ and P is an irreducible ideal. Then $P + A = \langle 1 \rangle$.

Proof. Since $0 \in A$, $P + A \supseteq P$. If $P + A = P$, then $P = P + A \sup A$, $P \mid A$, contradiction. Therefore, $P + A \supset P$, which gives $P + A = \langle 1 \rangle$. □

Now we are sure that there is UFT in $\mathrm{Id}(\mathbb{Z}_K)$. But why should we care?

Remark 1.7.5. $\mathbb{Z}_K$ is a PID $\Leftrightarrow$ $\mathbb{Z}_K$ is a UFD. (PID is UFD in general, but the backward claim is harder (TODO).)

Now let's consider the ring $\mathbb{Z}[\sqrt{-19}]$. This ring does not have a division algorithm regardless what the norm is, but we will show in the next lecture that it's still a UFD.

§1.8 Problem Session 4, August 4

Problem 1.8.1

Let I be a nonzero ideal of $\mathbb{Z}_K$. Suppose that $n, A + B\tau$ is a standard basis for I. Compute $\#\mathbb{Z}_K/I$, in terms of n, A, and B.

Proof. We claim that there are nB elements in the quotient ring. First, we prove that $\#\mathbb{Z}_K/I \neq nB$. For any $a + b\tau$, we can subtract a suitable $\mathbb{Z}$-multiple of $A + B\tau$ to get $a' + b'\tau$ where $0 \leq b < B$. We can then subtract a suitable $\mathbb{Z}$-multiple of n to get $a'' + b'\tau$ where $0 \leq a < n$. This will still be equivalent to $a + b\tau$, and together this gives at most nB elements.
Furthermore, the elements in the set $\{x + y\tau : 0 \leq x < n, 0 \leq y < B, x, y \in \mathbb{Z}\}$ are distinct. □

Problem 1.8.2

Show that $I\bar{I} = \langle m \rangle$, where $m = \#\mathbb{Z}_K/I$.

Proof. Using the above problem, we want to show that $I\bar{I} = \langle nB \rangle$ where n, B comes from the standard basis of I, which is $I = \langle n, a + b\tau \rangle$. Notice that

$$\begin{aligned} I\bar{I} &= \langle n, A + B\tau \rangle \langle n, A - B\tau \rangle \\ &= \left\langle n^2, n(A + B\tau), n(A - B\tau), (A + B\tau)(A - B\tau) \right\rangle \end{aligned}$$

Now it suffices to show that nB divides the four numbers in the angle bracket. We first introduce a lemma that $B \mid n$ and $B \mid A$.

Lemma 1.8.3

Suppose $I = \langle n, A + B\tau \rangle$ where $n, A + B\tau$ is the standard basis of I. Then $B \mid n$, $B \mid A$.

Proof. Because $n\tau \in I$, $B \mid n$ by the definition of B. Because

$$\tau^2 - \mathrm{Tr}(\tau)\tau + N(\tau) = 0$$

$$(A + B\tau)\tau = A + B(-N(\tau) + \mathrm{Tr}(\tau)) = (A + B\mathrm{Tr}(\tau))\tau - BN(\tau)$$

Because $A + B\mathrm{Tr}(\tau) \in I$, we have $B \mid A + B\mathrm{Tr}(\tau)$ and $B \mid A$. □

Back to the original problem: we now denote $n_0 = n/B$ and $a_0 = a/B$ and these are all integers by the lemma. Then, $I = \langle B \rangle \langle n_0, a_0 + \tau \rangle$ and $\bar{I} = \langle B \rangle \langle n_0, a_0 + \bar{\tau} \rangle$.

$$I\bar{I} = \left\langle B^2 \right\rangle \left\langle n_0^2, n_0(a_0 + \tau), n_0(a_0 - \tau), N(a_0 + \tau) \right\rangle$$

The $N(a_0+\tau)$ part can be absorbed in $\langle a_0 + \tau \rangle$. Moreover, $B \cdot N(a_0+\tau) \in \langle B \rangle \langle n_0, a_0 + \tau \rangle = I$. Therefore it's in $I \cap \mathbb{Z} = n\mathbb{Z}$. Dividing the B out, we get $n_0 \mid N(a_0 + r)$, and hence all the elements in the angle bracket of the expansion of $I\bar{I}$ are divisible by n_0.

$$I\bar{I} = \left\langle B^2 n_0 \right\rangle \left\langle n_0, (a_0 + \tau), (a_0 - \tau), \frac{N(a_0 + \tau)}{n_0} \right\rangle$$

Because $B^2 n_0 = nB$, it now suffices to show that the second ideal here is actually $\langle 1 \rangle$. Consider the ideal in $\mathbb{Z}$ generated by $n_0, \mathrm{Tr}(a_0 + \tau), \dfrac{N(a_0 + \tau)}{n_0}$. If this ideal doesn't contain 1, then these three numbers have a common divisor $d > 1$, but then

$$N\left(\frac{a_0 + \tau}{d}\right) \in \mathbb{Z}$$

$$\mathrm{Tr}\left(\frac{a_0 + \tau}{d}\right) \in \mathbb{Z}$$

This gives $\dfrac{a_0 + \tau}{d} \in \mathbb{Z}_K$, which is a contradiction to the definition of the $\mathbb{Z}$-basis.

□

Problem 1.8.4

Prove that for every nonzero $\alpha \in \mathbb{Z}_K$ we have $N(\langle \alpha \rangle) = |N(\alpha)|$. Here the norm on the left is the ideal norm and the norm on the right is the elementwise norm.

Proof. For a principal ideal $I = \langle \alpha \rangle$, $I\bar{I} = \langle \alpha \rangle \langle \bar{\alpha} \rangle = \langle N(\alpha) \rangle$. On the other hand, $I\bar{I} = \langle N(I) \rangle$. This gives

$$N(\alpha) = \pm N(\langle \alpha \rangle)$$
$$N(\langle \alpha \rangle) = |N(\alpha)|$$

□

Problem 1.8.5

Show that the ideal norm is multiplicative: $N(IJ) = N(I)N(J)$ for any two nonzero ideals I, J of $\mathbb{Z}_K$.

Proof. First, it's easy to check that $\overline{IJ} = \bar{I}\bar{J}$. Then

$$N(IJ) = IJ\overline{IJ} = (I\bar{I})(J\bar{J}) = N(I)N(J)$$

□

Problem 1.8.6

By WOPping on the norm (or otherwise), prove that every element of Id $(\mathbb{Z}_K)$ has a factorization into irreducible elements of Id $(\mathbb{Z}_K)$.

Proof. This is analogous to the proof of UFT in $\mathbb{Z}$. □

Problem 1.8.7

Show that for $P \in \mathrm{Id}(\mathbb{Z}_K)$, the following are equivalent:
(a) P is irreducible;
(b) whenever P divides AB for $A, B \in \mathrm{Id}(\mathbb{Z}_K)$, either P divides A or P divides B;
(c) whenever P contains AB for $A, B \in \mathrm{Id}(\mathbb{Z}_K)$, either P contains A or P contains B;
(d) $\mathbb{Z}_K/P$ is a field.

Proof. The equivalence of $(a)(b)(c)$ (equivalent meaning of "irreducible" and "prime") is addressed in the lecture as an analogus to the "Fundamental Lemma" of arithmetics in $\mathbb{Z}$. For $(a) \Leftrightarrow (d)$, we notice that P is an irreducible ideal and hence a maximal ideal. Now we can borrow the proof that I is a maximal ideal in commutative ring R iff R/I is a field. □

Problem 1.8.8

Show that if $\mathbb{Z}_K$ has unique factorization, and $\pi \in \mathbb{Z}_K$ is irreducible, then $\langle \pi \rangle$ is an irreducible ideal.

Proof. First, we claim that $N(\pi)$ is a rational prime. If $\pi\bar{\pi} = N(\pi) = mn$, then $\pi \mid m$ or $\pi \mid n$ because in a UFD (namely $\mathbb{Z}_K$), "prime is irreducible" for π. Then we have $\bar{\pi} \mid m$ or $\bar{\pi} \mid n$, which then gives $\pi\bar{\pi} \mid m$ or $\pi\bar{\pi} \mid n$. Therefore, either m or n should be 1.
Now notice that $N(\langle \pi \rangle) = |N(\pi)|$. If $\langle \pi \rangle = IJ$ for ideals I, J, then either $N(I)$ or $N(J)$ is 1, giving that either I or J is $\langle 1 \rangle$. Therefore, $\langle \pi \rangle$ is an irreducible ideal. □

Problem 1.8.9

Let K be a quadratic field. In this exercise we suppose that $\mathbb{Z}_K$ is a UFD and prove that every ideal of $\mathbb{Z}_K$ is principal.
(a) Reduce the claim to proving that every irreducible ideal is principal.
(b) Show that every irreducible ideal divides $\langle \pi \rangle$ for an irreducible element $\pi \in \mathbb{Z}_K$.
(c) Use Problem 7 and UFT in Id $(\mathbb{Z}_K)$ to conclude.

Proof. (a) follows from the fact that $\mathbb{Z}_K$ is a UFD. □

Problem 1.8.10

Prove that every irreducible ideal of $\mathbb{Z}_K$ divides $\langle p \rangle$ for some (positive) prime p from the ordinary integers $\mathbb{Z}$.

Proof. This is a corollary of part(b) of the problem above by noticing $\langle \pi \rangle \mid \langle N(\pi) \rangle$ where $N(\pi)$ must be a prime number. □

Problem 1.8.11

Let $K = \mathbb{Q}[\sqrt{-19}]$. Find a pair of $\alpha, \beta \in \mathbb{Z}_K$, with $\beta \neq 0$, such that for any $\gamma \in \mathbb{Z}_K$ one has $N(\alpha - \beta\gamma) > N\beta$.

Proof. Geometrically we can draw a lattice where we sent $a + b\sqrt{-19}$ to $(a, b\sqrt{19}) \in \mathbb{R}^2$. And then we notice that $\alpha = 1/2 + \sqrt{-19}$ and $\beta = 1$ satisfy the condition by visualizing the "norm" as the distance in the distorted complex plane in the lattice. □

Problem 1.8.12

(Motzkin) Recall that a domain R is said to possess a division algorithm (or be a Euclidean domain if there is a size function $n : R \to \mathbb{Z}^+ \cup \{0\}$ with the following property: For all $\alpha, \beta \in R$ with $\beta \neq 0$, there are $\gamma, \rho \in R$ with $\alpha = \beta\gamma + \rho$ and either $\rho = 0$ or $n(\rho) < n(\beta)$ Again, let $K = \mathbb{Q}[\sqrt{-19}]$. Suppose that $\mathbb{Z}_K$ has a division algorithm with $n(\cdot)$ the corresponding size function.
(a) Among all nonzero nonunits β, choose one for which $n(\beta)$ is as small as possible. Show that $\#\mathbb{Z}_K/\langle\beta\rangle \leq 3$. (b) Show that any nonzero nonunit $\beta \in \mathbb{Z}_K$ has $\#\mathbb{Z}_K/\langle\beta\rangle \geq 4$.

§1.9 Lecture 5, August 5

Let's recall that $\mathbb{Z}_K$ is UFD implies that every idael of $\mathbb{Z}_K$ is principal, which then means that "every irreducible ideal of $\mathbb{Z}_K$ is principal. (These are equivalent conditions.) We will use this fact to prove that $\mathbb{Z}_K$ is principal for $K = \mathbb{Q}[\sqrt{-19}]$ and $\mathbb{Z}_K = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$.
Also in the homework, we recall that P is an irreducible ideal is equivalent to the fact that $P \mid \langle p \rangle$ for some ordinary prime $p \in \mathbb{Z}$. The right terminology is "P lies above p". Now we explore how $\langle p \rangle$ actually factor in $\mathrm{Id}(\mathbb{Z}_K)$.
We notice that τ is a root of its minimal polynomial $x^2 - x + 5$. Therefore, P is an irreducible ideal means that $\mathbb{Z}_K/p$ is a field, which means that $\mathbb{Z}_p[x]_{x^2-x+5}$ is a field. This is true if and only if $x^2 - x + 5$ is an irreducible polynomial in $\mathbb{Z}_p$.

We can now check that the polynomial is irreducible mod 2 and 3, so $\langle 2\rangle$ and $\langle 3\rangle$ is irreducible themselves. For $\langle 5\rangle = P_1P_2\cdots P_k$, we have $25 = N(P_1)N(P_2)\cdots N(P_k) = 5\times 5$, forcing $k = 2$ and $N(P_1) = N(P_2) = 5$.

We can check that $\langle 5\rangle = \left\langle \frac{1+\sqrt{-19}}{2}\right\rangle\left\langle \frac{1-\sqrt{-19}}{2}\right\rangle$ is a factorization where each ideal on the right hand side is irreducible and principal. Similarly, we can factor $\langle 7\rangle = \left\langle \frac{3+\sqrt{-19}}{2}\right\rangle\left\langle \frac{3-\sqrt{-19}}{2}\right\rangle$ as a similar case. But is that enough to show that the ring is a PID?

Now let's prove that the ring is actually a PID. If there is a nonprincipal ideal in the ring, then there is a smallest p such that whenever we factor $\langle p\rangle$, we get a nonprincipal irreducible ideal P. By the above arguments, we know that $p > 7$, and suppose $\langle p\rangle = P_1P_2$ where $N(P_1) = N(P_2) = p$ where P_i are non-principal. We can also know that $x^2 - x + 5$ factors in $\mathbb{Z}_p$.

Now we claim that we can choose x between 1 and $(p+1)/2$ with $x^2-x+5 \equiv 0 \pmod p$. This is true because the two roots add up to get 1 mod$p$, so we can take one of them within the desired range. Notice that $x^2 - x + 5$ increases when $x \geq 1$, so

$$x^2 - x + 5 \leq \left(\frac{p+1}{2}\right)^2 - \frac{p+1}{2} + 5 \leq p^2$$

which works for $p > 2$. That's why we have to deal with the basic cases when $p = 2, 3, 5, 7$, and actually we've done more than enough.

On the other hand,

$$P \mid \langle p\rangle \mid \langle x^2 - x + 5\rangle = \langle x-\tau\rangle\langle x-\bar\tau\rangle$$

Because P is irreducible, it's also prime and $P \mid \langle x-\tau\rangle$ or $P \mid \langle x-\bar\tau\rangle$. Assume that the first one holds true, then $\langle x-\tau\rangle = PR$ for some ideal R. This gives $N(R) = N(x-\tau)/N(P) < p$.

Now we show that R must be principal! Let's take any irreducible ideal Q dividing R and $N(Q) < p$. We can choose q such that $Q \mid \langle q\rangle$ and thus $N(Q) \mid N(\langle q\rangle) = q^2$. Therefore, $N(Q) \geq q$ since it's not the trivial ideal, and we have $q \leq N(Q) \leq p$. Then Q is principal by the minimality of P, which means that any irreducible factor of R is principal, which makes R itself principal.

Let's denote $R = \langle\alpha\rangle$ and $x - \tau = P\langle\alpha\rangle = \alpha P$. This forces $\alpha \mid x-\tau$ in $\mathbb{Z}_K$, and $P = \left\langle \frac{x-\tau}{\alpha}\right\rangle$ is a principal ideal, contradiction!

We can actually extend this result into more general quadratic fields other than $\mathbb{Q}[\sqrt{-19}]$ introduced above (given in the problem set).