Math 243. Undergraduate Algebraic Number Theory.

Tom Sawada

June 7, 2019

Contents

1 Euclid's Proof and its Variants; Split Primes. - -Tuesday, 1.8.2019

1.1 Announcements.

1.) Homework due every Friday.
2.) Grading: HW 30, Midterm 30, Friday 40
3.) OH: Thursday 9am-11am at E308
4.) Notes: the courses will be related to this.
(a.) Tata

(b.) Pierre Simon
(c.) See canvas for notes from two years ago

Topics covered in this course are as follows.

1.) Prime numbers
2.) Primes in arithmetic progressions
3.) Quadratic number fields (emphasis on this)
4.) split primes

1.2 Prerequisites.

We assume the following results in this course:

Proposition 1. If F is a field, then then $F[x]$ is a PID.

Proposition 2. G is a subgroup of $F^\times$ under multiplication. If G is finite, then it is cyclic.

1.3 Euclid's Proof and its Variants.

We start with Euclid's proof of infinitude of primes.

PROOF 3. Suppose not, and let $p_1, ..., p_n$ are n distinct primes. Let

$$N := 1 + p_1...p_n > 1 \tag{1}$$

Then there is some prime q dividing it, so in particular $N \equiv 0 \mod q$. But since $N \equiv 1 \mod p_i$, we must have $q \neq p_1, ..., p_n$.

□

Proposition 4 (Dirichlet's Theorem of Arithmetic Progression.). Let $a, b \in \mathbb{N}$ mutually prime. Consider the arithmetic progression

$$a,\ a + b,\ a + 2b,\ a + 3b,\ ... \tag{2}$$

Then this contains infinitely many primes.

We will not prove this here, but instead look at some interesting special cases relevant to the course. (See Hardy & Wright or the Tata notes.)

Here is one:

Proposition 5. There are infinitely many primes which are $3 \mod 4$.

PROOF 6. This is a slight variation to Euclid's idea. There are n distinct primes that are $3 \mod 4$. We proceed by induction. $n = 0$ case is trivial.

Now let $p_1, ..., p_n$ be such primes. But since $3 \equiv -1 \mod 4$,

$$p_1...p_n \equiv (-1)^n \mod 4 \tag{3}$$

(For $n = 0$, we get $p_1...p_n = 1$) Now let

$$N := \begin{cases} 2 + p_1...p_n & n \text{ even} \\ 4 + p_1...p_n & n \text{ odd} \end{cases} \tag{4}$$

In both cases, $N \equiv 3 \mod 4$ and $N > 1$. Let q be a prime dividing N. Then $N \equiv 0 \mod q$, $N \equiv 2$ or $4 \neq 0 \mod p_i$.

Suppose $N = q_1 ... q_r$, q_i all primes. If all $q_i \equiv 1 \mod 4$, then $N \equiv 1 \mod 4$. Therefore, there exists i such that $q_i \equiv 3 \mod 4$.

□

Suppose now we want to prove there are infinitely many primes $\equiv 1 \mod 4$. Then we consider $N = 4 + p_1 ... p_n$, $N = q_1 ... q_r$ all primes. We cannot proceed with Euclid's argument alone. If all $q_i \equiv 3 \mod 4$ and r even, then $q_1 ... q_r \equiv 1 \mod 4$ and so we do not get a contradiction. Thus, we need some new idea.

Lemma. Let p be an odd prime. Then $p \equiv 1 \mod 4$ iff there exists $a \in \mathbb{Z}$ such that $p | 1 + a^2$.

PROOF 7. Suppose $p|1 + a^2$, p odd. Take

$$G := \{1, -1, \overline{a}, -\overline{a}\} \subseteq \mathbb{F}_p \tag{5}$$

Here, $a^2 \equiv -1 \mod p$. Then G is a subgroup of $\mathbb{F}_p^\times$ of order 4. We can prove this as follows:

Since p is odd, $\# \{-1, 1\}, \; \# \{-a, a\} = 2$. The two sets are disjoint because taking the square of the elements, the first set gives 1 whereas the second set gives -1.

Now by Lagrange's theorem (group theory), $4 | \# \mathbb{F}_p = p - 1$. This proves one direction (the one we need).

□

Proposition 8. There exists infinitely many primes p which are $\equiv 1 \mod 4$.

PROOF 9. Let $p_1 p_2 ... p_n$ be n such primes. Then take

$$N := 1 + 4(p_1 ... p_n)^2 \tag{6}$$

Then $N \equiv 1 \mod 4$ and $N > 1$. Let q be a prime that divides N. One direction of the lemma then gives $q \equiv 1 \mod 4$.

□

1.4 Split Primes.

Remark 10. Recall that polynomials can lose irreducibility with reduction mod p. For instance, $x^2 + 1 \in \mathbb{Z}[x]$ is irreducible, but $x^2 + 1 = (x - 2)(x + 2) \mod 5$.

Definition 11. Let $f \in \mathbb{Z}[x], \; d := \deg f > 1$. A **prime** p **is** f**-split** if there exists $a_1, ..., a_d \in \mathbb{Z}$ are distinct in $\mathbb{Z}/p\mathbb{Z}$ and

$$f(x) = (x - a_1) ... (x - a_d) \mod p \tag{7}$$

Example 12. For $f(x) = x^2 + 1$, from the lemma, p is f-split iff $p \equiv 1 \mod 4$. If there exists a such that $p | a^2 + 1$ then $x^2 + 1 \equiv (x - a)(x + a) \mod p$.

Remark 13. Finding the set of f-split primes (for a given f) is a major *unsolved* problem. (This belongs to the Langlands program.)

We look at special cases of this problem.

Example 14. Try $x^2 - 5$. Ignore $p = 2, 5$. (5 is silly because we get x^2.) Does there exist $a \in \mathbb{Z}$ such that $a^2 \equiv 5 \mod p$.

Let's start with $p = 3$. For this, $a \equiv \pm 1 \mod 3$ which implies $a^2 = 1 \mod 3$.

	1	4	9	16	25	36	49	64	81	100	Is there 5?
mod 7	1	4	2	2	4	1	...				No
mod 11	1	4	9	5	...						Yes
mod 13	1	4	9	3	-1	3	...				No
mod 13	...										No
mod 19	1	4	9	16	6	17	11	7	5		Yes

This follows from quadratic reciprocity.

Proposition 15 ((Special Case of) Quadratic Reciprocity.). Let $p \neq 2, 5$. There exists $a \in \mathbb{Z}$ such that $a^2 \equiv 5 \mod p$ iff $p \equiv \pm 1 \mod 5$.

Observe the power of this; this is much more efficient from the computation we did above with each individual a.

Next time: quadratic reciprocity.

2 Split Primes and Finite Fields. - -Wednesday, 4.3.2019

2.1 Announcements.

1.) OH Tues 5-6, Wed 4-5 at E 16
2.) PSession Tues 7-8

2.2 Split Primes: Examples.

We examine the following example today.

Question. What are the split primes for $x^n - 1$, i.e. when is

$$x^n - 1 = \prod_{i=1}^{n} (x - a_i) \tag{8}$$

in $\mathbb{F}_p[x]$ with all $a_i \in \mathbb{F}_p$ distinct.

Note that the roots form a group under multiplication contained in $\mathbb{F}_p^\times$. If p is split, we deduce that $n|p-1$ by Lagrange's theorem. Conversely, if $n|p-1$, because $\mathbb{F}_p^\times$ is cyclic, we see that $\mathbb{F}_p^\times$ contains a cyclic subgroup of order n. If the subgroup consists of n distinct elements $a_1, ..., a_n$, then these are the roots of $x^n - 1$.

Thus:

Proposition 16. p is split for $x^n - 1$ iff $p \equiv 1 \mod n$.

Now

$$x^n - 1 = (x-1)(x^{n-1} + ... + x + 1) \qquad n \geq 2 \tag{9}$$

Exercise. p is split for $x^{n-1} + ... + x + 1$ iff $p \equiv 1 \mod n$ for all $n \geq 3$.
The roots of $x^2 + x + 1 = 0$ is given by $\frac{-1+\sqrt{-3}}{2}$ which are on the unit circle. Now if we take $y := 2x + 1$, then we can rewrite this as $y^2 + 3 = 0$.

We claim that p is split for x^2+x+1 iff p is split for y^2+3 (where we ignore the case $p = 2$). Thus, factorizing $x^2 + x + 1 \in F[x]$, char$F \neq 2$ is "no different" from factoring $y^2 + 3 \in F[y]$. Then it follows that the split primes for $y^2 + 3$ is also $p \equiv 1 \mod 3$.

Proposition 17. $p \neq 3$ is a odd prime, then -3 is a square in $\mathbb{F}_p$ iff $p \equiv 1 \mod 3$.

Remark 18. This is one of the proofs of quadratic reciprocity. Gauss gave six of them. s

Now consider

$$x^4 + x^3 + x^2 + x + 1 = 0 \tag{10}$$

Let E be a field with char$E \neq 5$ which contains a root a of the above polynomial.

Dividing by a^2, we get

$$(a^2 + a^{-2}) + (a + a^{-1}) + 1 = 0 \tag{11}$$

Letting $b := a + a^{-1}$, we get

$$(b^2 - 2) + b + 1 = 0 \tag{12}$$

and we get

$$4b^2 + 4b + 1 = (2b+1)^2 = 5 \tag{13}$$

We now need to specify which field we are working in. Let p be a prime, and consider $\mathbb{F}^p$. Can we find $E/\mathbb{F}_p$ containing a a root as above?

More generally:

Proposition 19. If F is a field, $f \in F[x]$, $\deg f \geq 1$, then there exists E/F which contains a root a of f.

PROOF 20. This follows by the fact that $F[x]$ is a PID. Let $g \in F[x]$ be irreducible with $g|f$. Take $E := F[x]/(g)$. Take $\overline{x} \in F[x]/(f)$ be the image of x under the quotient homomorphism. If we take $a := \overline{x}$, then $g(a) = 0$, so $f(a) = 0$.

□

Thus, we have $(2a+1)^2 = 5$.

Proposition 21 (Frobenius Homomorphism.). If R is a commutative ring [1] . Assume that $p \cdot 1_R = 0$. Then

$$(u+v)^p = u^p + v^p \qquad u, v \in R \tag{14}$$

So in particular, the map $u \mapsto u^p$ is a ring homomorphism.

[1] In this course, all rings contain a 1.

Remark 22. Commutativity is crucial because we need binomial theorem.

PROOF 23. Binomial theorem and $p|\binom{p}{i},\ i \neq 0, p$.

□

Proposition 24. $\mathbb{F}_p$ is a subfield of a field E. Let $a \in E$. Then $a \in \mathbb{F}_p$ iff $a^p = a$.

PROOF 25. $\implies$ is Fermat's Little Theorem (or just from the previous proposition). For $\impliedby$, take $x^p - x \in E[x]$. This has p roots in $\mathbb{F}_p$, and $x^p - x$ can have at most p roots.

□

Now for $(2b+1)^2 = 5$, we claim that 5 is a square in $\mathbb{F}_p$ iff $(2b+1)^p = 2b+1$.

We know that $a^5 = 1$. Let $p \equiv k \mod 5$. Then our possibilities are $h = \pm 1, \pm 2$.

Then $a^p = a^h$, and $b = a + a^{-1}$, so

$$b^p = a^p + a^{-p} = a^h + a^{-h} \tag{15}$$

Now if $h = \pm 1$, we get $b^p = b$, so $b \in \mathbb{F}_p$, and thus, $2b + 1 \in \mathbb{F}_p$. Thus, we have shown that $p \equiv \pm 1 \mod 5$, then there exists $\alpha \in \mathbb{Z}$ such that $\alpha^2 \equiv 5 \mod p$.

Let's now consider $h = 2$. Then we get $a^p = a^2$, $b^p = a^2 + a^{-2}$. Thus,

$$0 = a^2 + a^{-2} + a + a^{-1} + 1 \tag{16}$$

Let $r := a^2 + a^{-2}$. Then $r + b + 1 = 0$, in particular $2r + 1 = -(2b+1)$.

In the homomorphism $x \mapsto x^p$ from E to itself, $b \mapsto r$ and $2b + 1 \mapsto 2r + 1 = -(2b+1) \neq 2b+1$. This concludes $h = 2$. The case $h = -2$ is similar.

We have thus proved

Proposition 26. $p \neq 2, 5$, then 5 is a square in $\mathbb{F}_p$ iff $p \equiv \pm 1 \mod 5$.

Now take an odd prime p, and consider the map $S_p : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ given by $z \mapsto z^2$. The kernel of this map is $\{\pm 1\}$. The cardinality of the image of this map is then $\frac{p-1}{2}$. These are the **quadratic residues**.

Proposition 27 (Euler). Let $0 \neq a \in \mathbb{F}_p$. Then a is a square iff $a^{\frac{p-1}{2}} = 1$ in $\mathbb{F}_p$.

PROOF 28. One direction is immediate: If $a = b^2$, then

$$a^{\frac{p-1}{2}} = (b^2)^{\frac{p-1}{2}} = b^{p-1} = 1 \tag{17}$$

Then $\mathbb{F}_p^\times$ is cyclic, so there exists $\alpha \in \mathbb{F}_p$ that has order $p-1$. Now since $\alpha^{\frac{p-1}{2}} \neq 1$, so $\alpha^{\frac{p-1}{2}} = -1$. The map $a \mapsto a^{\frac{p-1}{2}}$ is a homomorphism onto $\{\pm 1\} \subseteq \mathbb{F}_p^\times$.

□

3 Quadratic Residues and Quadratic Reciprocity. - -Friday, 4.5.2019

3.1 Legendre Symbol.

We start with a lemma.

Proposition 29. G is a cyclic group of order mn. Thene

$$H = \{g^m : g \in G\} \tag{18}$$

is a subgroup of order n. Here, $H = \ker\phi$ for $\phi : G \to G$ given by $\phi(g) = g^m$.

Remark 30. In particular, $G = \mathbb{F}_p^\times$, $m = 2$, $\frac{p-1}{2}$ then

$$\#\left\{a^2 : a \in \mathbb{F}_p^\times\right\} = \#(\mathbb{F}_p^\times)^2 = \frac{p-1}{2} \tag{19}$$

and $\mathbb{F}_p^\times = \ker\left(a \mapsto a^{\frac{p-1}{2}} = \pm 1\right)$.

Definition 31. Let $0 \neq a \in \mathbb{Z}$, let p be an odd prime. Then the **Legendre symbol**

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & p|a \\ 1 & (\exists b \in \mathbb{Z})(a \equiv b^2 \mod p) \text{ and } p \not| a \\ -1 & \text{otherwise} \end{cases} \tag{20}$$

Here is a corollary to the proposition:

Proposition 32.

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p \tag{21}$$

Remark 33. We know from last lecture that

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \tag{22}$$

and

$$\left(\frac{-3}{p}\right) = 1 \iff p \equiv 1 \mod 3 \tag{23}$$

and also

$$\left(\frac{5}{p}\right) = 1 \iff p \equiv \pm 1 \mod 5 \tag{24}$$

Recall that the proof of this last thing was to look at

$$a^4 + a^3 + a^2 + a + 1 = 0 \tag{25}$$

for $a \in E$ which taking $b = a + a^{-1}$ gives $(2b+1)^2 = 5$.

Remark 34 (Galois Theory.). Gauss observed that adjoining root of unity to a field gives adjoining square roots.

Example 35. For $\zeta^7 = 1$, $\zeta \neq 1$, taking linear combinations of powers of ζ gives $\sqrt{-7}$.

Remark 36 (Properties of Legendre Symbol.). The Legendre symbol gives a homomorphism, i.e. for all a, b

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \tag{26}$$

Thus, to know all Legendre symbols for p odd prime, it suffices to know

$$\left(\frac{-1}{p}\right), \left(\frac{2}{p}\right), \left(\frac{q}{p}\right) \tag{27}$$

for q odd prime.

This motivates the following theorem. Here is Gauss' quadratic reciprocity.

Proposition 37 (Quadratic Reciprocity.). Let p, q be distinct odd primes. Then

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \tag{28}$$

$$\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \mod 8 \tag{29}$$

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{30}$$

Remark 38. If both p, q are $\equiv 3 \mod 4$, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1 \tag{31}$$

Remark 39. Recall the proof for $\left(\frac{5}{p}\right)$. We can rewrite the expansion there using the above notation:

$$\begin{aligned} 2b + 1 &= (b+1) + b \\ &= -a^2 - a^3 + a + a^4 \\ &= \sum_k \left(\frac{k}{5}\right) a^k \end{aligned}$$

3.2 Proof of Quadratic Reciprocity via Gauss Sums.

PROOF 40 (Third Equality in Quadratic Reciprocity.). Let E be a field containing the primitive qth root of unity $\zeta \in E$. Then consider the **Gauss sum**

$$\begin{aligned} S &:= \sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \zeta^a \\ &= \sum_{a=1}^{q} \left(\frac{a}{q}\right) \zeta^a \end{aligned}$$

We claim that $S^2 = \left(\frac{-1}{q}\right) q$ in E. The claim implies the third equality since we know that $\mathbb{F}_p \subseteq E$ where E is a field and $b \in E$ such that

$$b^{q-1} + ... + b + 1 = 0 \tag{32}$$

The claim says we need to show that $\left(\frac{-1}{q}\right) q$ is a square in E. But by definition of the Legendre symbol,

$$\left(\frac{\left(\frac{-1}{q}\right) q}{p}\right) = 1 \iff S \in \mathbb{F}_p \tag{33}$$

by definition. But from last time, this holds iff $S^p = S$. Now if we look at the Frobenius homomorphism on E,

$$\begin{aligned} S^p &= \sum_{a=1}^{q-1} \left(\frac{a}{q}\right)^p b^{ap} \\ &= \sum_{a=1}^{q-1} \left(\frac{a}{q}\right) b^{ap} \qquad \text{since } \left(\frac{a}{q}\right) = \pm 1 \end{aligned}$$

But now, $a \mapsto ap$ is a bijection from $\mathbb{Z}/q\mathbb{Z}$ to itself. Thus,

$$\begin{aligned} &= \left(\frac{p}{q}\right) \sum_a \left(\frac{ap}{q}\right) b^{ap} \qquad \text{since } \left(\frac{p^2}{q}\right) = 1 \\ &= \left(\frac{p}{q}\right) \sum_b \left(\frac{b}{q}\right) \zeta^b \\ &= \left(\frac{p}{q}\right) S \end{aligned}$$

Therefore,

$$\left(\frac{\left(\frac{-1}{q}\right) q}{p}\right) = \left(\frac{p}{q}\right) \tag{34}$$

Now the LHS is $\left(\frac{\left(\frac{-1}{q}\right) q}{p}\right)\left(\frac{q}{p}\right)$. Thus, if

$$\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}} \tag{35}$$

then

$$\left(\frac{\left(\frac{-1}{q}\right) q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{36}$$

□

We still have not shown the claim.

Proof of Claim. Let

$$S = \sum_{a \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{a}{q}\right) \zeta^a \tag{37}$$

So,

$$S^2 = \sum_{a \in \mathbb{Z}/q\mathbb{Z}} \sum_{b \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{a}{q}\right) \left(\frac{b}{q}\right) \zeta^a \zeta^b \tag{38}$$

Now writing $c := a + b$, we can write

$$\begin{aligned} &= \sum_{c \in \mathbb{Z}/q\mathbb{Z}} \zeta^c \left(\sum_a \left(\frac{a}{q}\right) \left(\frac{c-a}{q}\right) \right) \\ &= \sum_{c \in \mathbb{Z}/q\mathbb{Z}} \zeta^c f(c) \end{aligned}$$

where

$$f(c) := \sum_{a \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{a(c-a)}{q}\right) \tag{39}$$

So, it suffices to compute the numbers $f(c)$. On the one hand, if $c \not\equiv 0 \mod q$

$$\begin{aligned} f(1) &= \sum_a \left(\frac{a(1-a)}{q}\right) \\ &= \sum_a \left(\frac{ca(c-ca)}{q}\right) && \left(\frac{c^2}{q}\right) = 1 \\ &= \sum_b \left(\frac{b(c-b)}{q}\right) && ca = b \end{aligned}$$

Thus, $f(1) = f(c)$ if $0 \neq c \in \mathbb{Z}/q\mathbb{Z}$.

Now

$$f(0) = \sum_{a=1}^{q-1} \left(\frac{a(-a)}{q}\right) = (q-1)\left(\frac{-1}{q}\right) \tag{40}$$

Then

$$\begin{aligned} S^2 &= (\zeta + \zeta^2 + \ldots + \zeta^{q-1}) f(1) + (q-1)\left(\frac{-1}{q}\right) \\ &= -f(1) + (q-1)\left(\frac{-1}{q}\right) \end{aligned}$$

We still have work to do since we do not know what $f(1)$ is.

We see that

$$T := \sum_{a \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{a}{q}\right) = 0 + \frac{q-1}{2} \cdot 1 + \frac{q-1}{2} \cdot (-1) = 0 \tag{41}$$

$$T^2 = \sum_c f(c) = (q-1)f(1) + \left(\frac{-1}{q}\right)(q-1) = 0 \tag{42}$$

So,

$$f(1) = -\left(\frac{-1}{q}\right) \tag{43}$$

Using this, we get

$$S^2 = q\left(\frac{-1}{q}\right) \tag{44}$$

as desired.

□

4 . - -Monday, 4.8.2019

4.1 Announcements.

1.) Homeworks due every Monday.
2.) See notes for details of previous lectures.
3.) Look at the two references online.
4.) Also see Vinogradov's elementary number theory book.

4.2 Solving $x^2 + y^2 = 1$ over $\mathbb{Q}$.

In the references, there is the following question: solve $x^2 + y^2 = z^2$ with integer solutions

$$\left\{(a,b,c) \in \mathbb{Z}^3 | a^2 + b^2 = c^2,\ \text{gcd}(a,b,c) = 1\right\} \tag{45}$$

We allow for a switch $(a,b) \mapsto (b,a)$.

Proposition 41. All solutions are of the form $(m^2 - n^2, 2mn, m^2 + n^2)$.

It is simpler to solve the equation in $\mathbb{Q}$ by dividing through by c^2. In particular, we can just take wlog $c = 1, a, b \in \mathbb{Q}$.

Thus, we may as well consider the set

$$\left\{(x,y) \in \mathbb{F}^2 |\ x^2 + y^2 = 1\right\} \tag{46}$$

$\mathbb{F}$ is a field of characteristic not equal to 2. Thus, we are just looking at rational points on a circle. But now, considering the line $y = t(x-1)$ (which always goes through $(1,0)$), we can get a bijection between the points on the circle and the slope t (i.e. stereographic projection for $\mathbb{S}^1$).

But now,

$$x^2 + t^2(x-1)^2 = 1 \tag{47}$$

$$(x-1)(x+1) + t^2(x-1)^2 = 0 \tag{48}$$

with $(x,y) \neq (1,0)$. So

$$(x+1)^2 + t^2(x-1) = 0 \tag{49}$$

$$x(1+t^2) = 1 - t^2 \tag{50}$$

so we get

$$x = \frac{1-t^2}{1+t^2} \tag{51}$$

and

$$y = \frac{2t}{1+t^2} \tag{52}$$

Thus,

$$\left(\frac{t^2-1}{t^2+1}, \frac{2t}{1+t^2}\right) \tag{53}$$

for $F \subseteq \mathbb{R}$.

If we now take $F = \mathbb{F}_q$ for q odd prime, then

$$S = \left\{(x,y) \in \mathbb{F}_q^2 | x^2 + y^2 = 1\right\} \tag{54}$$

Then

$$|S| = \begin{cases} 1+q & \left(\frac{-1}{q}\right) = -1 \\ 1+q-2 & \left(\frac{-1}{q}\right) = 1 \qquad \text{i.e., omit soln. of } t^2+1=0 \end{cases} \tag{55}$$

Thus,

$$|S| = q - \left(\frac{-1}{q}\right) \tag{56}$$

Read Pierre Samuel's book for the rest.

4.3 Solving $x^2 + y^2 = 1$ over $\mathbb{F}_q$.

Another method: how many solutions are there to $y^2 = f(x)$ with $(x,y) \in \mathbb{F}_q^2$. For this, take $x \in \mathbb{F}_q$. Then

$$1 + \left(\frac{f(x)}{q}\right) \begin{cases} 1 \text{ solutions} & f(x) = 0 \\ 2 \text{ solutions} & f(x) \text{ is a nonzero square} \\ 0 & f(x) \text{ not a square} \end{cases} \tag{57}$$

Thus,

$$|S| = \sum_{x \in \mathbb{F}_q} 1 + \left(\frac{f(x)}{q}\right) = q + \sum_{x \in \mathbb{F}_q} \left(\frac{f(x)}{q}\right) \tag{58}$$

So in particular, for $x^2 + y^2 = 1$, we get

$$q + \sum_{x \in \mathbb{F}_q} \left(\frac{1-x^2}{q}\right) \tag{59}$$

Now from last lecture, we get

$$f(c) = \sum_{m \in \mathbb{F}_q} \left(\frac{m(x-m)}{q}\right) \tag{60}$$

and $f(c) = f(1)$ for all $c \neq 0$. Thus,

$$\sum_{x \in \mathbb{F}_q} \left(\frac{(1-x)(1+x)}{q}\right) = f(2) \qquad (= f(1)) \tag{61}$$

4.4 Number Fields: Quadratic Fields over $\mathbb{Q}$.

Definition 42. A **quadratic field extension over** $\mathbb{Q}$ is just $E := \mathbb{Q}[\sqrt{d}]$ for nonzero, $\neq 1$, and square-free $d \in \mathbb{Q}$.

Remark 43. We assume square free because $\mathbb{Q}[\sqrt{d \cdot c^2}] = \mathbb{Q}[\sqrt{d}]$ for a nonzero $c \in \mathbb{Q}$.

Proposition 44. Every element of E is uniquely expressed as $u + v\sqrt{d}$ for $u, v \in \mathbb{Q}$. We have the ring homomorphism

$$\sigma : u + v\sqrt{d} \mapsto u - v\sqrt{d} \tag{62}$$

Here, for $\alpha \in E$,

$$\mathrm{Tr}(\alpha) := \mathrm{Trace}_{E/\mathbb{Q}}(\alpha) := \alpha + \sigma\alpha \qquad N(\alpha) := \mathrm{Norm}_{E/\mathbb{Q}})(\alpha) := \alpha\sigma\alpha \tag{63}$$

Remark 45. In particular,

$$\mathrm{Trace}_{E/\mathbb{Q}}(u + v\sqrt{d}) := 2u \qquad \mathrm{Norm}_{E/\mathbb{Q}})(u + v\sqrt{d}) := u^2 - v^2 d \tag{64}$$

Remark 46. A ring we could consider is $\mathbb{Z} + \mathbb{Z}\sqrt{d}$. But this is not always good, for instance the case $d = -3$. For this, we would like to consider the cube root of unity ζ_3. So we consider some different ring.

Exercise 47. Take $\alpha \in \mathbb{Q}[\sqrt{d}]$. Then α is a root of the equation (in $\mathbb{Q}$)

$$x^2 - \mathrm{tr}(\alpha)x + N(\alpha) = 0 \tag{65}$$

Here is the good ring we want to consider.

Definition 48.

$$R := \left\{\alpha \in \mathbb{Q}(\sqrt{d}) : \mathrm{Tr}(\alpha), N(\alpha) \in \mathbb{Z}\right\} \tag{66}$$

Exercise 49. Show:

$$R = \mathbb{Z} + \mathbb{Z}\theta \tag{67}$$

is a ring, where

$$\theta := \begin{cases} \sqrt{d} & d \equiv 2, 3 \mod 4 \\ \frac{1+\sqrt{d}}{2} & d \equiv 1 \mod 4 \end{cases} \tag{68}$$

Then θ satisfies the equation

$$x^2 - x + \frac{1-d}{4} = 0 \tag{69}$$

when $d \equiv 1 \mod 4$. In the first case, show

$$R \simeq \mathbb{Z}[x]/(x^2 - d) \tag{70}$$

and in the second case,

$$R \simeq \mathbb{Z}[x]/\left(x^2 - x + \frac{1-d}{4}\right) \tag{71}$$

where the isomorphism is $\theta \mapsto x$.

Here is a lemma.

Proposition 50. $0 \neq I \subseteq R$ is an ideal, then $[R : I] < \infty$.

PROOF 51. For example, if $I = Rn$ for $n \in \mathbb{N}$, then

$$R = \mathbb{Z} + \mathbb{Z}\theta, \ Rn = \mathbb{Z}n + \mathbb{Z}n\theta \tag{72}$$

for which we see that

$$R/I \simeq \mathbb{Z}/n \oplus \mathbb{Z}/n\theta \tag{73}$$

has n^2 elements.

More generally, let $0 \neq g \in I$. By definition of an ideal, $gh \in I$ for all $h \in R$. In particular,

$$N(g) = g\sigma g \in I \tag{74}$$

But now, $N(g) \in \mathbb{Z}$ and $N(g) \neq 0$ and $R \supseteq I \supseteq RN(g)$. Thus

$$[R : I] | N(g)^2 \tag{75}$$

which gives finiteness.

□

Definition 52. For a nonzero ideal $I \subseteq R$, the **norm of an ideal** is

$$N(I) := [R : I] \tag{76}$$

Proposition 53 (Relation between the two notions of the norm.). For a nonzero element $g \in R$,

$$N(Rg) = \left|N_{E/\mathbb{Q}}(g)\right| \tag{77}$$

Proposition 54. Take

$$T : \mathbb{Z}^2 \to \mathbb{Z}^2 \tag{78}$$

is a group homomorphism with $\det T \neq 0$ (when represented by an element of $M_n(\mathbb{Z})$). Then

$$[\mathbb{Z}^n : M_n(\mathbb{Z})] = |\det T| \tag{79}$$

This is in the Preliminaries of Tata Institute notes. (This is pure algebra.) In class, we will prove this geometrically in terms of volumes.

We use the above for number fields which is why we are stating it in full generality.

PROOF 55 (Proposition 54 implies 53). Let$g := u + v\theta$ for $u, v \in \mathbb{Z}$, $(u, v) \neq 0$. Then $\ell_g : \mathbb{R} \to R$ with $\ell_g := g\alpha$ for all $\alpha \in R$.

Now

$$R = \mathbb{Z} + \mathbb{Z}\theta \tag{80}$$

where the basis elements of this as a $\mathbb{Z}$-module are $1, \theta$. Then (verify:)

$$T = \begin{pmatrix} u & -vN(\theta) \\ v & u\mathrm{Tr}(\theta) + u \end{pmatrix} \tag{81}$$

Then (verify) $\det T = N(g)$.

□

4.5 Problem Session (HW 1.). Tues. 4.9.2019.

Problem session will move to to Thursday since HWs are due on Mondays.

We review what we did in class:

Proposition 56 (Dirichlet's Theorem of Arithmetic Progression.). For a, d mutually prime, there exists infinitely many primes of the form $a + nd$ for some $n \in \mathbb{Z}$.

This is a hard theorem to prove; it requires analytic number theory.

Example 57. There exists infinitely many primes of the form $1 \mod 3$ and $3 \mod 4$. We proved this using Euclid's method.

Euclid's method does not always work (in fact we can *prove* that there are cases in which this does not work).

Euclid's method: assume finitely many primes of the form $a \mod d$, say $p_1, ..., p_n$. Pick a good polynomial such that $p | f(p_1, ..., p_n)$ iff $p \equiv a \mod d$ and p cannot be one of $p_1, ..., p_n$. (Usually, letting the constant term be 1 meets the second condition.)

If

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 \tag{82}$$

then

$$p_i | a_j (p_1, ..., p_n)^j \tag{83}$$

Thus, if

$$p_i | f(p_1, ..., p_n) \tag{84}$$

implies $p_i | 1$.

Another thing we discussed was quadratic reciprocity. Recall that the Legendre symbol is given by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a square in } \mathbb{F}_p \\ 0 & p | a \\ -1 & a \text{ is not a square in } \mathbb{F}_p \end{cases} \tag{85}$$

Proposition 58 (Euler's Criteria.).

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p \tag{86}$$

As a corollary, we get

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \mod p \tag{87}$$

which is equal to 1 iff $p \equiv 1 \mod 4$.

We also know that the Legendre symbol is a homomorphism for a fixed prime. Finally, we have quadratic reciprocity:

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right) \tag{88}$$

Example 59. Using this, we can compute Legendre symbols:

$$\begin{aligned}\left(\frac{-30}{101}\right) &= \left(\frac{-1}{101}\right)\left(\frac{2}{101}\right)\left(\frac{3}{101}\right)\left(\frac{5}{101}\right) \\ &= 1\cdot(-1)\cdot\left(\frac{3}{101}\right)\left(\frac{5}{101}\right) \qquad \text{using values for 2, -1} \\ &= -1\cdot\left(\frac{101}{3}\right)\left(\frac{101}{5}\right)(-1)^{\frac{101-1}{2}\frac{3-1}{2}}(-1)^{\frac{101-1}{2}\frac{5-1}{2}} \qquad \text{quadratic reciprocity} \\ &= -1\cdot\left(\frac{2}{3}\right)\left(\frac{1}{5}\right) \\ &= (-1)\cdot(-1)\cdot 1 = 1\end{aligned}$$

Moral of the story:
1.) Keep reducing the numbers in size via quadratic reciprocity.
2.) When numbers are small enough, check directly.

We also have the Chinese Remainder Theorem:

Proposition 60 (Chinese Reminder Theorem.). If n, m are coprime, then

$$\mathbb{Z}/nm \simeq \mathbb{Z}/n \times \mathbb{Z}/m \tag{89}$$

i.e., given $a \mod n,\ b \mod m$, then there exists a unique $x \mod mn$ such that $x \equiv a \mod n$ and $b \mod m$.

There are two problems on the pset that requires this.

Example 61. For which p is $\left(\frac{-2}{p}\right) = 1$. We also assume p is an odd prime. Then

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) \tag{90}$$

Then there are two cases: both 1 or both -1. Considering the two conditions, we get $p \equiv 1, 3 \mod 8$.

Remark 62. For a primitive nth root of unity, then the $\frac{n}{2}$th power gives -1.

Hints for Problems:

Problem 3. CRT.

Problem 4. CRT. Assume a is a prime. Then by quadratic reciprocity,

$$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right)(-1)^{*} \tag{91}$$

and likewise for q.

If a is odd prime, then $p \equiv q \mod 4a$, then $p \equiv q \mod 4$ and $p \equiv q \mod a$ by CRT.

In the case when a is a composite, we can split it. We also have the consider the case when it is 2. Done.

Problem 5. Use the fact that ζ_n is a primitive nth root of unity and the characterization of $\mathbb{F}_p$ as $a^p = a$ (which is the only characterization we have).

Problem 6. Suppose $N \in \mathbb{Z}$, gcd$(N, n) = 1$ and $N \mod n \notin H$, then N has a prime factor not congruent to things in H.

The point is to use Euclid's algorithm. Suppose $p_1, ..., p_r$ are primes, fix $b \mod n$, then prove that there exists x such that $p_i \not| nx + b$ for all i.

Problem 7. For problem 1.5 is very important for Problem 1.7.

5 . - -Wednesday, 4.10.2019

We change the order a bit: We do norms, traces, etc later. We first do some stuff about ideals.

5.1 Ideals in Integer Rings.

Let $d \in \mathbb{Z}$ not equal to $0, 1$ and is squared free. Take

$$\theta := \begin{cases} \sqrt{d} & d \equiv 2, 3 \mod 4 \\ \frac{1+\sqrt{d}}{2} & d \equiv 1 \mod 4 \end{cases} \tag{92}$$

Consider the ring $R := \mathbb{Z} + \mathbb{Z}\theta$ which is a subring of the field $\mathbb{Q}(\sqrt{d})$. We examine the following example today:

Example 63. Take $\mathbb{Z}[\sqrt{-58}]$ and the ideal

$$I := \left\{a + b\sqrt{-58} : a, b \in \mathbb{Z},\ a \equiv 0 \mod 2\right\} \tag{93}$$

I is a subgroup of R.

Let's verify that I is an ideal. For $\alpha := a + b\sqrt{-58} \in I$, we get

$$\sqrt{-58} \cdot \alpha = a\sqrt{-58} - 58b \tag{94}$$

Since -58 is even, $\sqrt{-58}\alpha \in I$.

Now if $c, d \in \mathbb{Z}$, we have

$$(c + d\sqrt{-58})\alpha = c\alpha + \sqrt{-58}d\alpha \tag{95}$$

Now since I is a subgroup, $c\alpha \in I$. Thus $\sqrt{-58}\alpha \in I$, and since I is subgroup, we get $c\alpha + \sqrt{-58}d\alpha \in I$. Thus, I is an ideal.

Now suppose I is principal. We can write $I = (u + v\sqrt{-58})$, then

$$2 = [R : I] = N(u + v\sqrt{-58}) = u^2 + 58v^2 \tag{96}$$

which cannot be solved. So, I is not principle.

5.2 Prime Ideals.

Recall the following basic facts:

Proposition 64. $\mathfrak{p} \subseteq R$ is a prime ideal iff $R/\mathfrak{p}$ is an integral domain.

Proposition 65. $\mathfrak{m} \subseteq R$ is a maximal ideal iff $R/\mathfrak{m}$ is a field.

So in particular, maximal ideal is a prime ideal.

Exercise 66. Finite integral domain is a field.

Remark 67. In our situation (i.e. for $R = \mathbb{Z}[\sqrt{-58}]$), if $0 \neq I \subseteq R$ is an ideal, then R/I is a finite. Thus, a nonzero [2] prime ideal is the same thing as a maximal ideal.

Let $\mathfrak{p} \subseteq R := \mathbb{Z} + \mathbb{Z}\theta$ be a nonzero prime ideal. If $\mathfrak{p}$ is nonzero, then there exists a nonzero element $n \in \mathbb{Z}$ such that $n \in \mathfrak{p}$. If $n = \pm 1$, then $\mathfrak{p} = RX$. Then there exists a prime p such that $\mathfrak{p}$ is a prime ideal. We can then take the prime factorization

$$n = \pm p_1 ... p_k \tag{97}$$

where p_i are all primes. Now if $n \in \mathfrak{p}$ and $\mathfrak{p}$ is a prime ideal, then $p_i \in \mathfrak{p}$ for some i.

Proposition 68. If $\mathfrak{p}$ is a nonzero prime ideal of R, there exists a unique prime number p such that $p \in \mathfrak{p}$.

Fix a prime p and search for prime ideal $\mathfrak{p} \subseteq R$ such that $p \in \mathfrak{p}$.

Definition / Proposition 69. In this situation, we have exactly one of the following:

1.) $\mathfrak{p}$ is unique and $\mathfrak{p}^2 = (p)$. For this, p **is a ramified for** $\mathbb{Q}(\sqrt{d})$.

2.) $\mathfrak{p} = (p)$. p **is a nonsplit (inert) for** $\mathbb{Q}(\sqrt{d})$.

3.) There exists two distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$ such that p belongs to both. In this case, $(p) = \mathfrak{p}_1\mathfrak{p}_2$, and there exists a ring automorphism for which $\sigma\mathfrak{p}_1 = \mathfrak{p}_2$. p **is a split prime.**

Remark 70 (Consistency with Previous Terminology.). The third case occurs iff p is a f-split where $f \in \mathbb{Z}[X]$ monic degree 2 with $f(\theta) = 0$.

We now consider each of these cases.

Case 1. Work with $d \equiv 2, 3 \mod 4$. Consider prime $p$that divide d. Here, $\mathfrak{p} = (p, \sqrt{d})$ is the unique prime ideal containing p.

Remark 71. Let A be a ring containing the ideal I. All ideals of A/I are of the form J/I where $J \supseteq I$ is an ideal of A. This is equivalent to taking $\pi^{-1}(K)$ for an ideal $K \subseteq A/I$ for the quotient map π.

The prime ideals of A/I are P/I where $P \supseteq I$ is a prime ideal of A.

Remark 72. For our situation, we take $A = R$ with $I = (p)$ for $p \in \mathfrak{p}$ which is equivalent to $(p) \subseteq \mathfrak{p}$. In reality, we are fixing p and considering prime ideals for $R/(p)$.

[2] In books, people tend to omit the nonzero. But do remember that it is there.

Now consider

$$\mathbb{Z}[X]/(X^2 - d) \simeq R \tag{98}$$

with isomorphism given by the map

$$X \mapsto \sqrt{d} \tag{99}$$

which implies

$$R/(p) \simeq \mathbb{Z}[X]/(p, X^2 - d) \simeq (\mathbb{Z}[X]/(p))/(X^2 - d) \simeq (\mathbb{F}_p[X])/(X^2 - d) \tag{100}$$

If $p|d$, then $\mathbb{F}_p[X]/(X^2)$ has a unique prime ideal generated by $(X)/(X^2)$. Thus, the only choice of $\mathfrak{p}$ is $(p, \sqrt{d})$ from our earlier observation.

Now take $p = 2$, then $R/(p) \simeq \mathbb{F}_2[X]/(X^2 - \overline{d})$. But we recall that in characteristic 2, $(a+b)^2 = a^2 + b^2$. Thus,

$$X^2 - \overline{d} = (X - \overline{d})^2 \tag{101}$$

Once again $\mathfrak{p}$ is unique, and $\mathfrak{p} = (2, \sqrt{d} - d)$. This takes care of this case.

Now for p odd, $\mathfrak{p} = (p, \sqrt{d})$ for which

$$\mathfrak{p}^2 = (p, \sqrt{d})(p, \sqrt{d}) = (p^2, p\sqrt{d}, d) \tag{102}$$

But now, if $p \nmid \frac{d}{p}$, then there exists $a, b \in \mathbb{Z}$ for which

$$ap + b\frac{d}{p} = 1 \tag{103}$$

Thus,

$$ap^2 + bd = p \in (d, p^2) \subseteq (p) \tag{104}$$

Thus, $(p) = \mathfrak{p}^2$.

Exercise 73. Check the case $p = 2$.

Case 2. Now assume $p \nmid d$. Then

$$R/(p) \simeq \mathbb{F}_p[X]/(X^2 - d) \tag{105}$$

Now $\left(\frac{d}{p}\right) = -1$, then $X^2 - d$ is irreducible, thus the above ring is an integral domain, thus (p) is prime.

Case 3. If $\left(\frac{d}{p}\right) = 1$, then find $a \in \mathbb{Z}$ for which $a^2 \equiv d \mod p$. Then

$$X^2 - d = (X - a)(X + a) \tag{106}$$

in $\mathbb{F}_p[X]$. Now $\mathfrak{p}_1 = (p, \sqrt{d} - a),\ \mathfrak{p}_2 = (p, \sqrt{d} + a)$.

In regards to the automorphism, we can look at

$$\sigma\sqrt{d} = -\sqrt{d} \tag{107}$$

which implies $\sigma P_1 = P_2$.

For the other statement, the brute force method is to use Chinese Remainder Theorem. Here, we look at

$$\begin{aligned}\mathfrak{p}_1\mathfrak{p}_2 &= (p, \sqrt{d}-a)(p,\sqrt{d}+a) \\ &= (p^2, p(\sqrt{d}-a), p(\sqrt{d}+a), d^2-a) \subseteq (p)\end{aligned}$$

We then see that $2ap \in \mathfrak{p}^2$ and

$$\pi(\sqrt{d}-a) - p(\sqrt{d}+a) \tag{108}$$

and

$$\mathfrak{p}_1\mathfrak{p}_2 \supseteq (2ap, p^2) = p(2a, p) \tag{109}$$

Now p is an odd prime, and $p \nmid a$, so $\gcd(p, 2a) = 1$. Thus, the above is $p \cdot (1)$. Thus, $\mathfrak{p}_1\mathfrak{p}_2 = (p)$.

Remark 74. What are possible values of the norm in the three cases?

1.) Case 1. $N(\mathfrak{p}) = p$
2.) Case 2. $N(\mathfrak{p}) = p^2$
3.) Case 3. $N(\mathfrak{p}_i) = p$

6 . - -Friday, 4.12.2019

Today we continue our discussion of $R := \mathbb{Z} + \mathbb{Z}\theta$ for

$$\theta = \frac{1+\sqrt{d}}{2},\ d \equiv 1 \mod 4 \tag{110}$$

We let

$$f(x) := x^2 - x + \frac{1-d}{4} \tag{111}$$

Take $p = 2$ and ask for prime ideals p of R that contains (2). Then

$$R = \mathbb{Z}[X]/(f) \tag{112}$$

so

$$R/(2) \simeq \mathbb{F}_2[X]/(f) \tag{113}$$

We want prime ideals of this. If $d \equiv 5 \mod 8$, then $\overline{f} = x^2 - x + 1 \in \mathbb{F}_2[x]$ iff (2) is a nonsplit (**unramified**).

If $d \equiv 1 \mod 2$, then $\overline{f} = x(x-1) \in \mathbb{F}_2[X]$. We get two prime ideals $p_1 := (2, \theta)$ and $p_2 := (2, \theta - 1)$. 2 is a split prime. Thus,

$$2 \in (2,\theta)(2,\theta-1) = (4, 2\theta, 2(\theta-1), \frac{d-1}{4}) \subseteq (2) \tag{114}$$

and so,

$$2\theta - (2\theta - 1) = 2 \tag{115}$$

Thus, $(2) = p_1p_2$.

Now consider the "bad ring" $\mathbb{Z}+\mathbb{Z}\sqrt{d}$ contained in the good ring R. Let p be an odd prime. We have shown that

1.) $p|d \implies (p, \sqrt{d}) = P'$ is a prime ideal of R' and $P'P' = pR'$

2.) $\left(\frac{d}{p}\right) = -1 \implies R'p$ is a prime ideal of R'

3.) $\left(\frac{d}{p}\right) = 1 \implies$ if $a \in \mathbb{Z},\ a^2 = d \mod p$, then $P_1' = (p, \sqrt{d} - a),\ P_2' = (p, \sqrt{d} + a)$ where these are ideals generated in R'. Both P_1, P_2 are prime ideals, and $P_1'P_2' = pR'$

Now taking the embedding $R' \hookrightarrow R$, then we get a ring homomorphism $R'/nR' \to R/nR$ for $n \in \mathbb{N}$.

Proposition 75. If n is odd, then $R'/nR' \to R/nR$ is an isomorphism of rings.

PROOF 76. This is an exercise in group theory. Obvious comment: Both $R, R' \simeq \mathbb{Z}^2$ as abelian groups. Thus $R'/nR', R/nR \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ as abelian groups, and thus they both have n^2 elements.

Since we know that the map is a ring homomorphism, we just need to show that it is a bijection.

Now $R/R' \simeq \mathbb{Z}/2\mathbb{Z}$ as abelian groups. So for n odd, multiplication by n gives an isomorphism R/R' to itself. Given $\alpha \in R$, we can write

$$\alpha = n\alpha + (1-n)\alpha \tag{116}$$

where the first term is 0 in $\mathbb{Z}/n\mathbb{Z}$ and the second term is in R'. Thus, $\overline{\alpha} \in R/nR$ is the image of $(1-n)\alpha \in R'$ in $R'/nR' \to R/nR$. This shows surjectivity, and since we are dealing with finite things, we have bijection. □

Take $n = p$ an odd prime. Then

$$R'/pR' \simeq R/pR \tag{117}$$

as rings. From this, 1.) $(p, \sqrt{d}) \subseteq R$ is a prime ideal, 2.) $\left(\frac{d}{p}\right) = -1$ implies Rp is a prime ideal, and 3.) $\left(\frac{d}{p}\right) = 1$ implies $Rp + R(\sqrt{d} \pm a)$ are prime ideals of R.

We still need to show the identities.

Definition 77. Given a ring homomorphism $R' \hookrightarrow R$, and an ideal $I' \subseteq R$, then we have **extension of ideals**

$$I_e' := \{a_1b_1 + a_2b_2 + ... + a_kb_k : a_i \in R,\ b_i \in I'\} \subseteq R \tag{118}$$

Clearly, I_e' is an ideal of R.

Remark 78. If I', J' are ideals of R',

$$(I'J')_e = (I_e')(J_e') \tag{119}$$

This remark then gives 1.)

$$(p, \sqrt{d})^2 = pR \tag{120}$$

and for 2.) Rp is a prime ideal, and 3.)

$$Rp + R(\sqrt{d} \pm a) \tag{121}$$

are prime ideals of R

$$(p, \sqrt{d} - a)(p, \sqrt{d} + a) = (p) \tag{122}$$

6.1 Factorization in Integer Rings.

Go read up in the references to learn the details of the algebra. We require the following:
1.) R is an integral domains, i.e. 0 cancellations
2.) $0 \neq I \subseteq R$
3.) $0 \neq I \subseteq R$ is a nonzero ideal, then $[R : I] < \infty$. [3]
4.) For all nonzero prime ideals P of R, there exists nonzero ideal Q of R such that PQ is a principal ideal. (When $R = \mathbb{Z} + \mathbb{Z}\theta$, then we define $P\sigma P := ([R : P])$.)

If $n \neq \pm 1$, not a prime, then there exists a prime $p|n$. Then $n = mp, m < n$. Now $[R : I] < \infty$, so there is a maximal ideals containing this.

Now many number theoretic proofs go by induction, so we do induction on $[R : I]$.

Proposition 79. Let $0 \neq I \subseteq P \subseteq R$ where I is an ideal, and P is prime. Then 3 implies there exists an ideal $J \subseteq R$ such that $I = PJ$.

PROOF 80. We want to show that there exists J such that $I = PJ$, then $QI = QPJ$. But $QP = R\alpha$, so

$$QJ = QPJ = (R\alpha)J = \alpha J \tag{123}$$

Therefore,

$$J = \alpha^{-1}QI \tag{124}$$

Now if K is the field of fractions of R, then $J := \alpha^{-1}QI \subseteq K$. But now $I \subseteq P$, and

$$J \subseteq \alpha^{-1}P = \alpha^{-1}\alpha R = R \tag{125}$$

Exercise. $J \subseteq R$ is an ideal of R.

Now

$$JP = \alpha^{-1}PQI = \alpha^{-1}aRI = RI = I \tag{126}$$

Now for the induction, I is our n and J is our m, but we still need $m < n$. The way to do this would be Nakayama's lemma which we will not prove nor use. (We will just do it from scratch.)

4.) $0 \neq J$ is an ideal and $0 \neq P$ is a prime ideal, then $J \supsetneq PJ$. (The $\neq$ is implied by Nakayama's lemma.)

Now if $I \subseteq P$, then $I = JP \subsetneq J$, we have $[R : I] > [R : J]$ from which induction on $[R : I]$ shows that every nonzero ideal is a product of prime ideals.

We need to check $J \supsetneq PJ$ holds for our situation and also uniqueness.

Proof of 4.) For $R = \mathbb{Z} + \mathbb{Z}\theta$, Assume $J = PJ$, then $\sigma(J) = \sigma(P)\sigma(J)$. Let $H = J\sigma(J)$. Get

$$H = HP\sigma(P) = H[R : P] \qquad [R : P] > 1 \tag{127}$$

Here is an important general result we will use multiple times later.

Proposition 81. As an abelian group $H \subseteq R$ nonzero, then $H \simeq \mathbb{Z}$ or $H \simeq \mathbb{Z}^2$ as abelain groups.

Using this, clearly $H \supsetneq nH$ in both cases when $n > 1$.

□

[3] The algebraic language for this is Dedekind domains.

7 . - -Monday, 4.15.2019

7.1 Uniqueness of Prime Decomposition.

Last time we discussed prime decompositions of ideals. We now discuss the uniqueness of the decomposition. The idea is to do induction on the index $[R : I]$ for which $I = P_1 ... P_k$. We take the convention $I := R$ for $k = 0$. Here P_i are prime ideals.

If I is a prime ideal, there is nothing to do. If not, there exists a prime ideal $P \supseteq I$, and this, there exists an ideal J for which $I = JP$. (This that there exists Q such that $QP = R\alpha$.)

Now because $JP \subsetneq P$, $[R : J] < [R : I]$

$$J = P_1 ... P_{k-1} \implies I = P_1 ... P_{k-1}P \tag{128}$$

Here is a lemma.

Proposition 82. Let R be a commutative ring. $P \subseteq R$ is a prime ideal, $I, J \subseteq R$ are ideals. If P contains IJ, then P contains either I or J.

PROOF 83. Suppose for contradiction that P does not contain I. Then there exists $a \in I,\ a \notin P$. If P does not contain J, then there exists $b \in J,\ b \notin P$. We see that $ab \in IJ$. Because P is a prime ideal, $ab \notin P$. Contradiction. □

Uniqueness of factorization follows. However, we also would like to know when ideals are contained.

Proposition 84 (Uniqueness of Factorizations.). If $P_1 ... P_k \supseteq Q_1 ... Q_l$ and all the P_i, Q_j are prime ideals, then $l \geq k$ and after a permutation of $\{1, 2, ..., l\}$ we get $P_i = Q_i$ for each i.

PROOF 85. The LHS is contained in P_1. So, P_1 contains $Q_1 ... Q_l$. The lemma plus induction implies that $P_1 \supseteq Q_i$ for some i.

WLOG, take $Q_1 = P_1$. Let $P_2 ... P_k =: I,\ Q_2 ... Q_l =: J$. We then have $P_1 I = P_1 J$. We want to deduce from this that $I = J$. We have a nonzero ideal H such that $P_1 H = \alpha$. Thus, we can write

$$HP_1 I = HP_1 J \implies \alpha I = \alpha J \implies I = J \tag{129}$$

Then we have

$$P_2 ... P_k = Q_2 ... Q_l \tag{130}$$

and by induction on k, this proves the statement. □

This is like working in a group. One can cancel things. There is thus a larger group to look at.

7.2 Fractional Ideal.

If I, J are contained in R, we have $IJ \subseteq R$.

Definition 86. Let R be an integral domain contained in $K = \text{Frac}(R)$. A **fractional ideal** is a nonzero R-submodule M of K that is finitely generated as a R-module, i.e.

1.) $0 \neq M \subseteq K$ is an additive subgroup
2.) $c \in R, m \in M$ implies $cm \in M$
3.) $m_1, ... m_k \in M$ such that for all $m \in M$ there exists $c_1, ..., c_k \in R$ such that

$$m = c_1 m_1 + ... + c_k m_k \tag{131}$$

Example 87. What if $R = \mathbb{Z}, K = \mathbb{Q}$? Then $\alpha \in \mathbb{Q},\ \alpha > 0$. Then $\mathbb{Z}\alpha$ is a fractional ideal. These are

$$\mathbb{Z}\alpha = \mathbb{Z}\beta \implies \alpha = \pm\beta \tag{132}$$

In other words, there is a one-to-one correspondence between the positive rationals and the fractional ideals over $\mathbb{Z}$.

Definition / Proposition 88. If M, N are fractional ideals, then

$$MN := \{m_1n_1 + ... + m_en_e :\ m_i \in M,\ n_i \in N,\ e \in \mathbb{N}\} \tag{133}$$

and MN is a nonzero R-submodule of K. Additionally, if M, N are finitely generated, then MN is finitely generated as an R-module by $\{m_in_j\}_{\substack{1\leq i\leq k\\ 1\leq j\leq l}}$ where $m_1, ..., m_k$ and $n_1, ..., n_l$ are respectively generators of M, N.

Proposition 89. The collection of fractional ideals is a commutative monoid, i.e. $RM = M$ for all fractional ideal M.

Remark 90. For "our" rings [4] R, the collection of fractional ideals is a group. We do not do it in full generality in this class since we would have to sacrifice number theory.

Check the stuff in footnote.

Remark 91. $0 \neq \alpha \in K$, then $(R\alpha)(R\alpha^{-1}) = R$.

Remark 92. People sometimes drop the "fractional" in fractional ideal. In this case, ordinary ideals are called **integral ideals** to distinguish it from fractional ideals.

PROOF 93 (of Remark 90). *1.) Prime ideals have an inverse.*

If P is a prime ideal, then there exists Q an ideal and $\alpha \in R$ such that

$$PQ = R\alpha \implies P(\alpha^{-1}Q) = R \tag{134}$$

2.) If $0 \neq I \subseteq R$ is an ideal, then there exists free ideal J such that $IJ = R$.

We know that $I = P_1...P_k$ and so,

$$(P_1^{-1}...P_k^{-1})(P_1...P_k) = R \tag{135}$$

2.) The General Case.

Let $M \neq 0$ be a fractional ideal. Then $h_1, ..., h_k \in K$ that generate M as a R-module. There exists $a_i, b_i \in R, b_i \neq 0$ such that $h_i = \frac{a_i}{b_i}$. Then the idea is to clear denominators. Let

$$b := b_1...b_k \tag{136}$$

Then bM is the R-module generated by $bh_1, ..., bh_k$. Then

$$bh_1 = (b_2...b_k)(b_1h_1) = a_1b_2...b_k \in R \tag{137}$$

$$bh_2 = a_2b_1b_3...b_k \in R \tag{138}$$

etc. Thus, $bM = I$ is the ideal in R generated by $bh_1, ..., bh_k \in R$. (In particular, it is $M = b^{-1}I$.)

We can then check that $(bI^{-1})M = R$.

[4] The precise term here is Dedekind domains. Example of a not good ring is $\mathbb{Z}[\sqrt{d}]$ for $d \equiv 1 \mod 4$.

□

Remark 94. This proof is nice, but to find the inverse by factorizing it, i.e. this is the proper definition. See HW 2 for this.

Proposition 95 (Factorization of Fractional Ideals.). Every fractional ideal equals $p_1^{k_1}...p_m^{k_m}$ where p_i are prime ideals and $k_i \in \mathbb{Z}$.

PROOF 96. Every fractional ideal equals $b^{-1}I = (Rb)^{-1}I$ for $b \in R, I \subseteq R$.

Now

$$I = P_1...P_k, \; Rb = Q_1...Q_l \tag{139}$$

and

$$(Rb)^{-1}I = P_1...P_k(Q_1...Q_l)^{-1} \tag{140}$$

The remaining details are left as an exercise.

□

PROOF 97 (Uniqueness.). Take $P_1, ..., P_m$ are distinct prime ideals of R, $k_1, ..., k_m, l_1, ..., l_m \in \mathbb{Z}$, and

$$X := P_1^{k_1}...P_m^{k_m} \supseteq P_1^{l_1}...P_m^{l_m} =: Y \iff k_1 \leq l_1, \; k_2 \leq l_2, \; ..., \; k_m \leq l_m \tag{141}$$

This is a free abelian group on the set of prime ideals.

Since we already have uniqueness in the case of natural numbers, we can just multiply the above by a large enough number. Choose $N \in \mathbb{N}_0$ such that $1 + k_i, \; 1 + l_j \geq 0$ for all i, j. Let

$$M = (P_1...P_m)^N \tag{142}$$

Then MX, MY are ideals in R.

□

Remark 98. If M, X, Y are fractional ideals, $X \subseteq Y$, then $MX \subseteq MY$. If M has an inverse, then

$$M^{-1}MX \subseteq M^{-1}MY \implies X \subseteq Y \tag{143}$$

Thus the theorem is true iff it is true with all $k_i, l_j \geq 0$. But we proved the latter before, so we are done.

Next time: we look at the class group.

8 . - -Wednesday, 4.17.2019

We stick to the notation in Pierre Samuel.

Notation. Let $I(R)$ be the monoid of fractional ideals.

If R is "special," then $I(R)$ is a group.

Let K be the fraction field of R. $K^\times$ is a multiplicative group, so $\varphi : \alpha \mapsto R\alpha$ is a homomorphism from $K^\times$ to $I(R)$. (i.e., $R\alpha R\beta = R\alpha\beta$ for all $\alpha, \beta \in K^\times$.) The image of $K^\times$ under this map is the group of principal ideals.

Fill in rigorous definition of special.

Definition 99. The **class group of** R denoted $Cl(R)$ is the quotient $I(R)/\varphi(K^{\times})$.

The goal for today is to show that $Cl(R)$ is a group where $K = \mathbb{Q}(\sqrt{d})$ for $d < 0$, square free, $d \in \mathbb{Z}$.

Proposition 100. Assume R is special. Let $I, J \subseteq R$ be nonzero ideals. Then

$$N(IJ) = N(I)N(J) \tag{144}$$

where we recall that $N(I) := [R : I]$.

PROOF 101. *Case 1.* J is a prime ideal, P. Shown that $I \supsetneq PI$.

Let $a \in I,\ a \notin PI$. Then take an R-module homomorphism $\phi : R \to I$ given by $\phi(x) := ax,\ \forall x \in R$. Then $\phi(P) \subseteq IP$.

This induces the group homomorphism $\overline{\phi} : R/P \to I/PI$ where $\overline{\phi} = \overline{a} \in I/PI$ nonzero. Now ker$\overline{\phi} \neq R/P$ for P prime implies the kernel of $\overline{\phi}$ is 0. Now

$$\overline{\phi}(R/P) = H/PI \tag{145}$$

for some ideal H with $I \supseteq H \supseteq PI$. But from prime decomposition, we can write

$$I = P_1 ... P_k \supseteq H \supseteq PP_1 ... P_k \tag{146}$$

and so $H = I$ or PI. But $H \neq PI$ because $\overline{\phi} \neq 0$. So $H = I$, i.e. $\overline{\phi}$ is onto. Thus, $\overline{\phi} : R/P \to I/PI$ is an isomorphism.

Taking cardinalities on both sides gives

$$N(P) = |R/P| = |I/PI| = \frac{|R/PI|}{|R/I|} = \frac{N(PI)}{N(I)} \tag{147}$$

General Case. Write $J = P_1 ... P_k$ and by induction on k, we see that

$$N(I)N(J) = N(IJ) \tag{148}$$

Now taking $J' = P_1 ... P_{k-1}$, we have

$$N(IJ) = N(IJ'P_k) = N(IJ')N(P_k) = N(I)N(J) \tag{149}$$

by the induction hypothesis. We need Dedekind domains for these steps to work.

□

Now consider the imaginary quadratic field $K = \mathbb{Q}(\sqrt{d}),\ d < 0$. Let $M \in I(R)$, we've seen that there exists $\alpha \in K$ nonzero such that $I = M\alpha \subseteq R$.

Now taking $\beta \in I$ nonzero, we see

$$R = \mathbb{Z} + \mathbb{Z}\theta \supseteq I \supseteq \beta R = \mathbb{Z}\beta + \mathbb{Z}\beta\theta \tag{150}$$

It follows that there exists $\omega_1, \omega_2 \in \mathbb{C}$ such that $I = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. Here, $\frac{\omega_2}{\omega_1} \in K \setminus \mathbb{R}$.

We now define the notion of the fundamental set.

Definition 102. Given an ideal $I \subseteq R$, choose ω_1, ω_2 so that $I = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. The **fundamental parallelogram given by** ω_1, ω_2 is the set

$$\{t_1\omega_1 + t_2\omega_2 : t_1, t_2 \in [0,1]\} \tag{151}$$

The **area** of this is

$$\text{Area}(\mathbb{C}/I) := \frac{1}{2}\left|\overline{\omega}_1\omega_2 - \overline{\omega}_2\omega_1\right| \tag{152}$$

Proposition 103. The Fundamental Parallelogram is independent of the choice of ω_1, ω_2.

PROOF 104. If we now take $I = \mathbb{Z}\omega_1' + \mathbb{Z}\omega_2'$, then we can write

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} \tag{153}$$

for $a, b, c, d \in \mathbb{Z}$. Let A be the above matrix. Then $\det A = \pm 1$. It follows that the fundamental parallelogram does not depend on the choice of ω_1, ω_2.

□

Proposition 105. If $P \supseteq I \supseteq J$ are both ideals, then

$$\text{Area}(\mathbb{C}/J) = \text{Area}(\mathbb{C}/I)[I : J] \tag{154}$$

PROOF 106. Assume $I = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.Then we can write

$$J \cap \mathbb{Z}\omega_1 = \mathbb{Z}m_1\omega_1 \tag{155}$$

for some $m_1 \in \mathbb{N}$.

Then we can write

$$\{a \in \mathbb{Z} : (\exists n \in \mathbb{Z})(n\omega_1 + a\omega_2 \in J)\} \tag{156}$$

A less cumbersome way of saying this is taking the projection map $\pi : I \to \mathbb{Z}$ given by $\pi(u\omega_1 + v\omega_2) = v$ for which $\pi(J) = m_2\mathbb{Z}$ for a unique $m_2 \in \mathbb{N}$.

Then there exists $b \in \mathbb{Z}$ such that

$$\omega_2 = b\omega_1 + m_2\omega_2 \in J \tag{157}$$

Now if we take $\omega_1' := m_1\omega_1$.

Then $J = \mathbb{Z}\omega_1' + \mathbb{Z}\omega_2'$. We thus have the corresponding matrix

$$\begin{pmatrix} m_1 & 0 \\ b & m_2 \end{pmatrix}\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} \tag{158}$$

We can check that in general,

$$\frac{1}{2}\left|\overline{\omega}_1'\omega_2' - \overline{\omega}_2'\omega_1'\right| = |\det A|\left|\overline{\omega}_1\omega_2 - \overline{\omega}_2\omega_1\right| \tag{159}$$

for $A \in GL(2, \mathbb{R})$. Then $\det A = [I : J] = m_1m_2$.

We are interested in what $|I/J|$ is. Let

$$V := I/J \supseteq \mathbb{Z}\omega_1/J \cap \mathbb{Z}\omega_2 = \mathbb{Z}\omega_1/\mathbb{Z}m_1\omega_1 =: V' \tag{160}$$

Let $V'' := V/V'$. We can then simply check that V'' has m_2 elements.

Objective: given $0 \neq I \subseteq R$. Find $\alpha \in I$ nonzero such that

$$N(R\alpha) = |\alpha \cdot \sigma\alpha| = |\alpha\overline{\alpha}| = |\alpha|^2 \tag{161}$$

is as small as possible. i.e., consider the shortest vector possible.

Now taking $I \supseteq R\alpha$ then there exists $J \subseteq R$ such that $R\alpha = IJ$ and $N(I)N(J) = |\alpha|^2$ is being minimized. The $|\alpha|^2$ we get depends on Area$(\mathbb{C}/I)$.

Now for $\mathbb{C} \supseteq R \supseteq I$,

$$\text{Area}(\mathbb{C}/I) = \text{Area}(\mathbb{C}/R)N(I) \tag{162}$$

Now, from some geometric observations,

$$\text{Area}(\mathbb{C}/R) = \begin{cases} \sqrt{|d|} & d \equiv 2, 3 \mod 4 \\ \frac{1}{2}\sqrt{|d|} & d \equiv 1 \mod 4 \end{cases} \tag{163}$$

Objective: there exists $\alpha \in I$ nonzero such that

$$\text{Area}(\mathbb{C}/I) \geq \frac{\sqrt{3}}{2} |\alpha|^2 \tag{164}$$

If we use this, then

$$\text{Area}(\mathbb{C}/R)N(I) \geq \frac{\sqrt{3}}{2} N(I)N(J) \tag{165}$$

from which we get an upper bound on $N(J)$.

□

9 . - -Friday, 4.19.2019

Take R as usual in $\mathbb{Q}[\sqrt{d}],\ d < 0$. Take ideals $J \subseteq I \subseteq R \subseteq \mathbb{C}$. Recall from last time:

Proposition 107.

$$\text{Area}(\mathbb{C}/J) = \text{Area}(\mathbb{C}/I)[I : J] \tag{166}$$

in particular,

$$\text{Area}(\mathbb{C}/I) = \text{Area}(\mathbb{C}/R)[R : I] = \text{Area}(\mathbb{C}/R)N(I) \tag{167}$$

Claim. If $\omega_1, \omega_2 \in \mathbb{C}$ nonzero, and $\frac{\omega_2}{\omega_1} \notin \mathbb{R}$, then

$$S := \left\{ |m_1\omega_1 + m_2\omega_2|^2 : 0 \neq (m_1, m_2) \in \mathbb{Z}^2 \right\} \tag{168}$$

has a minimum. This is geometrically obvious, but it is left as an exercise to verify it.

Now assume that $mn = |\gamma|^2$, then $j = u\omega_1 + v\omega_2,\ u, v \in \mathbb{Z}$.

Claim. $\gcd(u, v) = 1$. If $\gcd(u, v) = d > 1$, then

$$\frac{j}{d} \in \{m_1\omega_1 + m_2\omega_2\} \tag{169}$$

Now we can write

$$\begin{pmatrix} u & v \\ -n & m \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} j \\ \delta \end{pmatrix} \tag{170}$$

Thus,

$$\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \mathbb{Z}j + \mathbb{Z}\delta \tag{171}$$

By scaling, we consider the case when the shortest vector is 1. Consider $L := \mathbb{Z}1 + \mathbb{Z}\tau$. Then by elementary geometry,

$$\text{Area}(\mathbb{C}/L) = |\text{Im}(\tau)| \tag{172}$$

We make the following observation:

$$\mathbb{Z}1 + \mathbb{Z}\tau = \mathbb{Z}1 + \mathbb{Z}(\tau - n) \tag{173}$$

for any $n \in \mathbb{Z}$. Thus, we can assume wlog that $\text{Re}(\tau) \leq \frac{1}{2}$.

We can now write

$$L = \mathbb{Z}1 + \mathbb{Z}\tau \tag{174}$$

where $|\text{Re}(\tau)| \leq \frac{1}{2},\ |\tau| \geq 1$.
Now

$$|\text{Im}\tau| \geq \frac{\sqrt{3}}{2} \tag{175}$$

Summary: If $1 \in L$, and is a shortest nonzero vector in L, then

$$\text{Area}(\mathbb{C}/L) \geq \frac{\sqrt{3}}{4} \tag{176}$$

Proposition 108. If $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subseteq \mathbb{C}$, $\frac{\omega_2}{\omega_1} \notin \mathbb{R}$ and $0 \neq j \in L$ is a shortest nonzero element of L, then

$$\text{Area}(\mathbb{C}/L) \geq \sqrt{\frac{3}{4}}\,|\gamma|^2 \tag{177}$$

In particular,

$$\text{Area}(\mathbb{C}/I) = \text{Area}(\mathbb{C}/R)[R : I] = \text{Area}(\mathbb{C}/R)N(I) \tag{178}$$

PROOF 109. Replace L by

$$\frac{1}{\gamma}L = \mathbb{Z}\frac{\omega_1}{j} + \mathbb{Z}\frac{\omega_2}{j} \tag{179}$$

1 is the shortest element of $\frac{1}{\gamma}L$, so

$$\text{Area}(\mathbb{C}/L) \cdot \frac{1}{|\gamma|^2} = \text{Area}(\mathbb{C}/\frac{1}{\gamma}L) \geq \sqrt{\frac{3}{4}} \tag{180}$$

□

Proposition 110 (Gauss Reduction of Positive Definite Binary Forms.). Take $R = \mathbb{Z} + \mathbb{Z}\theta$, every element of the class group $C(R) = I(R)/\text{prime ideals}$ is represented by an ideal $J \subseteq R$ with $N(J) \leq \text{Area}(\mathbb{C}/R)\sqrt{\frac{4}{3}}$.

PROOF 111. We derive the last bound. Let $0 \subsetneq I \subseteq R$ be an ideal. Then

$$\text{Area}(\mathbb{C}/I) = \text{Area}(\mathbb{C}/R)N(I) \geq \sqrt{\frac{3}{4}}|\gamma|^2 = \sqrt{\frac{3}{4}}\gamma\sigma(\gamma) = \sqrt{\frac{3}{4}}N(R\gamma) = \sqrt{\frac{3}{4}}N(I)N(J) \tag{181}$$

Now we used in the above that if $R\gamma \subseteq I$ implies that there is an ideal $J \subseteq R$ for which $IJ = R\gamma$. We thus get

$$N(J) \leq \text{Area}(\mathbb{C}/R)\sqrt{\frac{4}{3}} \tag{182}$$

This is the last bound.

Assume that $d \equiv 2, 3 \mod 4$. Then consider $J \subseteq R$

$$N(J) \leq \sqrt{|d|}\sqrt{\frac{4}{3}} \tag{183}$$

□

Proposition 112. If $\sqrt{\frac{4|d|}{3}} < 2$,i.e. $|d| < 3$, then every ideal of R is principal.

Proposition 113 (Fermat's Two Square Theorem.). If $p \equiv 1 \mod 4$, then there exists integers a, b such that $p = a^2 + b^2$.

PROOF 114. Let $R = \mathbb{Z} + \mathbb{Z}i$. Then $\left(\frac{-1}{p}\right) = 1$ then p is a split prime, then there exists a prime ideal P. Then $N(P) = p$ and

$$P = R(a + ib) \tag{184}$$

and $N(P) = a^2 + b^2$.

□

Remark 115. In algebra, things come with formulas. Number theory has existence and uniqueness without explicit constuction.

Exercise 116. Let n be a square free natural number in $R = \mathbb{Z}[-1]$. How many ideals $I \subseteq R$ have $N(I) = n$? Find

$$\#\left\{(a, b) \in \mathbb{Z}^2 : 0 \leq a \leq b,\ a^2 + b^2 = n\right\} \tag{185}$$

Here are some corollaries.

Proposition 117. If $p \equiv 1, 3 \mod 8$ prime, then there exists $a, b \in \mathbb{Z}$ such that $p = a^2 + 2b^2$.

Proposition 118. For $R = \mathbb{Z}[\sqrt{-2}]$, we have

$$\left(\frac{-2}{p}\right) = 1 \iff p \equiv 1, 3 \mod 8 \tag{186}$$

Since R is a PID, it has P for which $N(P) = p$ and $P = (a + b\sqrt{-2})$ for which $a^2 + 2b^2 = p$.

Proposition 119. If $\sqrt{\frac{4|d|}{3}} < 3$, then every ideal of R is equivalent in $C(R)$ to R or an ideal of norm 2.

Example 120. **Case 1.** Consider the case $d = -5$. We have a prime ideal Q such that $N(Q) = 2$. Then

$$N(a + b\sqrt{-5}) = a^2 + 5b^2 \neq 2 \tag{187}$$

If p is split in $\mathbb{Z}[\sqrt{-5}]$ (or equivalently $\left(\frac{-5}{p}\right) = 1$), then there exists ideal P such that $N(P) = p$. The theorem says that we get either $P \sim R$ or $P \sim Q$, i.e. either $p = a^2 + 5b^2$ or $2p = a^2 + 5b^2$. We get the latter because $N(QP) = 2p$.

10 . - -Monday, 4.22.2019

10.1

Recall that we are talking about $\mathbb{Z}[\sqrt{d}],\ d < 0$ square free, $\equiv 2, 3 \mod 4$. Every member of the class group of $\mathbb{Z}[\sqrt{d}]$ is represented by an ideal $J \subseteq \mathbb{Z}[]\sqrt{d}$ with $N(J) \leq \frac{4|d|}{3}$.

We looked at some applications. For instance,

1.) $d = -1,\ p \equiv 1 \mod 4$ then there exists $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$.
2.) $d = -2, p \equiv 1, 3 \mod 8$ then there exists $a, b \in \mathbb{Z}$ for which $p = a^2 + 2b^2$

where $N(J) \leq 1$.

Next, for $\sqrt{\frac{4|d|}{3}} < 3$, we take $d = -5, -6$. If $d = -6$, then

1.) $N(J) = 1$ (i.e. $J = \mathbb{Z}[\sqrt{-6}]$)
2.) $N(J) = 2$, $J = (2, \sqrt{-6})$ is unique, but not principal.

Here, $a^2 + 6b^2 = 2$ has no solutions. Thus, if $I \subseteq \mathbb{Z}[\sqrt{-6}]$ is an ideal, then either I is principal or IJ is principal.

For instacne, if p is a split prime in $\mathbb{Z}[\sqrt{-6}]$, then there exists $P \subseteq \mathbb{Z}[\sqrt{-6}]$ such that $N(P) = p$ and either $p = a^2 + 6b^2$ or $2p = a^2 + 6b^2$.

Now p is split iff $\left(\frac{-6}{p}\right) = 1$ iff either $\left(\frac{-3}{p}\right) = \left(\frac{2}{p}\right) = 1$ or $\left(\frac{-3}{p}\right) = \left(\frac{2}{p}\right) = -1$. One can then deduce that this is true iff either $p \equiv 1 \mod 3$ and $p \equiv \pm 1 \mod 8$ or $p \equiv 2 \mod 3$ and $p \equiv 3, 5 \mod 8$.

Now if $p = a^2 + 6b^2$, then thinking of the quadratic residues mod 3, we must have $p \equiv 1 \mod 3$. In the case $2p = a^2 + 6b^2$, we can take $a = 2a'$, and so, $p = 2{a'}^2 + 3b^2$. Here, $p \equiv 2 \mod 3$.

In the Pierre Samuels notes, see 2-torsions in absolute class group for an iff statement of the above.

10.2

Let's now consider the case $d < 0$ and $d \equiv 1 \mod 4$. Then $\theta = \frac{1+\sqrt{d}}{2}$, and as we deduced before

$$\text{Im}(\theta) = \frac{\sqrt{|\theta|}}{2},\ \text{Area}(\mathbb{C}/R) = \frac{\sqrt{|d|}}{2} = \sqrt{\frac{|d|}{4}} \tag{188}$$

Every element of the class group represented by $J \subseteq R = \mathbb{Z} + \mathbb{Z}\theta$ for which $N(J) \leq \sqrt{\frac{|d|}{3}}$ for which d is $\sqrt{\frac{|d|}{3}} < 3$.

Here is a corollary of this.

Proposition 121. If $d = -3, -7, -11$, then $\mathbb{Z} + \mathbb{Z}\theta$ is a PID.

Remark 122. This is stronger than what we do in Honors Algebra in which we use Euclidean domain to show PID.

Remark 123. Gauss found 9 cases in which they are PIDs, and it was proven in 1960s or so that those are all of them. See Wikipedia.

We see if there are more of these:

Example 124. Consider $d = -163$, then for $J \subseteq R$

$$N(J) = \sqrt{\frac{163}{3}} < 8 \tag{189}$$

We can thus look at all ideals J for which $N(J) \leq 7$.

$$N(J) = 1 \qquad J = R \tag{190}$$

$$N(J) = 2 \qquad -163 \equiv 5 \; mod 8 \implies \text{2 not split prime} \tag{191}$$

So, such a J does not exist.

$$N(J) = 3 \qquad -163 \equiv -1 \mod 3 \tag{192}$$

So no such J. But now

$$N(J) = 4 \tag{193}$$

for which we have principal ideal $J = (2)$.

$$N(J) = 5 \implies \left(\frac{-163}{5}\right) = -1 \tag{194}$$

but, $-163 \not\equiv \pm 1 \mod 5$, so such a J does not exist.

$N(J) = 6$ does not exist. Finally,

$$N(J) = 7 \implies \left(\frac{-163}{7}\right) = 1, \left(\frac{-2}{7}\right) = -1 \tag{195}$$

so J does not exist. Thus, $\mathbb{Z} + \mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right]$ is a PID.

As we see in the above, there is an element of luck for this ring to be a PID. But Gauss conjectured that luck would run out for larger d, and it was correct. But this is not entirely obvious.

Example 125. We have $-7 \equiv 1 \mod 8$ implies 2 is a split prime.

We can see that for the cases

$$d = -7, -15, ..., -39, ... \tag{196}$$

it is indeed a split prime, i.e. there exists a prime ideal P whose norm is 2.

What are the necessary conditions for this? If we have $\alpha \in \mathbb{Z} + \mathbb{Z}\theta$ with $N(\alpha) = p$, then $a^2 + b^2 = 4p$ for which taking $p = 2$, we get

$$a^2 + b^2 d = 8 \qquad a^2 + 7b^2 = 8 \tag{197}$$

10.3

Let's now consider subgroups B of $A := \mathbb{Z}^n$ which is a free abelian group.

Proposition 126 (Integral Basis.). Let $B \leq A := \mathbb{Z}^n$ with $[A : B] < \infty$. Then there exists $m_1, ..., m_n \in \mathbb{N}$ for which the elements in B given by

$$U_1 := (m_1, 0, ..., 0) \tag{198}$$

$$U_2 := (a_{12}, m_2, 0, ..., 0) \tag{199}$$

...

$$U_n := (a_{1n}, ..., a_{n-1,n}, m_n) \tag{200}$$

are an integral basis of B, i.e. satisfy the following properties:

1.) every $\alpha \in B$ can be expressed uniquely as

$$h_1 U_1 + ... + h_n U_n \qquad h_i \in \mathbb{Z} \tag{201}$$

2.) $[A : B] = m_1 ... m_n$

In particular, we have the following:

Proposition 127. For $T \in M_n(\mathbb{Z}),\ \det T \neq 0$, then $T(\mathbb{Z}^n) \leq \mathbb{Z}^n$ and $[\mathbb{Z}^n : T(\mathbb{Z}^n)] = |\det T| < \infty$.

PROOF 128 (Integral Basis implies the Matrix Theorem.). If $e_1, e_2, ...$ are the standard $\mathbb{Z}$-basis for $\mathbb{Z}^n$, then $Te_1, Te_2, ...$ form a $\mathbb{Z}$-basis for $T(\mathbb{Z}^n)$.

But now, $U_1, U_2, ...$, also form a $\mathbb{Z}$-basis. We can thus take a change of basis matrix $R \in M_n(\mathbb{Z})$ such that

$$[Te_1, Te_2, ...] = R[e_1, e_2, ...] \tag{202}$$

and in particular, $\det R = \pm 1$, so $|\det T| = |\det U|$ where U is the matrix whose columns are U_i. But $\det U$ can be computed easily since it is lower triangular. □

PROOF 129 (Integral Basis.). We do the proof in the special case $n = 2$. Take

$$\pi : \mathbb{Z}^2 \to \mathbb{Z} \tag{203}$$

$$(u, v) \mapsto v \tag{204}$$

Then $\pi(B) \leq \mathbb{Z}$. **Exercise.** $\pi(B)$ is not the zero subgroup.

Then there exists $m_2 \in \mathbb{N}$ such that $\pi(B) = \mathbb{Z}m_2$. Thus, there exists $a_{12} \in \mathbb{Z}$ for which $(a_{12}, m_2) \in B$.

But now, we take

$$B \cap \mathbb{Z} \times \{0\} = m_1 \mathbb{Z} \times \{0\} \tag{205}$$

then $(m_1, 0) \in B$.

Exercise. This does indeed give a basis.

Now taking

$$S := \big\{(u, v) \in \mathbb{Z}^2 :\ u \in [0, m_1),\ v \in [0, m_2)\big\} \tag{206}$$

every element of $\mathbb{Z}^2$ is uniquely expressed as $s + b$ for $s \in S, b \in B$ and likewise for B, we can write it as linear combination of U_1, U_2. □

11 . - -Wednesday, 4.24.2019

11.1 Announcements.

1.) OH
  (a.) Wednesday 4-6pm
  (b.) Thurs: 9:30am-11:30am, 2-4
2.) Psession
  (a.) Moved to Friday 4-5pm just for this week.
3.) See module for some sample computations
4.) Do HW 3 before midterm; it WILL be helpful

11.2

Up until now, we have considered quadratic fields. We will now consider higher degree extensions which are nice.

Definition 130. $\alpha \in \mathbb{C}$ is **algebraic** if it is a root of some $p \in \mathbb{Q}[X]$. It is **transcendental** otherwise.

Example 131. $\sqrt{d},\ d \in \mathbb{Z}$ is a root of $X^2 - d$.

Example 132. Primitive nth root of unity ζ_n is a root of $x^n - 1$. Note that this is not the polynomial of least degree for which it is a root. For instance, $\zeta_4 = i$ is a root of $x^4 + 1$.

Proposition 133. $\mathbb{Q}[x]$ is a PID.

PROOF 134. Let $I \subseteq \mathbb{Q}[X]$ be an ideal. Let $f \in I$ nonzero of least degree. Now given $g \in I$, the division algorithm says there are q, r such that

$$g = fq + r \tag{207}$$

for which $\deg r < \deg f$. Then $r \in I$ and $\deg r = 0$ by minimality, so $g \in (f)$. □

Now take $\alpha \in \mathbb{C}$ algebraic. Then from the proposition, there is some g for which

$$I = \{f \in \mathbb{Q}[x] : f(\alpha) = 0\} = (g) \tag{208}$$

Up to scaling, we can assume g is monic.

Definition 135. The unique polynomial given above is the **minimal polynomial** of α.

Proposition 136. Suppose $\alpha \in \mathbb{C}$ is algebraic with minimal polynomial of degree n. Then $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$ and it has a $\mathbb{Q}$-basis $1, \alpha, ..., \alpha^{n-1}$.

PROOF 137. The second statement is obvious. For the first, suppose

$$g(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 \tag{209}$$

$$g(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0 = 0 \tag{210}$$

$$\alpha^{-1} = \frac{\alpha^{n-1} + a_{n-1}\alpha^{n-1} + ... + a_1}{a_0} \in \mathbb{Q}[\alpha] \tag{211}$$

□

Definition 138. A **field** $K \subseteq \mathbb{C}$ **is algebraic over** $\mathbb{Q}$ of $[K : \mathbb{Q}] < \infty$.

Remark 139. We can replace $\mathbb{Q}$ in the above with an arbitrary field E and everything holds.

Example 140. If α is algebraic, then so is $\mathbb{Q}(\alpha)$.

Remark 141. If K is algebraic and $\alpha \in K$, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] < [K : \mathbb{Q}] < \infty$. Then α is algebraic (since $1, \alpha, ..., \alpha^{[\mathbb{Q}(\alpha):\mathbb{Q}]-1}$ are linearly dependent).

11.3 Trace and Norm.

Definition 142. The **trace** $\mathrm{Tr}_K(\alpha)$ and **norm** $N_K(\alpha)$ of $\alpha \in K$ are the trace and determinant of the multiplication by α map.

Let's demonstrate this. Take $K = \mathbb{Q}(\alpha)$ and $g = m_\alpha$ be the minimal polynomial of α. We know that $1, \alpha, ..., \alpha^{n-1}$ is a basis. Then

$$A = \begin{pmatrix} 0 & 0 & \dots & -a_0 \\ 1 & 0 & \dots & -a_1 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & -a_{n-1} \end{pmatrix} \tag{212}$$

where the a_i are the coefficients of the minimal polynomial. From this, we see that

$$\mathrm{Tr}_K(\alpha) = -a_{n-1},\ N_K(\alpha) = (-1)^n a_0 \tag{213}$$

Remark 143. We also have that if $K \supsetneq \mathbb{Q}(\alpha)$, we can pick a basis $\beta_1, ..., \beta_l$ of K over $\mathbb{Q}(\alpha)$. Then $\{\beta_i \alpha_j : i \in [1, l],\ j \in [0, n-1]\}$ is a basis of K over $\mathbb{Q}$.

Now the multiplication by α in this basis is just the block diagonal matrix whose blocks are all A. Thus,

$$\mathrm{Tr}_K(\alpha) = l\mathrm{Tr}_{\mathbb{Q}(\alpha)}(\alpha),\ N_K(\alpha) = N_{\mathbb{Q}(\alpha)}(\alpha)^l \tag{214}$$

11.4

Proposition 144 (Primitive Element Theorem.). If K is algebraic, then there exists $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$.

Remark 145. This theorem is magical but not nice in practice. For one thing, we do not know how the Galois group acts on α. Also, when we come up with K, we pick the generators to be nice anyways.

Proposition 146. Suppose $g \in \mathbb{Q}[x]$ is the minimal polynomal of some $\alpha \in \mathbb{C}$. Then it has no repeated roots (i.e. g is a separable polynomial).

PROOF 147. Suppose β is another root of g. Then it has to be the root of the minimal polynomial of β (from irreducibility of g). Now if we assume α is a repeated root, then taking formal derivatives

$$g(x) = (x-\alpha)^2 f(x) \tag{215}$$

$$g'(x) = 2(x-\alpha)f + (x-\alpha)f' \tag{216}$$

and $g'(\alpha) = 0$ but this violates minimality.

□

Proposition 148. If α_1, α_2 have the same minimal polynomial g, then $\mathbb{Q}[\alpha_1] \cong \mathbb{Q}[\alpha_2]$ (i.e. normal extension).

PROOF 149.

$$\mathbb{Q}(\alpha_1) = \mathbb{Q}[\alpha_1] \cong \mathbb{Q}[x]/(g) \cong \mathbb{Q}[\alpha_2] = \mathbb{Q}(\alpha_2) \tag{217}$$

□

Note that we do not necessarily get *equality*.

Example 150. $m_{\sqrt[4]{2}} = x^4 - 2$ and $\mathbb{Q}(\sqrt[4]{2}) \cong \mathbb{Q}[i\sqrt[4]{2}]$ but they are not equal.

Remark 151. Let $K = \mathbb{Q}(\alpha)$, $g = m_\alpha$. Suppose $\alpha := \alpha_1; \alpha_2, ..., \alpha_n$ are roots of n, then for each i there exits a field isomorphism

$$\sigma_i : \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha_i) \cong \mathbb{Q}(\alpha_i) \tag{218}$$

$$p(\alpha_1) \mapsto p(\alpha_i) \tag{219}$$

Definition 152. If $\mathbb{Q}(\alpha_i) \subseteq \mathbb{R}$, then σ_i is a **real embedding**. If $\mathbb{Q}(\alpha_i) \not\subset \mathbb{R}$, this is a **complex embedding**. If $\alpha_i \in \mathbb{C} \setminus \mathbb{R}$, then $\overline{\alpha}_i$ is also a root, i.e. complex embeddings come in pairs. $n = r_1 + 2r_2$ where r_1 is the number of real embeddings and r_2 is the number of complex embeddings.

Definition 153. $\alpha \in \mathbb{C}$ is an **algebraic integer** if α is a root of a monic polynomial in $\mathbb{Z}[x]$.

Definition / Proposition 154. If K is an algebraic field, then the ***ring* of algebraic integers**is

$$\mathcal{O}_K = \{\alpha \in K | \text{ algebraic integer}\} \tag{220}$$

Example 155. $K = \mathbb{Q}(\sqrt{d})$ then

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \mod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \mod 4 \end{cases} \tag{221}$$

Example 156. $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$

12 . - -Monday, 4.29.2019

We start where we left off last time.

Definition 157. $\alpha \in \mathbb{C}$ is an algebraic integer if it is a root of a monic polynomial $p \in \mathbb{Z}[x]$.

Definition 158. Suppose K is an algebraic number field (i.e. finite extension of $\mathbb{Q}$). The **ring of integers** is

$$\mathcal{O}_K := \{\alpha \in K : \alpha \text{ is an algebraic integer}\} \tag{222}$$

Example 159. For $K = \mathbb{Q}[\sqrt{d}]$, then $\mathcal{O}_K = R$.

Example 160. $K = \mathbb{Q}$ then $\mathcal{O}_K = \mathbb{Z}$.

Proof. $\alpha \in \mathbb{Z}$ is a root of $\mathbb{Z}[x]$.

On the other hand, if $p/q \in \mathbb{Q}$ reduced, then assume it is a root of a monic polynomial over $\mathbb{Z}$. Then we can clear denominators, and see from $\gcd(p, q) = 1$ that we must have $q = 1$. □

Proposition 161. Suppose α is an algebraic number. Then there exists $m \in \mathbb{Z}$ such that $m\alpha$ is an algebraic integer.

PROOF 162. Let

$$m_\alpha(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 \in \mathbb{Q}[x] \tag{223}$$

Let $m \in \mathbb{Z}$ be the common denominator of the coefficients. Then $m\alpha$ is the root of

$$x^n + ma_{n-1}x^{n-1} + ... + m^n a_0 \in \mathbb{Z}[x] \tag{224}$$

□

Here is one of the big theorems for today:

Proposition 163. TFAE:

1.) α is an algebraic integer
2.) $m_\alpha \in \mathbb{Z}[x]$
3.) $\mathbb{Z}[\alpha]$ is finitely generated $\mathbb{Z}$-module
4.) there exists finitely generated $\mathbb{Z}$-module $M \subseteq \mathbb{C}$ nonzero such that $\alpha M \subseteq M$

PROOF 164. We skip $1 \implies 2$ for now. $2 \implies 3$ follows from taking the powers of α to be the generators. For $3 \implies 4$, take $M = \mathbb{Z}[\alpha]$.

($4 \implies 1$.) The idea is to observe that α is related to some matrix and hence some characteristic polynomial. The natural choice of this matrix is the multilication by α matrix.

Write

$$M = \mathbb{Z}\omega_1 + ... + \mathbb{Z}\omega_n \tag{225}$$

and since $\alpha M \subseteq M$, we can write

$$\alpha\omega_i = \sum_j a_{ij}\omega_j \tag{226}$$

for $a_{i,j} \in \mathbb{Z}$. Let $A := (a_{i,j})$ and take $B := \alpha\mathbf{Id}_n - A$. Then B has nontrivial kernel, so $\det(B) = 0$. Thus, $\det(x\mathbf{Id} - A) \in \mathbb{Z}[x]$ with root α which proves our claim.

□

Definition 165. A **polynomial over $\mathbb{Z}$ is primitive** if the coefficients are relatively prime.

Proposition 166 (Gauss Lemma). Product of primitive polynomials is primitive.

PROOF 167. Suppose $f, g \in \mathbb{Z}[x]$ primitive, and assume for contradiction that the product is not primitive. Then there exists a prime $p \in \mathbb{Z}$ which divides the coefficients of fg. Then consider the quotient map $\mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$. Then $\overline{fg} = 0$, but $\overline{f}, \overline{g}$ by hypothesis. But this is a contradiction since $(\mathbb{Z}/p\mathbb{Z})[x]$ is an integral domain.

□

Remark 168. For $f \in \mathbb{Q}[x]$, there exists $m, n \in \mathbb{Z}$ relatively prime so that $\frac{m}{n} \cdot f$ primitive. We choose m to clear the denominators and n to kill off gcd of the coefficients of f.

We use this remark to finish $1 \implies 2$ in the previous proof.

PROOF 169 ($1 \implies 2$). Take $f \in \mathbb{Z}[x]$ monic with $f(\alpha) = 0$, and $g = m_\alpha \in \mathbb{Q}[x]$. Take $f = gh$ for some $h \in \mathbb{Q}[x]$. Then by the remark, take $m, n, u, v \in \mathbb{Z}$ with m, n and u, v respectively relatively prime and so that

$$g = \frac{m}{n}\psi_1, \ h = \frac{u}{v}\psi_2 \tag{227}$$

hwere $\psi_1, \psi_2 \in \mathbb{Z}[x]$ are primitive. Then

$$nvf = mu\psi_1\psi_2 \tag{228}$$

where $\psi_1\psi_2$ is primitive by Gauss lemma and f primitive because it's monic.

Then $f = \pm\psi_1\psi_2$, and since f is monic, the leading coefficent of ψ_1 is ± 1. Now $g = \frac{m}{n}\psi_1$ so $\frac{m}{n} = \pm 1$ and thus $g \in \mathbb{Z}[x]$.

□

Here is a corollary.

Proposition 170. $\mathcal{O}_K$ is a ring.

PROOF 171. Suppose $\alpha, \beta \in \mathcal{O}_K$, consider $\mathbb{Z}[\alpha, \beta]$. Let $\gamma = \alpha + \beta$ or $\alpha\beta$ then $\gamma\mathbb{Z}[\alpha, \beta] \subseteq \mathbb{Z}[\alpha, \beta]$. Thus, $\gamma \in \mathcal{O}_K$.

□

Proposition 172. Let M be a $\mathbb{Z}$-module generated by $e_1, ..., e_m$. Suppose $N \subseteq M$ be a $\mathbb{Z}$-submodule. Then there exists $\beta_1, ..., \beta_n, \ n \leq m$ such that

$$\beta_i = \sum_{i \leq j} k_{i,j} e_j \qquad k_{i,j} \geq 0 \tag{229}$$

PROOF 173. We do induction.

Let $p_1 : M \to \mathbb{Z}e_2 + ... + \mathbb{Z}e_m$ be the projection onto the last $n - 1$ coordinates. Let $p_2 : M \to \mathbb{Z}$ be the projection onto the first coordinate.

Now $N^1 := p_1(N)$. By induction hypothesis, we get $\beta_2, ..., \beta_n$ generating N^1 and satisfying the desired conditions. We also have some $k_{11} \geq 0$ so that $p_2(N) = k_{11}\mathbb{Z}$.

Let $\beta_1 \in N$ be such that $p_1(\beta_1) = k_{11}$. We need to show $\beta_1, ..., \beta_n$ generates N. Suppose $\alpha \in N$, then $p_1(\alpha) = sk_{11}$. Then $\alpha - s\beta_1 \in (\mathbb{Z}e_2 + ... + \mathbb{Z}e_m) \cap N$ so it is spanned by $\beta_2, ..., \beta_n$.

□

Proposition 174. If $K/\mathbb{Q}$ is a finite extension, then there exists $\beta_1, ..., \beta_n \in \mathcal{O}_K$ such that

$$\mathcal{O}_K = \mathbb{Z}\beta_1 + ...\mathbb{Z}\beta_n \tag{230}$$

and likewise for K.

Example 175. We already know the example for $K = \mathbb{Q}[\sqrt{d}]$.

PROOF 176. Start with any basis $f_1, ..., f_n \in K$ whcih we can assume wlog are in $\mathcal{O}_K$ because we can always multiply by $m \in \mathbb{Z}$ so that $mf_i \in \mathcal{O}_K$.

Then define the nondegenerate bilinear form

$$B(x, y) := \mathrm{Tr}_K(xy) \tag{231}$$

on K. We get a dual basis $e_1, ..., e_n$ with respect to B. Here, we do not require that $B(f_i, e_i) = 1$, but we do require that $B(f_i, e_j) = 0$ for $i \neq j$.

If we now take

$$z = \sum a_i e_i \in \mathcal{O}_K \tag{232}$$

then $B(z, f_i) = a_j \in \mathbb{Z}$.

Then $\mathcal{O}_K \subseteq \mathbb{Z}e_1 + ... + \mathbb{Z}e_n$. From the lemma, there exists $\beta_1, ..., \beta_n$ with the desired property.

□

13 Review Lecture. - -Wednesday, 5.1.2019

13.1 Announcements.

1.) Billy's OH: 11am
2.) Nori OH: moved from 2pm start to 4pm start
3.) No psession

13.2 Review of Quadratic Extensions.

We review topics from the earlier part of the course since there has been misconceptions in the midterm.

Let $K = \mathbb{Q}(\sqrt{d})$ and the ring of integers is given by $\mathcal{O}_K = \mathbb{Z}[\theta]$ for

$$\theta = \begin{cases} \sqrt{d} & d \equiv 2, 3 \mod 4 \\ \frac{1+\sqrt{d}}{2} & d \equiv 1 \mod 4 \end{cases} \tag{233}$$

1.) Ramified prime: Finite set since the condition is $p|d$ or $p = 2$ if $d \equiv 2, 3 \mod 4$
   (a.) When $d \equiv 2, 3 \mod 4$, then $P = (p, \sqrt{d})$ for which $|\mathcal{O}_K/P| = p$
   (b.) When $d \equiv 3 \mod 4$, then $p = 2$ and $P = (2, 1 + \sqrt{d})$
2.) Nonsplit prime. $p \equiv 3 \mod 4$
   (a.) The condition is just $\left(\frac{d}{p}\right) = -1$ and the unique prime ideal giving this is $P = (p)$
3.) Split prime. $p \equiv 1 \mod 4$
   (a.) Here, we can take $P = (p, \sqrt{d})$.
   (b.) The condition is $\left(\frac{d}{p}\right) = 1$ and we have the two prime ideals $P = (p, \sqrt{d} \pm a)$ where $a^2 = d \mod p$.

Note that unramified primes are infinite by Euclid's argument.

Problem. How many ideals are there of norm p^{101} in $\mathcal{O}_K$, $K = \mathbb{Q}(\sqrt{d})$ where p is a prime.

1.) If p is ramified, then it is unique: P^{101}.
2.) If p is nonsplit, then there aren't any because 101 is odd.
3.) When p is split, there are 101+1 = 102. The first 100 come in pairs. The last one is given by the choice between $P,\ \sigma P$.

13.3 Computation of the Class Group.

Example 177. Take $K = \mathbb{Q}[\sqrt{-37}]$. Then

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-37} \tag{234}$$

Gauss says we need to consider ideals $J \subseteq \mathcal{O}_K$ for which $N(J) = sm \leq \sqrt{\frac{4}{3} \cdot 37} < 8$. So we need to look at $m = 1, 2, 3, 4, 5, 6, 7$.

m	1	2	3	4	5	6	7
	$\mathcal{O}_K$	P_2	None	$P_2^2 = (2)$	None.	None.	None.

Thus, Gauss says all primes are P_2 or $\mathcal{O}_K$. But now, P_2 is not principal as we can see from the fact that $a^2 + 37b^2 = 2$ does not have integer solutions. Thus, the class group is C_2.

We recall from before that $P_2 = (2, \sqrt{-37} + 1)$.

Example 178. Take $K = \mathbb{Q}[\sqrt{-42}]$. Then $m^2 \leq 56$.

m	1	2	3	4	5	6	7
	$\mathcal{O}_K$	P_2	P_3	P_2^2	None.	P_2P_3	P_7

So we must think about $\mathcal{O}_K, P_2, P_3, P_2P_3, P_7$.

Now observe that we must have $(\sqrt{-42}) = P_2P_3P_7$, so we don't have to consider P_7. Also, P_2, P_3 must have order 2. P_2P_3 is not principal by the same argument as before and so P_2, P_3, P_2P_3 are distinct.

There are only two choices: V_4 or C_4.

14 . - -Friday, 5.3.2019

Example 179. Take $K = \mathbb{Q}[\sqrt{d}]$ and $\mathcal{O}_K$ the ring of integers. Take $\alpha \in \mathcal{O}_K$ for which the norm has absolute value 23. We can deduce from this that $\mathcal{O}_K/(\alpha)$ has 23 elements, and hence it is a field. Thus, (α) is a prime ideal, and since 23 is a zero in the quotient, we have $(23, \alpha)$.

Example 180. Suppose instead that $|N(\alpha)| = 46$. Here $23 \notin (\alpha)$. What is $(23, \alpha) \supsetneq (\alpha)$? Consider the prime factorization of $(\alpha) = P_1P_2$. Then wlog, $(\alpha) \subseteq P_2$, and we have $N(P_1) = 2,\ N(P_2) = 23$. So, $P_2 = (23, \alpha)$.

14.1 Volumes.

We work in $\mathbb{R}^n$. We define the volume of $\prod_{i=1}^n [a_i, b_i]$ in the obvious way (given by Lebesgue measure). Translation invariance etc can be formalized in terms of Lebesgue measures (in particular, sets should all be Lebesgue measurable).

Definition 181. Let $\omega_1, ..., \omega_n$ be an $\mathbb{R}$-basis. The **lattice given by** $\omega_1, ..., \omega_n$ is the set

$$\Gamma := \mathbb{Z}\omega_1 + ... + \mathbb{Z}\omega_n = \left\{ \sum_{i=1}^n a_i \omega_i : a_i \in \mathbb{Z} \right\} \tag{235}$$

Exercise 182. A subgroup of Γ of $\mathbb{R}^n$ is a lattice if Γ is a discrete subset of $\mathbb{R}^n$ and if $\mathbb{R}^n/\Gamma$ is compact.

Definition 183. A subset $F \subseteq \mathbb{R}^n$ is a **fundamental set for** Γ if $\mathbb{R}^n$ is the disjoint union of translates $F + \gamma$ for all $\gamma \in \Gamma$.

Example 184. If $\Gamma = \mathbb{Z}\omega_1 + ... + \mathbb{Z}\omega_n$ (where ω_i are linearly independent), then

$$F = \left\{ \sum_{i=1}^n t_i \omega_i : t_i \in [0, 1) \, \forall i \right\} \tag{236}$$

is a fundamental set for Γ.

Proof. Let $x \in \mathbb{R}^n$. Then $\omega_1, ..., \omega_n$ is a basis, so

$$x = \sum_{i=1}^n x_i \omega_i \tag{237}$$

where we can write $x_i = m_i + t_i$ for $m_i \in \mathbb{Z}, \ 0 \leq t_i < 1$ so

$$x = \sum_i m_i \omega_i + \sum_i t_i \omega_i \tag{238}$$

where the first term is in Γ and the second in F. □

Remark 185. Here is how one computes the volume of $G \subseteq \mathbb{R}^n$. By definition,

$$\mathbb{R}^n = \amalg_{\gamma \in \Gamma} \gamma + F \tag{239}$$

from which we see that

$$G = \amalg_{\gamma \in \Gamma} \Gamma \cap (\gamma + F) \tag{240}$$

Thus, the volume is

$$\mathrm{Vol}(G) = \sum_{\gamma \in \Gamma} \mathrm{Vol}(G \cap (\gamma + F)) = \sum_{\gamma \in \Gamma} \mathrm{Vol}(G - \gamma \cap F) \tag{241}$$

Remark 186. If F', F are fundamental sets for Γ, then $\mathrm{Vol}(F') = \mathrm{Vol}(F)$.

Proof. Put $G = F'$ in the previous remark, and take $\gamma_1, \gamma_2 \in \Gamma$ distinct. Then $F' - \gamma_1, F' - \gamma_2$ are disjoint, and it follows that

$$((F' - \gamma_1) \cap F) \cap ((F' - \gamma_2) \cap F) = \emptyset \tag{242}$$

Thus, the set $(F' - \gamma) \cap F,\ \gamma \in \Gamma$ are all disjoint. Thus

$$\mathrm{Vol}(F') = \sum_{\gamma \in \Gamma} \mathrm{Vol}((F' - \gamma) \cap F) \leq \mathrm{Vol}(F) \tag{243}$$

The other direction follows likewise. □

Definition 187. Let $\Gamma \subseteq \mathbb{R}^n$ be a lattice. Then

$$\mathrm{Vol}(\mathbb{R}^n/\Gamma) := \mathrm{Vol}(F) \tag{244}$$

where F is a fundamental set for Γ.

This volume is clearly finite since it is contained in a compact set.

Remark 188. Take $\mathbb{R}^n \supseteq \Gamma \supseteq \Gamma'$ where Γ, Γ' are lattices. Then $[\Gamma : \Gamma'] < \infty$ and

$$\mathrm{Vol}(\mathbb{R}^n/\Gamma') = \mathrm{Vol}(\mathbb{R}^n/\Gamma)[\Gamma : \Gamma'] \tag{245}$$

Proof. Let F be a fundamental set for Γ. Choose a set $S \subseteq \Gamma$ which is a set of coset representatives for Γ/Γ' (i.e. $S \to \Gamma/\Gamma'$ is a bijection). We claim that

$$F' = \amalg_{s \in S} s + F \tag{246}$$

is a fundamental set for Γ'.

Proof of Claim. Let $x \in \mathbb{R}^n$, then $\gamma \in \Gamma$ and $y \in F$ such that $x = y + \gamma$. Since $S \to \Gamma/\Gamma'$ is a bijection, so $\gamma = \gamma' + s$ for $\Gamma' \in \Gamma, s \in S$. Now

$$x = (y + s) + \gamma' \tag{247}$$

where $y + s \in F',\ \gamma' \in \Gamma'$.

Now (**exercise**):

$$\mathbb{R}^n = \amalg_{\gamma' \in \Gamma'} F + \gamma' \tag{248}$$

Thus,

$$\mathrm{Vol}(\mathbb{R}^n/\Gamma') = \mathrm{Vol}(F') = \sum_{s \in S} \mathrm{Vol}(F + s) = \#S \cdot \mathrm{Vol}(F) = [\Gamma : \Gamma']\mathrm{Vol}(\mathbb{R}^n/\Gamma) \tag{249}$$

Remark 189. $\Gamma \subseteq \mathbb{R}^n$ is a lattice and $G \subseteq \mathbb{R}^n$. Assume $\mathrm{Vol}(G) > \mathrm{Vol}(\mathbb{R}^n/\Gamma)$. Then there exists $g_1, g_2 \in G$ distinct and $g_1 - g_2 \in \Gamma$.

Proof. Choose a fundamental set F for Γ. If the sets $(G - \gamma) \cap F$ taken over alla $\gamma \in \Gamma$, where mutually disjoint, then

$$\mathrm{Vol}(F) \geq \sum_{\gamma \in \Gamma} \mathrm{Vol}(F \cap (G - \gamma)) = \mathrm{Vol}(G) \tag{250}$$

which is a contradiction.

Thus, there exists $\gamma_1, \gamma_2 \in \Gamma$ distinct and $(G - \gamma_1), G - \gamma_2$ disjoint. □

15 . - -Monday, 5.6.2019

Recall from last time: we proved that $\Gamma \subseteq \mathbb{R}^n$ is a lattice and if $G \subseteq \mathbb{R}^n$ is Lebesgue measurable [5] and if $\text{Vol}(G) > \text{Vol}(\mathbb{R}^n/\Gamma)$, then there exists distinct elements $g_1, g_2 \in G$ whose difference lies in Γ. [6]

Proposition 190 (Minkowski's Convex Body Lemma.). Let $\Gamma \subseteq \mathbb{R}^n$ is a lattice, $G \subseteq \mathbb{R}^n$ convex, symmetric, and $\text{Vol}(G) > 2^n \text{Vol}(\mathbb{R}^n/\Gamma)$, then there exists $\gamma \in \Gamma \cap G$ nonzero.

PROOF 191. Since

$$\text{Vol}\left(\frac{1}{2}G\right) = \frac{1}{2^n}\text{Vol}(G) > \text{Vol}(\mathbb{R}^n/\Gamma) \tag{251}$$

there exists $g_1, g_2 \in G$ distinct and their difference lies in Γ. Then $g_2 \in \frac{1}{2}G$ and the region is symmetric, so $-g_2 \in \frac{1}{2}G$. Thus,

$$\gamma := g_1 + (-g_2) \in G \tag{252}$$

which is nonzero by assumption.

□

Example 192. We use the above argument to the special case $\mathbb{R}^2 = \mathbb{C}$. Take G to be the open ball around the origin with radius r. Then its area is πr^2 which has area larger than $4\text{Area}(\mathbb{C}/\Gamma)$, so by Minkowski, there is $\gamma \in \Gamma \cap G$ nonzero with $|\gamma|^2 < r^2$.

Then taking

$$\tilde{r}^2 = \frac{4}{\pi}\text{Area}(\mathbb{C}/\Gamma) \tag{253}$$

Now for $\epsilon > 0$, we get $\gamma \in \Gamma$ nonzero, so $|\gamma| < \tilde{r} + \epsilon$ which implies that there is a nonzero element $\gamma \in \Gamma$ with $|\gamma| \leq \tilde{r}$. We get $\gamma \in \Gamma$ nonzero such that $|\gamma|^2 \leq \frac{4}{\pi}\text{Area}(\mathbb{C}/\Gamma)$.

Note that this is a better bound than what we get from Gauss Reduction for Positive Definite Binary Forms: $\leq \frac{4}{3}\text{Area}(\mathbb{C}/\Gamma)$.

Definition 193. Let K be a number field. We define the **ring of integers over** K $\mathcal{O}_K$ as the collection of $\alpha \in K$ integral over $\mathbb{Z}$.

Remark 194. As an additive group,

$$\mathcal{O}_K = \mathbb{Z}\omega_1 + ... + \mathbb{Z}\omega_d \tag{254}$$

for $d := \deg(K/\mathbb{Q})$.

[5] Most books just restrict to open sets.

[6] References: Hardy and Wright, Nagel.

Definition 195. The **discriminant of** K is

$$\det(\mathrm{Tr}_{\mathbb{Q}}^{K}(w_i w_j)) \tag{255}$$

where this matrix is a $d \times d$ symmetric matrix over $\mathbb{Z}$.

Remark 196. The discriminant is independent of the choice of $\mathbb{Z}$-basis. In the case $d \equiv 2, 3 \mod 4$, if B is the change of $\mathbb{Z}$-basis matrix in $\mathcal{O}_K$ and A' is the matrix given by this new matrix, then we get

$$\det(A') = \det A \cdot (\det B)^2 = \det A \tag{256}$$

Example 197. If K is a quadratic extension of $\mathbb{Q}$ for $d \equiv 2, 3 \mod 4$, then we can take $w_1 = 1,\ w_2 = \sqrt{d}$. Then

$$D(K) = \begin{pmatrix} \mathrm{Tr}(1^2) & \mathrm{Tr}(\sqrt{s}) \\ \mathrm{Tr}(\sqrt{s}) & \mathrm{Tr}(\sqrt{s} \cdot \sqrt{s}) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d \tag{257}$$

In the case $d \equiv 1 \mod 4$, we have $\det B = \pm 2$ in the previous remark, so we can then verify that $D(K) = d$. Thus,

$$D(K) = \begin{cases} 4d & d \equiv 2, 3 \mod 4 \\ d & d \equiv 1 \mod 4 \end{cases} \tag{258}$$

15.1 Real Quadratic Fields.

We focus on $d \in \mathbb{Z}$ positive and square free. For instance, the ring $\mathbb{Z}[\sqrt{2}]$, embedded inside $\mathbb{R}$ is not discrete (in fact it is dense), and so it is not very nice. We need to think of a better space to embed it into.

Embed into the ring $\mathbb{R}^2$ where the embedding is given by the map

$$K = \mathbb{Q}[\sqrt{d}] \to \mathbb{R}^2 \tag{259}$$

$$a + b\sqrt{d} \mapsto (a + b\sqrt{d}, a - b\sqrt{d}) \tag{260}$$

The key here is that we defined the map to be a ring homomorphism. This identified $\mathbb{Z} + \mathbb{Z}\sqrt{d}$ with a subring (which is also a lattice) of $\mathbb{R}^2$. The basis is just the image of the basis in the domain, namely $(1,1),\ (\sqrt{d}, -\sqrt{d})$.

It follows that

$$\text{Area}(\mathbb{R}^2/\mathbb{Z}(1,1) + \mathbb{Z}(\sqrt{d}, -\sqrt{d})) = \left| \det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix} \right| = 2\sqrt{d} \tag{261}$$

which in particular is equal to $\sqrt{D(K)}$ when $d \equiv 2, 3 \mod 4$.

Proposition 198. If K is a *real* quadratic field, then

$$\text{Area}(\mathbb{R}^2/\mathcal{O}_K) = \sqrt{|D(K)|} \tag{262}$$

Remark 199 (Back to Class Groups.). Let $I \subseteq \mathcal{O}_K$ be a nonzero ideal. Take $\alpha \in I$ nonzero with

$$N(\mathcal{O}_K\alpha) = \left|N_{\mathbb{Q}}^K(\alpha)\right| \tag{263}$$

as small as possible. Then $I \supseteq \mathcal{O}_K\alpha$, then $\mathcal{O}_K\alpha \supseteq IJ$. So, every element in the class group is represented by the "same such J."

Now since we defined our embedding by $\alpha \mapsto (\alpha, \sigma\alpha)$, in order to minimize $N_{\mathbb{Q}}^K(\alpha)$, we need to minimize $|xy|$. So consider the subset S of $\mathbb{R}^2$ for which $|xy| \leq 1$. This is neither compact nor convex. We instead consider a subregion S' (which has nice properties) for which $|x| + |y| \leq 2$. This is indeed a subregion by the AM-GM inequality. This region S' is a square with region 8.

Now by the same argument,

$$\text{Area}(\left\{|xy| \leq r^2\right\}) \leq \text{Area}(\{|x| + |y| \leq 2r\}) = 8r^2 \tag{264}$$

and so, if $\alpha \in \mathcal{O}_K$ is such that $|x| + |y| \leq 2r$, then $\left|N_{\mathbb{Q}}^K(\alpha)\right| \leq r^2$.

Now if

$$8r^2 > 4\text{Area}(\mathbb{R}^2/I) = \text{Area}(\mathbb{R}^2/\mathcal{O}_K)[\mathcal{O}_K : I] = \sqrt{|D|}N(I) \tag{265}$$

Then $\alpha \in I$ nonzero such that $|N(\alpha)| \leq r^2$.

The conclusion is then that if $I \subseteq \mathcal{O}_K$ nonzero, then there exists $\alpha \in I$ nonzero such that

$$|N(\mathcal{O}_K\alpha)| \leq \frac{N(I)}{2}\sqrt{|D|} \tag{266}$$

16 . - -Wednesday, 5.8.2019

We recall from last time that for $K = \mathbb{Q}[\sqrt{d}],\ d < 0$ squarefree, $\mathcal{O}_K$, and for an ideal $I \subseteq \mathcal{O}_K$, we have

$$\text{Area}(\mathbb{R}^2/\mathcal{O}_K) = \sqrt{|D|} \tag{267}$$

$$\text{Area}(\mathbb{R}^2/I) = N(I)\sqrt{|D|} \tag{268}$$

We also recall that we take the compact region

$$G(r) := \left\{(x, y) \in \mathbb{R}^2 : \ \frac{|x| + |y|}{2} < 2\right\} \tag{269}$$

whose area is just $8r^2$. Now Minkoski's Convex Body Lemma says that

$$\text{Area}G(r) = 8r^2 > 4\text{Area}(\mathbb{R}^2/N(I)) = 4N(I)\sqrt{|D|} \tag{270}$$

Then there exists $\alpha \in I$ nonzero such that $(\alpha, \sigma\alpha) \in G(r)$.

Here are some corollaries.

Proposition 200. There exists $0 \in I$ nonzero such that

$$\left(\frac{|\alpha| + |\sigma\alpha|}{2}\right)^2 \leq \frac{N(I)\sqrt{|D|}}{2} \tag{271}$$

Proposition 201.

$$\left|N_{\mathbb{Q}}^{K}(\alpha)\right| \leq \frac{N(I)\sqrt{|D|}}{2} \tag{272}$$

Proposition 202. Every element of the class group of $\mathcal{O}_K$ is represented by $J \subseteq \mathcal{O}_K$ wiht $N(J) \leq \frac{1}{2}\sqrt{|D|}$.

Here are some concrete consequences:

Example 203. If $\frac{1}{2}\sqrt{|D|} < 2$, i.e. if $\sqrt{|D|} < 4$, then $\mathcal{O}_K$ is a PID, so for instance, in the cases $d = 2, 3, 5, 13$.

Example 204. Let's look at $\frac{1}{2}\sqrt{|D|} < 3$ i.e. $|D| < 36$.

Let's first look at $d \equiv 2, 3 \mod 4$. Then our bound gives $d < 9$. So we take $d = 6, 7$ there exists a unique J whose norm is 2. We can verify that they are principal, so respectively, $\mathbb{Z}[\sqrt{6}],\ \mathbb{Z}[\sqrt{7}]$ are PIDs.

In the case $d \equiv 1 \mod 4$, we have $d < 36$, so we must look at $d = 17, 21, 29, 33$.

For $d = 17$, we have $d \equiv 1 \mod 8$ so it is split, and there is a solution to $N(\alpha) = \pm 2$, so we get a PID. Likewise, for $d = 21, 29$, we get PIDs since for these, 2 is nonsplit.

Now for $d = 33$, we get a ramification.

Remark 205. We can see from working out examples that we have a better chance of getting a PID for imaginary quadratic fields since it is easier to check the unsolvability of $x^2 - dy^2 = p$ for $d < 0$.

Definition 206. For a real quadratic extension K, $\alpha \in K$ **is totally positive** if $\alpha > 0,\ \sigma\alpha > 0$.

Example 207. $\alpha = \sqrt{2} - 1$ is not totally positive in $\mathbb{Q}[\sqrt{2}]$.

Definition 208. The **absolute class group of** $\mathcal{O}_K$ is the group of fractional ideals modulo $\mathcal{O}_K\alpha$ for α totally positive.

Clearly, there is a surjective map φ from the absolute class group to the class group. By considering the kernel of the map φ, we can see that $\mathcal{O}_K\alpha$ is the trivial element of the absolute class group iff there exists β totally positive such that $\mathcal{O}_K\alpha = \mathcal{O}_K\beta$.

Here is a lemma we will complete next time.

Proposition 209. Let I be an element of the absolute class group such that I^2 is trivial. Let $p_1, ..., p_m$ be the set of ramified primes for $\mathcal{O}_K$, and P_i be such that $P_i^2 = (p_i)$. Then I is represented by $\prod_{i=1}^{m} P_i$.

PROOF 210. Let I be a fractional ideal for which $I^2 = (\alpha)$ with α totally positive. Then

$$I\sigma I = (N(I)) \tag{273}$$

for all ideals $I \subseteq \mathcal{O}_K$. If I is fractional, then there exists $n \in \mathbb{N}$ such that $nI \subseteq \mathcal{O}_K$ and $(nI)(\sigma(nI))$ is generated by a natural number.

Now for all fractional ideals I, we have $I\sigma I = (\beta)$ for some $\beta \in \mathbb{Q},\ \beta > 0$.

So putting these together, we write

$$\sigma I = \frac{\beta}{\alpha} I = \gamma I \tag{274}$$

with γ totally positive.

Thus,

$$I = \sigma(\sigma I) = \sigma(\gamma I) = \sigma\gamma \cdot \sigma I = \sigma\gamma \cdot \gamma I = N_{\mathbb{Q}}^{K}(\gamma) I \tag{275}$$

So, $N_{\mathbb{Q}}^{K}(\gamma) = \mathcal{O}_K$ which implies that it is a unit of $\mathcal{O}_K$.

Now since this belongs to $\mathcal{O}_K \cap \mathbb{Q}$, its inverse must belong to $\mathcal{O}_K \cap \mathbb{Q}$, and thus equals ± 1. Since it is totally positive, we get $N_{\mathbb{Q}}^{K}(\gamma) = 1$.

Now we invoke a version of **Hilbert's Theorem 90** which says that $\sigma\gamma \cdot \gamma = 1$ then there exists $\eta \in K$ such that $\gamma = \frac{\sigma\eta}{\eta}$.

Then $\sigma I = \gamma I = \frac{\sigma\eta}{\eta} I$ then $\sigma(\eta^{-1} I) = \eta^{-1} I$. We can then recall the condition for which $\sigma I = I$ and we're done. □

17 . - -Friday, 5.10.2019

17.1 Real Quadratic Fields: An Example.

Example 211. Consider $K = \mathbb{Q}[\sqrt{19}] \supseteq \mathcal{O}_K = \mathbb{Z}[\sqrt{19}]$. For the class group, we enumerate all ideals of norm $\leq \frac{1}{2}\sqrt{|D|} < 5$.

We see that there are 5 ideals:

$$\mathcal{O}_K,\ (2, \sqrt{19} - 1),\ (3, \sqrt{19} \pm 1),\ (2) \tag{276}$$

We need to check if the middle two are principal. For the third one, we must look for solutions of

$$x^2 - 19y^2 = \pm 3 \tag{277}$$

Checking small numbers, we find $(3, \sqrt{19} \pm 1) = (4 \pm \sqrt{19})$. We see that P_2 is principal because we can observe that there is the ideal $(5 + \sqrt{19})$ for which

$$N(5 + \sqrt{19}) = 6 \tag{278}$$

and so $(5 + \sqrt{19}) = P_2 P_3$. To find the generator,we take

$$\frac{5 + \sqrt{19}}{4 - \sqrt{19}} = -(13 + 3\sqrt{19}) \tag{279}$$

and indeed, this has norm -2. Thus, $P_2 = (13 + 3\sqrt{19})$. We thus conclude that $\mathcal{O}_K$ has class number 1.

But now we observe that 2 is a ramified prime, and so in particular $P_2 = \sigma P_2$, thus $(13 + 3\sqrt{19}) = (13 - 3\sqrt{19})$. This implies that

$$\frac{13 + 3\sqrt{19}}{13 - 3\sqrt{19}} = 170 + 39\sqrt{19} \in \mathcal{O}_K^{\times} \tag{280}$$

This is thus a solution to $x^2 - 19y^2 = \pm 1$. But now, $\left(\frac{-1}{19}\right) = -1$. So, indeed this is a solution to $x^2 - 19y^2 = 1$.

We looked at this example because the result gives large numbers. In fact, this is the smallest solution to $x^2 - 19y^2 = 1$.

17.2

Proposition 212 (Lagrange). Let $d \in \mathbb{N}$, not a square (not necessarily square free), then $x^2 - dy^2 = 1$ has a nontrivial (i.e. $y \neq 0$) solution $(x, y) \in \mathbb{Z}^2$.

This is a special case of the following:

Proposition 213 (Dirichlet's Unit Theorem). For a real quadratic field K, there exists $\eta \in \mathcal{O}_K^\times$ such that every $\alpha \in \mathcal{O}_K^\times$ equals $\pm\eta^m$ for a unique integer m (i.e. $\mathcal{O}_K^\times = \{\pm 1\} \times \mathbb{Z}$).

PROOF 214. Recall that we had the embedding $\mathcal{O}_K \hookrightarrow \mathbb{R} \times \mathbb{R}$ with the map $\alpha \mapsto (\alpha, \sigma\alpha)$ for which we have

$$\text{Area}\,(\mathbb{R} \times \mathbb{R}/\mathcal{O}_K) = \sqrt{|D|} \tag{281}$$

Take $(x, y) \in \mathbb{R}^2$ such that $|xy| = 1$ for which diag(x, y) will preserve the area. Thus for the lattice $(x, y)\mathcal{O}_K \subseteq \mathbb{R}^2$, we have

$$\text{Area}\,(\mathbb{R} \times \mathbb{R}/(x, y)\mathcal{O}_K) = \sqrt{|D|} \tag{282}$$

Now consider the set

$$G(r) := \left\{(a, b) \in \mathbb{R}^2 : \frac{|a| + |b|}{2} < r\right\} \tag{283}$$

Then we have Area$G(r) > \sqrt{|D|}$ and we get $(u, v) \in (x, y)\mathcal{O}_K \cap G(r)$ nonzero, by the Minkowski lemma.

This shows that $8r^2 = 4\sqrt{|D|}$ which implies that there exists $(u, v) \in (x, y)\mathcal{O}_K$ nonzero such that

$$|uv| \leq \left(\frac{|u| + |v|}{2}\right)^2 \leq \frac{1}{2}\sqrt{|D|} \tag{284}$$

Now by definition, there exists $\alpha \in \mathcal{O}_K$ such that $(u, v) = (x\alpha, y\sigma\alpha)$. So we have $|uv| \leq \frac{1}{2}\sqrt{|D|}$ and $|xy| = 1$ which implies

$$|\alpha\sigma\alpha| \leq \frac{1}{2}\sqrt{|D|} \tag{285}$$

Now let $J_1, J_2, ..., J_m$ be the list of all ideals contained in $\mathcal{O}_K$ of norm at most $\frac{1}{2}\sqrt{|D|}$ where $(\alpha) = J_i$ for some i.

We then have

$$|uv| \leq \frac{|u| + |v|}{2} \leq \sqrt{\frac{1}{2}\sqrt{|D|}} \tag{286}$$

and so, taking the logarithm of both sides, and calling the log of RHS the constant C, we have

$$\log|x| + \log|\alpha| \leq C \tag{287}$$

Now taking $x = \left(n, \frac{1}{n}\right)$, we get $\alpha_n \in \mathcal{O}_K$. We then get $\left|N_{\mathbb{Q}}^K(\alpha_n)\right| \leq \frac{1}{2}\sqrt{|D|}$.

It follows that there is an infinite subset $S \subseteq \mathbb{N}$ such that (α_n) for all S are all equal to each other. In particular, we get $n_1 < n_2$ so that $\log|\alpha_{n_1}| > \log|\alpha_{n_2}|$ and $(\alpha_{n_1}) = (\alpha_{n_2})$. It follows that $\theta := \frac{\alpha_{n_1}}{\alpha_{n_2}} \in \mathcal{O}_K^\times$ and is not ± 1.

This gives the first part of theorem (the cyclic group part).

To finish the proof, it suffices to prove that the set of $\beta \in \mathcal{O}_K^\times$ totally positive is an infinite cyclic group. If we show this, then $[\mathcal{O}_K : \{\pm 1\} \times \{\gamma^m : m \in \mathbb{Z}\}] = 1, 2$.

In the case when the index is 1 not true, we have $\delta \in \mathcal{O}_K^\times$ so that $\delta^2 = \gamma^m$ for some m. If $m = 2m$, then $\delta = \pm\gamma^n$ which is bad. So, $m = 2n + 1$ in which case

$$\gamma = \left(\frac{\delta}{\gamma^n}\right)^2 \tag{288}$$

Taking $\epsilon := \frac{\delta}{\gamma^n}$ we have $\mathcal{O}_K^\times = \{\pm 1\} \times \{\epsilon^m : \ m \in \mathbb{Z}\}$.

In the second case, $\mathcal{O}_K$ is discrete in $\mathbb{R}^2$. Then the set $T := \mathcal{O}_K \cap M$ is discrete and is the set of totally positive units where

$$M := \left\{(x, y) \in \mathbb{R}^2 : x > 0, \ xy = 1\right\} \tag{289}$$

Now we have a bijection

$$M \to \mathbb{R} \tag{290}$$

$$(x, y) \mapsto \log x \tag{291}$$

Follows $\{\log \alpha : \alpha \in T\} \hookrightarrow \mathbb{R}$ is a discrete subgroup. We can then show that if $Z \subseteq \mathbb{R}$ is a discrete subgroup and $Z = \mathbb{Z}h$. We can show that $h = \min\{|z| : z \in Z, \ z \neq 0\}$.

□

18 . - -Monday, 5.13.2019

We will talk about general number fields for the next few lectures. Let K be a number field of degree n, and let $\mathcal{O}_K$ be the ring of integers in K (i.e. the integral closure of $\mathbb{Z}$ in K):

$$\mathcal{O}_K := \left\{\alpha \in K : (\exists a_i \in \mathbb{Z})(\alpha^r + a_{r-1}\alpha^{r-1} + ... + a_0 = 0)\right\} \tag{292}$$

This is a subring of K (as we showed before). Furthermore, $w_1, ..., w_n \in K$ such that $\mathcal{O}_K = \mathbb{Z}w_1 + ... + \mathbb{Z}w_n$. Then $w_1, ..., w_n$ is a $\mathbb{Q}$-basis for K. All of this is a review from Billy's lecture.

Furthermore, there exists $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$, and let $F \in \mathbb{Q}[X]$ be a monic polynomial with $f(\alpha) = 0$. Now consider the evaluation homomorphism $\varphi : \mathbb{Q}[X] \to K$ given by $X \mapsto \alpha$, then

$$\mathbb{Q}[X]/(f) \cong K \tag{293}$$

Let's now consider polynomials with complex coefficients $f \in \mathbb{C}[X]$. Then we can write it as

$$f(x) = \prod_{i=1}^{r_1} h_i(x) \prod_{j=1}^{r_2} g_j(x) \tag{294}$$

where $h_i(x) = x - \alpha_i, \ \alpha_i \in \mathbb{R}$, $g_j(x) = (x - \beta_j)(x - \overline{\beta}_j), \ \beta_j \in \mathbb{C} \setminus \mathbb{R}$ with $\alpha_1, ..., \alpha_{r_1}, \beta_1, ..., \beta_{r_2} \in \mathbb{C}$ distinct. We then have $\deg f = r_1 + 2r_2$.

We then see by CRT that

$$\mathcal{O}_K \hookrightarrow K \cong \mathbb{Q}[X]/(f) \hookrightarrow \mathbb{R}[X]/(f) \cong \prod_{i=1}^{r_1} \mathbb{R}[X]/(X - \alpha_i) \times \prod_{j=1}^{r_2} \mathbb{R}[X]/(g_j(X)) = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \tag{295}$$

Thus we get the following inclusion of embeddings:

$$\begin{tikzcd}
\mathcal{O}_K \arrow[r, "\subseteq"] & K \arrow[r, "\subseteq"] \arrow[d, "\sigma_i"] & \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \arrow[d] \\
& \mathbb{R} & \mathbb{R}^{r_1} \arrow[l, "p_i"]
\end{tikzcd}
\qquad
\begin{tikzcd}
K \arrow[r, "\subseteq"] \arrow[d, "\tau_j"] & \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \arrow[d] \\
\mathbb{R} & \mathbb{C}^{r_2} \arrow[l, "q_j"]
\end{tikzcd}$$

where we let $\sigma_i : K \to \mathbb{R}, i = 1, ..., r_1$ and $\tau_j : K \to \mathbb{C},\ j = 1, ..., r_2$ be the canonical projections.

Now to compute the volume of subsets of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, we take the standard $\mathbb{R}$-basis $w_1, ..., w_n$ of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$:

$$(1, 0, ..., 0), ..., (\underbrace{0, 0, ..., 0}_{r_{,}1 \text{ times}} 1, 0, ..., 0),\ ...,\ (0, 0, ..., 0, 1) \tag{296}$$

where the first r_1 is a basis of $\mathbb{R}^{r_1}$.

Now using this, we compute Vol($\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}/I$) where $I \subseteq \mathcal{O}_K$ is an ideal. We begin with $K = \mathbb{Q}[X]/(f)$. Let $w_1, ..., w_n$ be any $\mathbb{Q}$-basis for K, then consider $\text{Tr}_{\mathbb{Q}}^{K}(w_i w_j) = X$. Note that $w_1, ..., w_n$ is also a $\mathbb{R}$-basis for $\mathbb{R}[X]/(f)$, and we get a change of basis matrix $T = (t_{ij}) \in GL_n(\mathbb{R})$ with

$$w_i = \sum_{j=1}^{n} t_{i,j} w'_j \tag{297}$$

We recall that for this ,

$$\text{Vol}(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}/\mathbb{Z}w_1 + ... + \mathbb{Z}w_n) = |\det T| \tag{298}$$

Now if we denote $M := \mathbb{R}[X]/(f)$, then we can take $X' = \text{Tr}_{\mathbb{R}}^{M}(w'_p w'_q)$ with

$$w_i = \sum_{p=1}^{n} t_{ip} w'_p,\ w_j = \sum_q t_{iq} w'_q \tag{299}$$

thus

$$w_i w_j = \sum_{p,q} t_{ip} t_{jq} w'_p w'_q \qquad t_{ip}, t_{jq} \in \mathbb{R} \tag{300}$$

and so,

$$\text{Tr}_{\mathbb{Q}}^{K}(w_i w_j) = \text{Tr}_{\mathbb{R}}^{\mathbb{R}[X]/(f)}\left(w'_p w'_q\right) = \sum_{p,q} t_{i,p} t_{j,q} \text{Tr}_{\mathbb{R}}^{M}(w'_p w'_q) \tag{301}$$

We then have $X = TX'^{t}T$, so

$$\det X = (\det T)^2 \det(X') \tag{302}$$

Now if we look at the 2×2 blocks on the diagonal, we have

$$w'_i w'_j = \begin{cases} 0 & i \neq j \\ w'_i & i = j \end{cases} \tag{303}$$

fro which we see that the $\det X' = (-4)^{r_2}$, and so $\det X = (-4)^{r_2}\text{Vol}(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}/\sum_i \mathbb{Z}w_i)$.

Here is the result of this computation:

Proposition 215. If $w_1, ..., w_n$ is any $\mathbb{Q}$-basis of K, then

$$\det \text{Tr}_{\mathbb{Q}}^{K}(w_i w_j) = \text{Vol}\left(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}/\sum_i \mathbb{Z}w_i\right)^2 \cdot (-4)^{r_2} \tag{304}$$

Definition 216. Let $w_1, ..., w_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$. Then the **discriminant of the field** K is

$$D := \det\left(\text{Tr}_{\mathbb{Q}}^K(w_i w_j)\right) \qquad \text{Tr}_{\mathbb{Q}}^K(w_i w_j) \in M_n(\mathbb{Z}) \tag{305}$$

Remark 217. The lemma can be restated as just

$$\text{Vol}\left(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}/\mathcal{O}_K\right) = 2^{-r_2}\sqrt{|D|} \tag{306}$$

Then

$$\text{Vol}\left(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}/\mathcal{O}_K\alpha\right) = 2^{-r_2}\sqrt{|D|}\,|\det(\ell_\alpha)| = 2^{-r_2}\sqrt{|D|}\left|N_{\mathbb{Q}}^K(\alpha)\right| \tag{307}$$

where ℓ_α is the multiplication by α matrix.

Now work with $r_2 = 0$. Take $I \subseteq \mathcal{O}_K$ and minimize $\left|N_{\mathbb{Q}}^K(\alpha)\right|$ for a $\alpha \in I$ nonzero. Now

$$N(\alpha) = \prod_{i=1}^n \sigma_i \alpha \tag{308}$$

and by AMGM inequality,

$$|x_1 ... x_n| \leq \left(\frac{|x_1| + ... + |x_n|}{n}\right)^n \tag{309}$$

for $x_i \in \mathbb{R}$. Now for

$$G(r) := \left\{(x_1, ..., x_n) \in \mathbb{R}^n : \frac{\sum_i |x_i|}{n} < r\right\} = rG(1) \tag{310}$$

Then

$$\begin{aligned}\text{Vol}G(r) &= r^n \text{Vol}G(1) \\ &= 2^n r^n \text{Vol}(G(1) \cap [0, \infty)^n \\ &= \frac{2^n r^n n^n}{n!}\end{aligned}$$

19 . - -Wednesday, 5.15.2019

Let r_1, r_2 respectively be the number of embeddings of K into $\mathbb{R}, \mathbb{C}$. Then $n := \deg(K/\mathbb{Q}) = r_1 + 2r_2$. We assume $r_2 = 0$, so $r_1 = n$. We also recall that

$$\text{Vol}(\mathbb{R}^n/\mathcal{O}_K) = \sqrt{|D|} \tag{311}$$

For $r > 0$, let

$$G(r) := \left\{x \in \mathbb{R}^n : \frac{\sum_{i=1}^n |x_i|}{n} < r\right\} \tag{312}$$

and the volume of this is $2^n r^n \cdot \frac{n^n}{n!}$ where 2^n is the number of tetrahedra.

Now let $I \subseteq \mathcal{O}_K$ nonzero, then $[\mathcal{O}_K : I] < \infty$ and

$$\text{Vol}(\mathbb{R}^n/I) = \text{Vol}(\mathbb{R}^n/\mathcal{O}_K)[\mathcal{O}_K : I] = \sqrt{|D|}[\mathcal{O}_K : I] \tag{313}$$

Minkowski says that if $\text{Vol}G(r) > 2^n \text{Vol}(\mathbb{R}^n/I)$, then there exists $\gamma \in I \cap G(r)$ nonzero.

Proposition 218. If Vol$G(r) = 2^n$Vol$(\mathbb{R}^n/I)$, then there exists $\gamma \in G(r) \cap I$ nonzero.

PROOF 219. From the expression of $G(r)$, we have

$$\text{Vol}G\left(r + \frac{1}{k}\right) > \text{Vol}(\mathbb{R}^n/I) \tag{314}$$

and so, by Minkowski there exists $\gamma_k \in I \cap G\left(r + \frac{1}{k}\right)$ nonzero and $\gamma_1, \gamma_2, ...$ is a bounded sequence.

Then there exists a convergent subsequence, but I is a discrete set, so the convergent sequence is eventually constant, i.e. $\gamma_{k_1}, \gamma_{k_2}$,... . Thus,

$$\frac{\sum_{i=1}^n |\sigma_i \gamma|}{n} < r + \frac{1}{k_j} \tag{315}$$

for all j. This proves the claim.

□

Proposition 220. There exists $\gamma \in I$ nonzero such that

$$\left|N_{\mathbb{Q}}^K(\gamma)\right| \leq \left(\frac{\sum_{i=1}^n |\sigma_i \gamma|}{n}\right)^n \leq \sqrt{|D|}[\mathcal{O}_K : I]\frac{n!}{n^n} \tag{316}$$

PROOF 221. If $\gamma \in I$, then $\mathcal{O}_K\gamma \subseteq I$ and

$$\begin{aligned}[I : \mathcal{O}_K\gamma] &= [\mathcal{O}_K : \mathcal{O}_K\gamma]/[\mathcal{O}_K : I] \\ &= \left|N_{\mathbb{Q}}^K(\gamma)\right|/[\mathcal{O}_K : I] \leq \sqrt{|D|}\frac{n!}{n^n}\end{aligned}$$

Also for $K \supseteq \mathcal{O}_K \supseteq \mathcal{O}_K\gamma$, we have a bijection from K to itself given by $c \mapsto c\gamma^{-1}$, and so

$$[I : \mathcal{O}_K\gamma] = [\gamma^{-1}I : \mathcal{O}_K] \leq \sqrt{|D|}\frac{n!}{n^n} \tag{317}$$

□

Remark 222. Recall the requirements for unique prime factorization of ideals in $\mathcal{O}_K$. Note that unique factorization was not part of the definition of Dedekind domains but rather a consequence.

1.) If $\gamma \in \mathcal{O}_K$ nonzero, then $[\mathcal{O}_K : \mathcal{O}_K\gamma] < \infty$.
2.) If I is a fractional ideal of $\mathcal{O}_K$ and $P \subseteq \mathcal{O}_K$ nonzero, is a prime ideal, then $PI \subsetneq I$
3.) For all nonzero prime ideals $P \subseteq \mathcal{O}_K$, there exists fractional ideals P^{-1} such that $P^{-1}P = \mathcal{O}_K$.
We will check these.

Remark 223. We already know that $[\mathcal{O}_K : \mathcal{O}_K\gamma] = \left|N_{\mathbb{Q}}^K\right|$.

More elementarily, $\gamma \in \mathcal{O}_K$ implies that γ is integral over $\mathbb{Z}$. So in particular, the minimal polynomial of γ lies in $\mathbb{Z}[X]$.

Let a_r be the nonzero constant term of this minimal polynomial. Then $a_r \in \mathcal{O}_K\gamma$. To show that $\mathcal{O}_K/\mathcal{O}_K\gamma$ is finite, suffices to show that

$$\mathcal{O}_K/a_r\mathcal{O}_K \cong (\mathbb{Z}/|r|)^n \tag{318}$$

is finite.

Proposition 224 (Nakayama's Lemma). Let R be a commutative ring and M a f.g. R-module so that $IM = M$ for any ideal $I \subseteq R$. Then there is $\alpha \in I$ such that

$$(1-\alpha)M = 0 \tag{319}$$

PROOF 225 (Nakayama's lemma implies the condition 2 in Remark 222). Now let M nonzero be a $\mathcal{O}_K$ fractional ideal. Let $P \subseteq \mathcal{O}_K$ is a nonzero prime idea. Assume $PM = M$. Nakayama says there exists $\alpha \in P$ so that $(1-\alpha)M = 0$.

But if $v \in M$ nonzero, then $(1-\alpha)v = 0$ implies that $1 - \alpha = 0$, so $\alpha = 1 \in P$. Then $\mathcal{O}_K = P$ which contradicts the definition of a prime ideal.

□

Remark 226. Let $I(\mathcal{O}_K)$ is the collection of nonzero $\mathcal{O}_K$-fractional ideals lying inside K.

THen $I(\mathcal{O}_K)$ is an associative, commutative monoid, where for $M, N \in I(\mathcal{O}_K)$, we have

$$MN = NM \in I(\mathcal{O}_K),\ M\mathcal{O}_K = M,\ (\mathcal{O}_K\alpha)(\mathcal{O}_K\alpha^{-1}) = \mathcal{O}_K \tag{320}$$

We then have condition 3 in Remark 222: for all nonzero prime ideal $P \subseteq \mathcal{O}_K$, there exists prime ideal P^{-1} such that $PP^{-1} = \mathcal{O}_K$.

Definition 227. Let $M_1 \sim M_2$ in $I(\mathcal{O}_K)$ iff there is $\alpha \in K$ so that $M_2 = \alpha M_1$. Then $C(\mathcal{O}_K)$ is the set of equivalence classes of $I(\mathcal{O}_K)$ modulo these equivalence classes.

Proposition 228. $C(\mathcal{O}_K)$ is a finite set.

PROOF 229. Let $M \in I(\mathcal{O}_K)$. Then there exists $\alpha \in \mathcal{O}_K$ nonzero such that $I = \alpha M \subseteq \mathcal{O}_K$ (so $M \sim I$).

We have $\gamma \in I$ nonzero such that $H = \gamma^{-1}I \supseteq \mathcal{O}_K$. Thus every fractional ideal $M \sim H$ where $H \supseteq \mathcal{O}_K$ and $[H : \mathcal{O}_K] \leq C = \sqrt{|D|}\frac{n!}{n^n}$.

Let $r \in \{1, 2, ..., [C]\}$. If $[H : \mathcal{O}_K] = r$, then $|H/\mathcal{O}_K| = r$, and so multiplying any elemnent of $H/\mathcal{O}_K$ gives 0 so $rH \subseteq \mathcal{O}_K$, thus $H \subseteq r^{-1}\mathcal{O}_K$.

Thus $\mathcal{O}_K \subseteq H \subseteq \frac{1}{r}\mathcal{O}_K$. Clearly there exists finitely many such H

□

PROOF 230 (Condition 3 in Remark 222.). Let $M \in I(\mathcal{O}_K)$. Consider $M^0 = \mathcal{O}_K, M, M^2, ...$ By claim, there exists $m < n$ such that $M^m \sim M^n$ i.e $M^m = (\alpha M^{n-m})M^m$.

Now the key observations are that:

1.) $\alpha M^{n-m} \subseteq \mathcal{O}_K$. If $hM^m \subseteq M^m$, then $h \in \mathcal{O}_K$

2.) If $\alpha M^{n-m} \neq \mathcal{O}_K$, then $\alpha M^{n-m} \subseteq P \subseteq Q$ for a prime ideal P. So $hM^m = \mathcal{O}_K$. This contradicts condition 2.

□

20 . - -Friday, 5.17.2019

Recall:

Proposition 231. For a number field K, for a nonzero fractional ideal $M \subseteq K$, if $\alpha \in K$ has the property that $\alpha M \subseteq M$, then $\alpha \in \mathcal{O}_K$.

PROOF 232. We know that any subgroup of

$$M := \mathbb{Z}\omega_1 + ... + \mathbb{Z}\omega_n \tag{321}$$

is finitely generated. Take $v \in M$ nonzero, and let

$$N := \mathbb{Z}v + \mathbb{Z}\alpha v + \mathbb{Z}\alpha^2 v + ... \subseteq M \tag{322}$$

But N is finitely generated, so there is $m \in \mathbb{N}$ so that

$$N = \mathbb{Z}v + \mathbb{Z}\alpha v + ... + \mathbb{Z}\alpha^m v \tag{323}$$

So, there are $a_i \in \mathbb{Z}$ so that

$$\alpha^{m+1} v = a_1 \alpha^m v + a_2 \alpha^{m-1} v + ... + a_{m+1} v \tag{324}$$

$$\alpha^{m+1} - (a_1 \alpha^m + ... + a_{m+1}) = 0 \tag{325}$$

□

Proposition 233. Every fractional ideal of $\mathcal{O}_K$ has an inverse.

PROOF 234. We've shown that $C(\mathcal{O}_K)$ is a finite set. Let $M \in I(\mathcal{O}_K)$. Then

$$\mathcal{O}_K = M^0, M^1, ... \in I(\mathcal{O}_K) \tag{326}$$

Now $C(\mathcal{O}_K)$ is finite, so there exists $0 \leq m < n$ so that $M^m \sim M^n$, i.e. there exists $\alpha \in K$ so that $M^m = \alpha M^n = (\alpha M^{n-m}) M^m$.

We claim that $\alpha M^{n-m} = \mathcal{O}_K$. Let $\beta \in \alpha M^{n-m}$. Then $\beta M^m \subseteq M^m$. By the previous proposition, $\beta \in \mathcal{O}_K$. Thus, $\alpha M^{n-m} = I \subseteq \mathcal{O}_K$if $I \neq \mathcal{O}_K$, then $IM^m = M^m$ contradicts Nakayama's lemma. This proves the claim.

Now

$$\mathcal{O}_K = \alpha M^{n-m} = M \cdot \alpha M^{n-m-1} \tag{327}$$

and $n - m - 1 \geq 0$, Thus, M has an inverse, it is αM^{n-m-1}.

□

Remark 235. This avoids Dedekind domain proof. Number theory gives it to us for free.

Proposition 236. M is a f.g. R-module, R is a commutative ring, and $IM = M$ where $I \subseteq R$ is an ideal. Then there exists $\alpha \in I$ such that $(1 - \alpha)M = 0$.

PROOF 237. Let $e_1, ..., e_n$ be generators of M as R-module with $e_i \in M = IM$ so that there are α_{ij} so that

$$e_i = \sum_{j=1}^{n} \alpha_{i,j} e_j \tag{328}$$

Let $T \in M_n(R)$ with

$$(T)_{ij} = \begin{cases} -\alpha_{ij} & i \neq j \\ 1 - \alpha_{ij} & i = j \end{cases} \tag{329}$$

So,

$$\text{adj}(T)T \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = (\det T)\mathbf{Id} \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \tag{330}$$

We conclude that $\det T e_i = 0$ for all i. Thus,

$$\det T \sum_i h_i e_i = 0 \tag{331}$$

for all $h_i \in R$. Thus, $\det(T)v = 0$ for all $v \in M$.

Now

$$\det T \equiv \prod_{i=1}^{n} (1 - \alpha_{ii}) \qquad \mod I \tag{332}$$

which iplies

$$(1 - \alpha_{11}) ... (1 - \alpha_{nn}) = 1 - \alpha' \tag{333}$$

for $\alpha' \in I$.

□

We also have the following:

1.) Unique factorization holds for fractional ideals, i.e. every fractional ideal of $\mathcal{O}_K$ equals $p_1^{m_1} ... p_r^{m_r}$ where $m_i \in \mathbb{Z}$ and $p_1, ..., p_r$ are distinct nonzero prime ideals of $\mathcal{O}_K$ and the expression is unique.
2.) $I \subseteq \mathcal{O}_K$ nonzero, then $[\mathcal{O}_K : I] < \infty$ and denoted by $N(I)$.

Furthermore, we have $N(IJ) = N(I)N(J)$ for ideals $I, J \subseteq \mathcal{O}_K$.

When $n = r_1$ (so $r_2 = 0$), we've shown that for all $I \subseteq \mathcal{O}_K$, $I \sim J,\ J \subseteq \mathcal{O}_K$ and $1 \leq N(J) \leq \sqrt{|D|} \frac{n^n}{n!}$.

It follows that

Proposition 238.

$$\sqrt{|D|} \geq \frac{n^n}{n!} > 1 \tag{334}$$

if $n > 1$.

We recall from calculus that

$$\lim_{n \to \infty} \frac{n^n / n!}{e^n} = 1 \tag{335}$$

so the ratio goes to infinity quite fast.

Proposition 239. If $n = \deg(K/Q) > 1$, then $|D| > 1$ (even if $r_2 > 0$).

Definition 240. Let K be a number field. The **ramification index of P_i over the prime** p is the number e_i so that

$$(p) = P_1^{e_1}...P_r^{e_r} \tag{336}$$

Remark 241. p is ramified if

$$\max(e_1, ..., e_r) > 1 \tag{337}$$

We let

$$k(P_i) := \mathcal{O}_K/P_i,\ f_i := \deg(K(P_i)/\mathbb{F}_p) \tag{338}$$

Proposition 242.

$$\deg(K/\mathbb{Q}) = \sum_{i=1}^{r} e_i f_i \tag{339}$$

PROOF 243. $k(P_i)$ is a $\mathbb{F}_p$-vector space of dimension f_i, so $|k(P_i)| = p^{f_i}$, i.e. $N(P_i) = p^{f_i}$.

$\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n = \deg(K/\mathbb{Q})$. $\mathcal{O}_K/\mathcal{O}_K p$ is a $\mathbb{F}_p$-vector space of dimension n, so has p^n elements so

$$N(\mathcal{O}_K p) = p^n = \prod_i N(P_i)^{e_i} = p^{\sum_i e_i f_i} \tag{340}$$

Thus, $n = \sum_i e_i f_i$.

□

Proposition 244. A prime p is ramified in K iff $p|D$.

PROOF 245. Let

$$\mathcal{O}_K = \mathbb{Z}\omega_1 + ...\mathbb{Z}\omega_n \tag{341}$$

with

$$D = \det(\text{Tr}_{\mathbb{Q}}^{K}(\omega_i\omega_j)) \tag{342}$$

Then

$$\mathcal{O}_K/p\mathcal{O}_K = \mathbb{Z}\overline{\omega}_1 + ... + \mathbb{Z}\overline{\omega}_n \tag{343}$$

with the $\overline{\omega}_i$ form a $\mathbb{F}_p$-basis for $\mathcal{O}_K/p\mathcal{O}_K$.

Now if $\alpha \in \mathcal{O}_K$,

$$\overline{\text{Tr}_{\mathbb{Q}}^{K}(\alpha)} = \text{Tr}_{\mathbb{F}_p}^{\mathcal{O}_K/p\mathcal{O}_K}(\overline{\alpha}) \tag{344}$$

with $\overline{\alpha} \in \mathcal{O}_K/p\mathcal{O}_K$. Here, $\bar{\cdot}$ of an integer is just reduction mod p.

Thus, $p|D$ iff

$$\det \text{Tr}_{\mathbb{F}_p}^{\mathcal{O}_K/p\mathcal{O}_K}(\overline{\omega}_i\overline{\omega}_j) = 0 \tag{345}$$

independent of choice of basis. Now

$$p\mathcal{O}_K = \prod_{i=1}^{r} P_i^{e_i} \tag{346}$$

and

$$\prod_{i=1}^{r} \mathcal{O}_K / p_i^{e_i} = R_1 \times ... \times R_r \tag{347}$$

Now $D_i \in \mathbb{F}_p$ is $\det \mathrm{Tr}_{\mathbb{F}_p}^{R_2}(\beta_k \beta_l)$ where the $\beta_1, ..., \beta_m$ form $\mathbb{F}_p$-basis for R_i.

□

21 . - -Monday, 5.20.2019

Recall:

Proposition 246. Let $D := \mathrm{Disc}(K)$, with $|D| > 1$ if $\deg(K/\mathbb{Q}) = n > 1$. Then

$$|D| \geq \frac{n^n}{n!} \tag{348}$$

when K is totally real.

We also had the factorization

$$\mathcal{O}_K p = \prod_{i=1}^{r} P_i^{e_i} \tag{349}$$

with $p \nmid D$ iff $e_i = 1$ for each i.

Now letting $R_i := \mathcal{O}_K / P_i^{e_i}$ with

$$\mathrm{Disc}(R_i) = \det \mathrm{Tr}_{\mathbb{F}_p}^{R_i}(\alpha_m \alpha_n) \tag{350}$$

where α_i are the $\mathbb{F}_p$-basis of R_i.

We've shown that $p \nmid D$ iff $\mathrm{Disc}(R_i) \neq 0$ in $\mathbb{F}_p$ for all i.

Now we have a map $B_i : \mathbb{R}_i^2 \to \mathbb{F}_p$ given by

$$B_i(x, y) := \mathrm{Tr}_{\mathbb{F}_p}^{R_i}(xy) \tag{351}$$

Then $D_i := \mathrm{Disc}(R_i) \neq 0$ iff B_i is a nondegenerate bilinear form on R_i, i.e. for all $v \in R_i$ nonzero, there exists $w \in R_i$ such that $B_i(v, w) \neq 0$.

We claim that if $e_i > 0$, then for all $v \in P_i / P_i^{e_i} \subseteq \mathcal{O}_K / P_i^{e_i} = R_i$, we get $\mathrm{Tr}_{\mathbb{F}_p}^{R_i}(v) = 0$.

If we let $M_j := P_i^j / P_i^{e_i}$, then we have

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq ... \supseteq M_{e_{i-1}} \supseteq M_{e_i} = 0 \tag{352}$$

Now $vM_r \subseteq M_{r+1}$, and if we write the multiplication by v matrix, then we get a lower triangular matrix which in particular has 0's down the diagonal.

Thus, for all $v \in P_i / P_i^{e_i}$, $v \in R_i$, we have $vw \in P_i / P_i^{e_i}$, then

$$B_i(v, w) = \mathrm{Tr}_{\mathbb{F}_p}^{R_i}(vw) = 0 \tag{353}$$

So, $\text{Disc}(R_i) = 0$. Thus, B_i is not nondegenerate. It remains to show that $\text{Tr}_{\mathbb{F}_p}^{\mathcal{O}_K/P_i} = B(x, y)$ is nondegenerate.

Proposition 247. E is a finite field extension of F. Then 1.) E is a separable extension of F iff 2.) there is $v \in E$ such that $\text{Tr}_F^E(v) \neq 0$ iff 3.) $(v, w) \mapsto \text{Tr}_F^E(vw)$ is a nondegenerate F-bilinear form on E.

PROOF 248 (2 $\implies$ 3). This is one line. If there is $v_0 \in E$ with the above property, then taking $v \in E$ nonEro, we have

$$\text{Tr}_F^E\left(v \cdot \frac{v_0}{v}\right) = \text{Tr}_F^E(v_0) \neq 0 \tag{354}$$

□

Proposition 249. For $E = F(\alpha)$, $f = m_{\alpha,F} \in F[x], \deg f = n$, then

$$\text{Tr}_F^E\left(\frac{\alpha^{n-1}}{f'(\alpha)}\right) = 1 \tag{355}$$

Remark 250. Recall: if

$$(p) = \prod_i p_i^{e_i} \tag{356}$$

p is unramified of p is not ramified. We define that p is split iff

$$(p) = \prod_i p_i \tag{357}$$

with $\mathbb{F}_p \overset{\cong}{\to} \mathcal{O}_K/P_i$ for all i, i.e. $N(P_i) = p$.

In Billy's lecture, we introduced ring of integers for general field extensions, but we noted that in general, they are hard to compute. We need to resolve this issue without introducing too much general theory.

Remark 251. Let K be a number field of degree n. Suppose $w_1, ..., w_n$ is a $\mathbb{Q}$-basis for K, and assume $R = \mathbb{Z}w_1 + ... + \mathbb{Z}w_n \subseteq K$ is a subring. Then $R \subseteq \mathcal{O}_K$. Let $N := [\mathcal{O}_K : R]$. Then the natural map

$$R/pR \to \mathcal{O}_K/p\mathcal{O}_K \tag{358}$$

is an isomorphism for all primes $p \nmid N$.
Now define $j : \mathcal{O}_K \to K$ by $j(z) = Nz$, then

$$R \xrightarrow{i} \mathcal{O}_K \xrightarrow{j} R \tag{359}$$

for which $j \circ i$ is multiplication bu N. This induces the maps

$$R/pR \xrightarrow{\bar{i}} \mathcal{O}_K/p\mathcal{O}_K \xrightarrow{\bar{j}} R/pR \tag{360}$$

and again, $\bar{j} \circ \bar{i}$ is multiplication by N and is an isomorphism.

Both rings have p^n elements, and $\bar{j} \circ \bar{i}$ is 1-1, so $\bar{i}$ is a bijection.

Now observe that p is unramified iff $e_i = 1$ for all i iff $\mathcal{O}_K/p\mathcal{O}_K \cong \prod_i \mathcal{O}_K/p_i^{e_i}$ is a product of fields.

Example 252. For $K = \mathbb{Q}(2^{1/3})$, we take $p \equiv 2, 3$. Then $m_\alpha = x^3 - 2$, and

$$R = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 \cong \mathbb{Z}[x]/(x^3 - 2) \tag{361}$$

and so,

$$R/pR \cong \mathbb{F}_p[x]/(x^3 - 2) \tag{362}$$

Now for $p \equiv 1 \mod 3$ (for which we have $\omega \in \mathbb{F}_p,\ \omega \neq 1$ and $\omega^3 = 1$), we have two cases: for p split, there is at least one root, so $x^3 - 2$ is a product of linear factors, and so $(p) = P_1 P_2 P_3$ where $N(P_i) = p$ for $i = 1, 2, 3$. In the second case, $p)$ is prime for which the norm is p^3.

Now for $p \equiv 2 \mod 3$, since the map $x \mapsto x^3$ is an isomorphism, there is a cube root of 2. Thus, we can write

$$x^3 - 2 = (x - c)q(x) \in \mathbb{F}_p[x] \tag{363}$$

But now, $2 = c^3$, so

$$x^3 - 2 = x^3 - c^3 = (x - c)(x^2 + cx + c^2) \tag{364}$$

and so,

$$q(x) = x^2 + cx + c^2 = c^2\left(\left(\frac{x}{c}\right)^2 + \left(\frac{x}{c}\right) + 1\right) \tag{365}$$

which is irreducible since $x^2 + x + 1$ is irreducible. Thus, $p\mathcal{O}_K = P_1 P_2$ with $N(P_1) = p,\ N(P_2) = p^2$.

Thus, there is there different types of behavior if we ignored the ramified primes, and we could do all of this without finding $\mathcal{O}_K$.

Remark 253. Recall: for $R \subseteq \mathcal{O}_K \subseteq R^\perp$ where

$$R^\perp = \left\{\alpha \in K : \mathrm{Tr}_{\mathbb{Q}}^K(\alpha R) \subseteq \mathbb{Z}\right\} \tag{366}$$

and for $R \subseteq \mathcal{O}_K \subseteq \mathcal{O}_K^\perp \subseteq R^\perp$ where

$$\mathcal{O}_K^\perp = \left\{\alpha \in K : \mathrm{Tr}_{\mathbb{Q}}^K(\alpha \mathcal{O}_K) \subseteq \mathbb{Z}\right\} \tag{367}$$

Then $|\mathrm{Disc}(K)| = [\mathcal{O}_K^\perp : \mathcal{O}_K]$ and $N_{\mathbb{Q}}^K f'(\alpha) = [R_K^\perp : R_K] = \mathrm{Disc}(K)[\mathcal{O}_K : R]^2$.

See Lagrange interpolation on Wikipedia for all of this.

22 . - -Wednesday, 5.22.2019

Announcement. Billy's office hours: today at 5pm-6pm.

Recall:

Proposition 254 (Dirichlet's Unit Theorem). K is a number field of degree n where $n = r_1 + 2r_2$ for r_1 the number of real embeddings of K and r_2 the complex ones. $\mathcal{O}_K$ is the ring of algebraic integers in K. Then

$$\mathcal{O}_K^\times \cong \mathbb{Z}^{r_1 + r_2 - 1} \times \mu(K) \tag{368}$$

where

$$\mu(K) = \left\{\alpha \in K : (\exists n \in \mathbb{N})(\alpha^N = 1)\right\} \tag{369}$$

is a finite cyclic group.

Example 255. For $n = 1$, we have $\mathcal{O}_K^\times = \{\pm 1\}$

Example 256. For $n = 2$, we have $r_2 = 1$ which gives an imaginary quadratic extension, and so, $\mathcal{O}_K = \{\pm 1\}$ are roots of unity in K except in $\mathbb{Q}[\sqrt{-1}],\ \mathbb{Q}[\sqrt{-3}]$.

For $r_1 = 2$, we have the real quadratic field for which $\mathcal{O}_K \cong \{\pm 1\} \times \mathbb{Z}$.

22.1 Lagrange Interpolation Theorem.

Proposition 257 (Lagrange Interpolation). Let F be a field and $a_1, ..., a_n \in F$ are all distinct. For $b_1, ..., b_n \in F$ arbitrary, then there exists unique $g \in F[x]$ with degree $< n$ so that $g(a_i) = b_i$ for each i.

PROOF 258. (*Uniqueness.*) If $g_1(a_i) = g_2(a_i) = b_i$ for each i, then $g_1 - g_2$ has roots $a_1, ..., a_n$ but its degree is $< n$. Thus, $g_1 - g_2 = 0$.

(*Existence.*) Take

$$f_1(x) = \frac{(x_1 - a_2)...(x_n - a_n)}{(a_1 - a_2)...(a_1 - a_n)} \tag{370}$$

then $f_1(a_1) = 1,\ f_1(a_i) = 0,\ i \neq 1$. We can construct f_i with degree $n - 1$ for each $i = 1, ..., n$ for which $f_i(a_j) = \delta_{i,j}$,

$$g = \sum_{i=1}^{m} b_i f(x) \tag{371}$$

$$g(a_j) = b_j f_j(a_j) = b_j \tag{372}$$

□

Check this part.

Observe: Let $h \in F[x]$ have degree $< n$ and let $b_i = h(a_i)$ for each $i = 1, ..., n$. Then by uniqueness, we have $g = h$ from Lagrange's theorem. In particular, we can take $h(x) = x^m$ for $0 \leq m \leq n - 2$.

Remark 259. If

$$f(x) = (x - a_1)...(x - a_n) \tag{373}$$

$$f'(x) = (x - a_2)...(x - a_n) + (x - a_1)(x - a_3)...(x - a_n) + ... + (x - a_1)(x - a_2)...(x - a_{n-1}) \tag{374}$$

Let

$$g_i(x) = \frac{f(x)}{x - a_i} \in F[x] \tag{375}$$

which is monic and degree $n - 1$. The g in Lagrange's formula equals

$$\sum_{i=1}^{n} b_i \frac{g_i(x)}{f'(a_i)} \tag{376}$$

We can then continue with our observation. If $h(x) = x^m,\ 0 \leq m \leq n-1$, then

$$x^m = \sum_{i=1}^{n} a_i^m \frac{g_i(x)}{f'(a_i)} \tag{377}$$

with the coefficient of x^{n-1} being $\sum_{i=1}^{n} \frac{a_i^m}{f'(a_i)}$.

It follows that:

Proposition 260.

$$\sum_{i=0}^{n} \frac{a_i^m}{f'(a_i)} = \begin{cases} 0 & m = 0, 1, ...n-2 \\ 1 & m = n-1 \end{cases} \tag{378}$$

where $f(x) = \prod_{i=1}^{n}(x - a_i)$.

Another corollary:

Proposition 261. Let $K = \mathbb{Q}[\theta]$ be a number field of degree n. Let $f \in \mathbb{Q}[x]$ be a unique monic polynomial with $f(\theta) = 0$. Then

$$\text{Tr}_{\mathbb{Q}}^{K}\left(\frac{\theta^m}{f'(\theta)}\right) = \begin{cases} 0 & m = 0, ..., n-2 \\ 1 & m = n-1 \end{cases} \tag{379}$$

PROOF 262. If $\sigma_1, ..., \sigma_n$ are the distinct embeddings of K in $\mathbb{C}$, then for all $\alpha \in K$,

$$\text{Tr}_{\mathbb{Q}}^{K}(\alpha) = \sum_{i=1}^{n} \sigma_i \alpha \tag{380}$$

Now take $F = \mathbb{C}$, then

$$f(x) = \prod_{i=1}^{n}(x - \sigma_i \theta) \tag{381}$$

Letting $a_i = \sigma_i \theta$ in the previous proposition, then we can put $\alpha = \frac{\alpha}{f'(\theta)}$, and we get

$$\text{Tr}_{\mathbb{Q}}^{K}\left(\frac{\theta^m}{f'(\theta)}\right) = \begin{cases} 0 & m = 0, ..., n-2 \\ 1 & m = n-1 \end{cases} \tag{382}$$

as desired.

□

Proposition 263. Let $K = \mathbb{Q}[\theta], R = \mathbb{Z}[\theta] \subseteq \mathcal{O}_K$ with $\deg(K/\mathbb{Q}) = n$, and let $f \in \mathbb{Z}[x]$ monic polynomial of degree n. Let

$$R^{\perp} := \left\{\beta \in K : \text{Tr}_{\mathbb{Q}}^{K}(\beta R) \subseteq \mathbb{Z}\right\} \tag{383}$$

then

$$R^{\perp} = \frac{1}{f'(\theta)} R \tag{384}$$

PROOF 264. We know that

$$\mathrm{Tr}^K_{\mathbb{Q}}\left(\frac{\theta^i}{f'(\theta)}\right) \subseteq \mathbb{Z} \tag{385}$$

for each $i = 0, ..., n-1$. But now,

$$R = \sum_{i=1}^{n-1} \mathbb{Z}\theta^i \tag{386}$$

so,

$$\mathrm{Tr}^K_{\mathbb{Q}}\left(\frac{1}{f'(\theta)}R\right) \subseteq \mathbb{Z} \tag{387}$$

Now if $\beta \in R$, then $\frac{\beta}{f'(\theta)}R \subseteq \frac{R}{f'(\theta)}$ which implies

$$\mathrm{Tr}^K_{\mathbb{Q}}\left(\frac{\beta}{f'(\theta)}R\right) \subseteq \mathbb{Z} \tag{388}$$

Thus, $\frac{\beta}{f'(\theta)} \in R^{\perp}$, which shows one inclusion: $\frac{R}{f'(\theta)} \subseteq R^{\perp}$.

Now notice that if $w_1, ..., w_n$ form a $\mathbb{Z}$-basis for R, we can take $w^{(i)} \in K$ such that $\mathrm{Tr}^K_{\mathbb{Q}}(w_i w^{(j)}) = \delta_{ij}$. So,

$$R^{\perp} = \sum_i \mathbb{Z}w^{(i)} \tag{389}$$

To get the claim, take any basis $w'_1, ..., w'_n$ of $\frac{1}{f'(\theta)}R$, and it suffices to check that

$$\det\left(\mathrm{Tr}^K_{\mathbb{Q}}(w_i w'_j)\right) = \pm 1 \tag{390}$$

Now taking $w_1, ..., w_n$ be respectively $1, \theta, ..., \theta^{n-1}$ and $w'_1, ..., w'_n$ be $\frac{1}{f'(\theta)}, \frac{\theta}{f'(\theta)}, ..., \frac{\theta^{n-1}}{f'(\theta)}$, then

$$\begin{pmatrix} \mathrm{Tr}(w_i w'_1) \\ \mathrm{Tr}(w_i w'_2) \\ \vdots \\ \mathrm{Tr}(w_i w'_n) \end{pmatrix} \tag{391}$$

is the ith column and we get something of the form

$$\begin{pmatrix} 0 & 0 & \dots & 1 \\ & \vdots & \vdots & \\ & 1 & & \\ 1 & & & \end{pmatrix} \tag{392}$$

where the lower right triangle are all integers. This proves the claim.

□

It follows that:

Proposition 265.

$$\left|\mathrm{Norm}^K_{\mathbb{Q}}(f'(\theta))\right| = ([\mathcal{O}_K : R])^2 \left|\mathrm{Disc}(K)\right| \tag{393}$$

Remark 266. These proofs are much better when one learns completions.

ASK ABOUT ALL OF THIS.

Recall: Eisenstein criterion.

Proposition 267. Let

$$f = x^n + a_{n-1}x^{n-1} + ... + a_n \tag{394}$$

such that $p|a_i$ for $i = 1, ..., n$ and $p^2 \nmid a_n$. Let $f(\theta) = 0$, and consider $R = \mathbb{Z}[\theta]$. THen $P = (p, \theta)$ is a prime ideal and $P^n = pR$ for $n = \deg f$. In particular,

$$P(P^{n-1}p^{-1}) = R \tag{395}$$

PROOF 268. We have

$$P^2 = (\theta^2, \theta p, p^2) \tag{396}$$

so, $\theta^2 \in P^2$ which implies that $a_{m-1}\theta + a_m \in P^2$ thus, $a_m \in P^2$ and $(a_m, p) \in P^2$ and so $p = \gcd(a_m, p^2)$. Thus, $P^2 = (\theta^2, p)$.

Now we can show by induction that $P^r = (\theta^r, p), \ r = 2, ..., n$.

Then $P^m = (\theta^m, p) = (p)$ but $\theta^m \in (p)$.

□

A corollary of this:

Proposition 269. If the minimal polynomial of an algebraic integer θ is Eisenstein, then $p \nmid |\mathcal{O}_K/\mathbb{Z}[\theta]|$.

PROOF 270. If p divides the order of $\mathcal{O}_K/R$, then there exists $\alpha \in \mathcal{O}_K$ not in R so that $p\alpha \in R$ and $(p, \theta)^n\theta \subseteq R$.

Now we can use this to get $\beta \in \mathcal{O}_K$ not in R so that $\beta P \subseteq R$. We can then find the least m such that $P^m\alpha \subseteq R$.

Thus, $\beta \notin R$ but $\beta \subseteq P^{-1}$ $\beta \notin R$ so $\beta^m \in P^{-m}$ but not in $P^{-(m-1)}$. Thus $\mathcal{O}_K/R$ is infinite. This is a contradiction.

□

23 Finite Fields. - -**Friday, 5.24.2019**

We won't prove Dirichlet's theorem (it's the same idea as before). We've been talking about stuff up to mid 19th century mathematics. We will now talk to stuff up to early 20th century. Hyperelliptic curves over finite fields for next lecture.

We review some basic properties of finite fields. We avoid using splitting fields and cyclotomic polynomials. Consider $\mathbb{F}_p \subseteq R$ for a commutative ring R, and the Frobenius homomorphism $\Phi : R \to R$ given by

$$\Phi(a) := a^p \tag{397}$$

Since this is a ring homomorphism, the compositions of Φ with itself is a ring homomorphism.

Proposition 271. If $f, g : R \to S$ are ring homomorphism, then

$$\{a \in R : f(a) = g(a)\} \tag{398}$$

is a subring of R.

Proof is left as an exercise.

Proposition 272. A finite field F has p^k elements for some $k \in \mathbb{N}$ and prime p.

PROOF 273. Consider the ring homomorphism $f : \mathbb{Z} \to F$ given by $f : m \mapsto m \cdot 1_F$. Then $\mathbb{Z}/\text{ker}(f) \hookrightarrow F$. Now since $\mathbb{Z}/\text{ker}(f), F$ are integral domains, we must have $\text{ker}(f) = (p)$ for some prime p.

Now F is a $\mathbb{F}_p$-vector space, and since F is finite, F must be a finite dimensional vector space. Now let k be its dimension. THen $\#F = p^k$ as desired.

□

Proposition 274. If $F \subseteq E$ are both fields, then there is $k \in \mathbb{N}$ such that $(\#F)^k = \#E$.

PROOF 275. Let $k = \dim_F E$. Then repeat the argument from the previous proposition.

□

Proposition 276. Assume F and E are finite fields and there is $k \in \mathbb{N}$ such that $(\#F)^k = \#E$. Then F is isomorphic to a subfield of E.

Proposition 277. Given $q = p^m$ for a prime p, then there exists at most one field of q elements (up to isomorphism).

PROOF 278 (Prop. 276 implies Prop. 277). **Lemma.** Let K be a field, let F and E be a finite field extension of K and assume there is $\alpha \in F$ such that $F = K(\alpha)$. Then there is a field $E' \supseteq E$ an $h : F \to E'$ such that diagram commutes:

$$\begin{tikzcd}
K \arrow[r, hook] \arrow[d, hook] & F \arrow[d, "h"] \\
E \arrow[r, hook] & E'
\end{tikzcd}$$

Proof of Lemma. We have

$$\begin{tikzcd}
K \arrow[r, "\phi"] \arrow[d] & F \\
K[X]/(f) \arrow[ur, "\cong"] &
\end{tikzcd}$$

for $\phi(x) = \alpha,\ \text{ker}\phi = (f)$ for $f \in K[X] \subseteq E[X]$ irreducible.

Now there exists $g \in E[X]$ irreducible such that $g|f$ and

$$\begin{tikzcd}
K[X] \arrow[r] \arrow[d] & E[X] \arrow[d] \\
K[X]/(f) \arrow[r] & E[X]/(g) = E'
\end{tikzcd}$$

and

$$\begin{tikzcd}
K \arrow[r, hook] \arrow[d, hook] & E \arrow[d, hook] \\
F = K[X]/(f) \arrow[r, hook, "h"] & E[X]/(g) = E'
\end{tikzcd}$$

This proves the lemma. □

Let $K = \mathbb{F}_p$. We see that $\#F = q = p^m$ where p is a prime, then $\#E = p^{mk}$. $F^\times$ is cyclic, and there exists $\alpha \in F^\times$ whose order is $p^m - 1$ and $h(\alpha) \in E'$ has order $p^m - 1$.

$$\begin{tikzcd}
\mathbb{F}_p \arrow[r, hook] \arrow[d, hook] & F = \mathbb{F}_p(\alpha) \arrow[d, hook, "h"] \\
E \arrow[r, hook] & E'
\end{tikzcd}$$

But $E^\times$ is cyclic if order $p^{mk} - 1$ and $p^m - 1 | p^{mk} - 1$. It follows that $h(\alpha) \in E$, i.e. $h : \mathbb{F}_p(\alpha) \to E$.

□

We now want to prove the following:

Proposition 279. If $q = p^m$ for a prime p, then there exists a field $\mathbb{F}_q$ with q elements.

For this, we need the following lemma:

Proposition 280. If there exists a field E of q elements and if n is a prime, then there exists a field of q^n elements.

PROOF 281. Now there exists $\alpha \in E^\times$ not an nth power. Then consider $E' = E(\alpha^{1/n})$. If $q \equiv 1 \mod n$, then replace E by $E' = E(\zeta)$ so that

$$\zeta^{n-1} + \zeta^{n-2} + ... + \zeta + 1 = 0 \tag{399}$$

and $E \subseteq E' \subseteq E''$ with $[E'' : E'] = n$.

□

Proposition 282. Let L be a field of q^k elements. Let

$$L' = \{x \in L : x^q = x\} \tag{400}$$

Then L' is a subfield of q elements of L.

PROOF 283. We have

$$L' \setminus \{0\} = \big\{x \in L' : x^{q-1} = 1\big\} \tag{401}$$

but $|L^\times| = q^k - 1$. Since $q - 1 | q^k - 1$, $|L' \setminus \{0\}| = q - 1$.

Thus L' has q elements. But the Frobenius map is a ring homomorphism from L to L, and $\{x \in L : x = x^q\}$ is a subring of L.

□

This show: If $q \not\equiv 1 \mod n$, then $E^\times$ contains a cyclic group of order n so that we can take the homomorphism $p : E^\times \to E^\times$ given by $p(a) := a^n$. Then $E^\times / p(E^\times)$ has n elements.

23.1

How do we extend what we have from $\mathbb{Z}$ to finite fields?

Observe that $\mathbb{F}_p[t]$ is i.) a PID, and ii.) if $\pi \in \mathbb{F}_p[t]$ is irreducible of degree d, then $\mathbb{F}_p[t]/(\pi) = \mathbb{F}_{p^d}$.

For instance, we can take $\pi = t - a$ for $a \in \mathbb{F}_p$, then

$$\mathbb{F}_p[t]/(\pi) \cong \mathbb{F}_p \tag{402}$$

In fact, let F be any field of characteristic not 2. Then let $P \in F[t]$ be square free. We get

$$\begin{aligned} R &= F[t][\sqrt{P}] \\ &= F[t] \oplus F[t][\sqrt{P}] \end{aligned}$$

where we can take $y := \sqrt{P}$. So in the case $F = \mathbb{C}$, the maximal ideal of R are

$$\left\{(t, y) \in \mathbb{C}^2 : y^2 = P(t)\right\} \tag{403}$$

Table 1: Analogy between the number theory in $\mathbb{Z}$ and $\mathbb{F}_p$.

$\mathbb{Z}$	$\mathbb{F}_p$
Primes	$\pi \in \mathbb{F}_p[t]$ irreducible
$\mathbb{Z}/p\mathbb{Z}$	$\mathbb{F}_{p^d}$

Something different between the two: different irreducible polynomials can give the same residue field.

24 - -Wednesday, 5.29.2019

F is a perfect field of characteristic not 2 (where we are replacing $(\mathbb{Z}, \mathbb{Q})$ by $(F[T], F(T))$). Let $H \in F[T]$ be squarefree and degree > 0 (which is true iff $\gcd(H, H') = 1$). Today and Friday, we show that we said for numbers also holds for this.

Take $K = F(T)(\sqrt{H})$ and $\mathcal{O}_K = F[T] \oplus F[T]\sqrt{H}$.

Table 2: Analogy between the number field case and function field case.

Number Field.	Function Field.
$(\mathbb{Z}, \mathbb{Q})$	$(F[T], F(T))$
Number of elements	Dimension of F vector space

We establish some general theory, but we are primarily interested in $\mathbb{C}$ and finite fields.

Proposition 284. If $I \subseteq \mathcal{O}_K$ is a nonzero ideal, then $\mathcal{O}_K/I$ is a finite dimensional F-vector space.

PROOF 285. We have $a + b\sqrt{H} \in I$ with $(a, b) \in F[T] \times F[T]$ nonzero. Then

$$f := a^2 - b^2 H \in I \tag{404}$$

is nonzero and lies in $F[T]$. Now $F[T]/(f)$ has the F-basis $1, T, ..., T^{d-1}$, and so it is a d-dimensional vector space.

We see that

$$\mathcal{O}_K / f\mathcal{O}_K \cong F[T]/(f) \oplus F[T]/(f)\sqrt{H} \tag{405}$$

has $1, T, ..., T^{d-1}, \sqrt{H}, T\sqrt{H}, ..., T^{d-1}\sqrt{H}$ is a F-basis, so $\mathcal{O}_K / f\mathcal{O}_K$ has dimension $2d$, and $\mathcal{O}_K f \subseteq I$. Now $\mathcal{O}_K / \mathcal{O}_K f$ maps onto $\mathcal{O}_K / I$, so $\mathcal{O}_K / I$ is finite dimensional.

□

Definition 286. The **rank** is

$$\text{rk}_F V := \dim_F V \tag{406}$$

and for a nonzero ideal $I \subseteq \mathcal{O}_K$, its **degree** is

$$\deg(I) := \text{rk}_F(\mathcal{O}_F / I) \tag{407}$$

We let π denote an irreducible polynomial in $F[T]$.

Proposition 287. If $P \subseteq \mathcal{O}_K$ nonzero is a prime ideal, then there exists a unique irreducible $\pi \in F[T]$ such that $\pi \in P$.

PROOF 288. Since $P \subseteq \mathcal{O}_K$ nonzero, by the proof of Proposition 284, $P \cap F[T]$ is nonzer. So let $f \in P \cap F[T]$ be nonzero, and take the prime factorization

$$f = \pi_1 ... \pi_r \in P \qquad \pi_i \in F[T] \tag{408}$$

for irreducibles π_i. Since P is prime, there exists $\pi_i \in P$. Call this prime element π. Find all prime ideals $P \subseteq \mathcal{O}_K$ such that $\pi \in P$. We casework by whether π is ramifield, split, or nonsplit.

Case 1. If $\pi | H$, then $(\pi, H) = P$ is the only prime ideal containing π. This is the case when π is ramified.

If we take $E := F[T]/(\pi)$, then for this case $\mathcal{O}_K = F[T] \oplus F[T]\sqrt{H}$, so

$$\mathcal{O}_K / \pi\mathcal{O}_K = E \oplus E\sqrt{H} \tag{409}$$

If $P \supseteq (\pi)$, then $P/(\pi) \subseteq \mathcal{O}_K / \pi\mathcal{O}_K$ is a prime ideal, and $(\sqrt{H})^2 = 0$. So, $\sqrt{H} \in P$, and thus,

$$P \supseteq I := F[T\pi \oplus F[T]\sqrt{H} \tag{410}$$

Now clearly, $\mathcal{O}_K / I \cong F[T]/(\pi)$, thus $I = P$.

Now

$$P^{=}(\pi, \sqrt{H})^2 = (\pi^2, H, \pi\sqrt{H}) \subseteq (\pi) \tag{411}$$

and since $H = \pi hin F[T]$ and H is squarefree, we have $\pi \nmid h$, so $\gcd(\pi, h) = 1$. Thus, $\gcd(\pi^2, \pi h) = \pi$ and thus, $\pi \in P^2$. This shows the other inclusion.

Case 2. Suppose H is not divisible by π and H is not a square in $F[T]/(\pi)$, then $P = (\pi)$ is a prime ideal. π is unramified and nonsplit.

Case 3. Let H not divisble by π and there exists $a \in F[T]$ such that $a^2 = H \mod (\pi)$, then there are exactly two prime ideals containing π. Then we have

$$P := (\pi, a - \sqrt{H}),\ \sigma P = (\pi, a - \sqrt{H}) \tag{412}$$

We also have $P\sigma P = (\pi)$. This is the unramified and split case.

In this case, we have $\mathcal{O}_K \cong \mathbb{F}[T][X]/(X^2 - H)$, so

$$\mathcal{O}_K/\pi\mathcal{O}_K \cong E[X]/(X^2 - \overline{H}) \tag{413}$$

Now we have

$$X^2 - H = (X - a)(X + a) \tag{414}$$

in $E[T]$ for a nonzero in E. Then

$$P = (\pi, \sqrt{H} \pm a) \tag{415}$$

and $\deg P = \deg \pi$. Now

$$P\sigma P = (\pi, a + \sqrt{H})(\pi, a - \sqrt{H}) = (\pi^2, \pi(a + \sqrt{H}), \pi(a - \sqrt{H}), a^2 - H) \subseteq (\pi) \tag{416}$$

Now $2\pi a \in P\sigma P$ which implies $\pi a \in P\sigma P$ for $\gcd(\pi, a) = 1$ in $F[T]$, so $\pi \in (\pi^2, a\pi) \subseteq P\sigma P$.

□

Proposition 289. Every nonzero ideal of $\mathcal{O}_K$ equals $P_1 ... P_r$ where P_i are prime ideals and the factorization is unique.

PROOF 290. For a nonzero prime P, we have Q nonzero such that PQ is principal and $J \subseteq \mathcal{O}_K$ such that $J \supsetneq JP$. We then prove by induction on $\deg I$.

□

Example 291. Take $F = \mathbb{C}$. What are all the nonzero ideals of $\mathcal{O}_K$?

Ramified. The π are $(T - \alpha)$ with $\alpha \in \mathbb{C}$. $\pi = T - \alpha | H$ iff $H(\alpha) = 0$, i.e. for all $\alpha \in \mathbb{C}$ such that $H(\alpha) = 0$, there is a prime ideal $P = (T - \alpha, \sqrt{H})$.

Unramified nonsplit. Does not exists since $\mathbb{C}[T]/(T - \alpha) \cong \mathbb{C}$.

Unramified Split. For $\alpha \in \mathbb{C}$, $\pi = T - \alpha$, with $\pi \nmid H$, i.e. $H(\alpha) \neq 0$. We have $a \in \mathbb{C}$ nonzero such that $a^2 = H(\alpha)$ so that we have $(T - \alpha, \pm a - \sqrt{H})$.

Remark 292. For $F = \mathbb{C}$, there is a bijection between

$$\left\{(\alpha, \beta) \in \mathbb{C}^2 : \beta^2 = H(\alpha)\right\} \tag{417}$$

and the nonzero prime ideals of $\mathcal{O}_K$ under the map

$$(\alpha, \beta) \mapsto P = (T - \alpha, \sqrt{H} - \beta) \tag{418}$$

We can now define fractional ideals in $\mathcal{O}_K$ defined as just $M \subseteq K$ which is a nonzero finitely generated $\mathcal{O}_K$-module. This forms a multiplicative group $C(\mathcal{O}_K)$ which is the fractional ideal modulo principal ideal.

25 Riemann-Roch. - -Friday, 5.31.2019

On Monday, we will attempt to count $\#\left\{(\alpha,\beta) : H(\alpha)=\beta^2\right\}$ with $F=\mathbb{F}_q$ a finite field.

Recall: Let F be a perfect field with characteristic not 2. $R := F[T] \subseteq F(T)$ and $H \subseteq R[X]$ squarefree. Take

$$K := F(T)[\sqrt{H}],\ \mathcal{O}_K = F[T] \oplus F[T]\sqrt{H} \tag{419}$$

Take a nonzero ideal $I \subseteq \mathcal{O}_K$ and

$$\deg(I) = \text{dim}_F(\mathcal{O}_K/I) \tag{420}$$

i.e., dimension as F-vector space.

For $\pi \in F[T]$ irreducible, $P \subseteq \mathcal{O}_K$ prime ideal such that $\pi \in P$. Then

1.) π ramified iff $\pi|H$, $P=(\pi,\sqrt{H})$ and $\deg P = \deg(\pi)$ (i.e. degree of polynomial $\pi \in F[T]$)
2.) π unramified nonsplit, $P=(\pi)$, and $\deg P = 2\deg(\pi)$
3.) π unramified split, $P=(\pi,\sqrt{H}\pm a)$ where $a^2 = H \mod \pi$, $\deg P = \deg(\pi)$

Which prime ideals $P \subseteq \mathcal{O}_K$ have degree 1? This is equivalent to asking which ramified or split prime has degree 1.

We can for instance have $\pi = T-\alpha$ and $P=(T-\alpha,\sqrt{H}-\beta),\ \alpha,\beta \in F$ and $\beta^2 = H(\alpha)$.

It follows that:

Proposition 293. There is a 1-1 correspondence between P prime ideal of $\mathcal{O}_K$ of degree 1 and $\left\{(\alpha,\beta) : H(\alpha)=\beta^2\right\}$ (where F is algebraically closed, thus is all prime ideals of $\mathcal{O}_K$).

We have the following lemmas:

Proposition 294. For $f \in R := F[T]$ nonzero, $\text{rank}_F(R/(f)) = \deg f$.

Proposition 295. If $M \subseteq R^2 = Re_1 \oplus Re_2$ is a R-submodule of rank 2, then M is a free R-module with basis fe_1, he_1+ge_2 and R^2/M has a F-basis $T^ie_1,\ T^je_2,\ 0 \le i \le \deg f,\ 0 \le j \le \deg g$ and

$$\text{rk}_F(R^2/M) = \deg f + \deg g = \deg(fg) = \deg\det\begin{pmatrix} f & h \\ 0 & g\end{pmatrix} \tag{421}$$

Proposition 296. If $A \in M_2(R),\ \det A \neq 0$, then

$$\text{rank}_F R^2/A(R^2) = \deg(\det A) \tag{422}$$

PROOF 297 (Proposition 296). Using Proposition 295 to $M=A(R^2)$, we get $C \in \text{GL}_2(R)$ such that $A=CD$ for

$$D := \begin{pmatrix} f & h \\ 0 & g\end{pmatrix} \tag{423}$$

Now $\det C \in R^\times$, so $\deg\det C = 0$. Thus

$$\det A = \det C \deg D \tag{424}$$

$$\deg\det A = \deg\det D = \text{rank}_F(R^2/A(R^2)) \tag{425}$$

□

Proposition 298. For $\alpha := a + b\sqrt{H} \in \mathcal{O},\ a, b \in F[T]$, then

$$\deg(N(\alpha)) = \deg(a^2 - b^2 H) = \text{rank}_F\left(\mathcal{O}_K/\alpha\mathcal{O}_{\mathcal{K}}\right) \tag{426}$$

From now on, we let $g := \left|(\alpha, \beta) : H(\alpha) = \beta^2\right|$ be the genus of the curve, and let $\deg(H) = 2g + 1$.

Consider

$$V(m) := \{\alpha \in \mathcal{O}_K : \deg N(\alpha) \leq m\} \subseteq \mathcal{O}_K \tag{427}$$

Proposition 299. $V(m)$ is a F-vector space and $\dim_F V(m) = m + 1 - g$ if $m \geq 2g + 1$.

PROOF 300. Observe that for $\alpha = a + b\sqrt{H},\ a, b \in F[T]$, then $\deg(a^2 - b^2 H) \leq m$ iff $\deg a \leq \frac{m}{2}$ and $\deg b \leq \frac{m-1-2g}{2}$. Now

$$a \in \text{span}\ 1, T, T^2, ..., T^{\left\lfloor \frac{m}{2} \right\rfloor},\ b \in \text{span}\ 1, T, T^2, ..., T^{\left\lfloor \frac{m-1-2g}{2} \right\rfloor} \tag{428}$$

and so, there are $m + 1 - g$ of them.

□

Proposition 301. Every fractional ideal I of $\mathcal{O}_{\mathcal{K}}$ is of the form αJ for $\alpha \in K^\times$ and $J \subseteq \mathcal{O}_K$ as an ideal with

$$\dim_F(\mathcal{O}_F/J) \leq g \tag{429}$$

PROOF 302. Let $I \subseteq \mathcal{O}_K$ be an ideal with

$$\dim_F\left(\mathcal{O}_K/I\right) \geq 2g + 1 \tag{430}$$

Consider $V(m) \hookrightarrow \mathcal{O}_K \to \mathcal{O}_K/I$ where γ is the map from left to right. Then $I \cap V(m) = \ker\gamma$, so

$$\dim_F V(m) = m + 1 - g > \dim_F(\mathcal{O}_K/I) \tag{431}$$

implies $I \cap V(m)$ is nonzero.

So

$$m - g \geq \dim_F(\mathcal{O}_K/I) \tag{432}$$

which implies there is $\alpha \in I \cap V(m)$ nonzero. So take $m = g + \dim_F(\mathcal{O}_K/I)$ and

$$\mathcal{O}_K \supseteq I \supseteq \mathcal{O}_K/\alpha\mathcal{O}_K \tag{433}$$

Now

$$m \geq \deg N(\alpha) = \dim_F\left(\mathcal{O}_K/\alpha\mathcal{O}_K\right) = \dim_F(\mathcal{O}_K/I) + \dim_F(I/\alpha\mathcal{O}_K) \tag{434}$$

$$m = g + \dim_F(\mathcal{O}_K/I) \geq \dim_F(\mathcal{O}_K/I) + \text{rank}(I/\alpha\mathcal{O}_K) \tag{435}$$

Thus,

$$\text{rank}(I/\mathcal{O}_K) \leq g \tag{436}$$

$$\text{rank}(\mathcal{O}_K/J) \leq g \tag{437}$$

and $\mathcal{O}_K = IJ$. Recall

$$\dim_F(\mathcal{O}_K/IJ) = \deg_F(\mathcal{O}_K/I) + \deg_F(\mathcal{O}_K/J) \tag{438}$$

Now given I, consider βI^{-1} so that $\beta I^{-1} \subseteq \mathcal{O}_K$ and

$$\dim_F(\mathcal{O}_K/\beta I^{-1}) \geq 1 + 2g \tag{439}$$

□

Proposition 303. When $g = 1$, i.e. $\deg H = 3$, there exists a 1-1 correspondence between $C(\mathcal{O}_K) = \{e\}$ and $\big\{(\alpha, \beta) : \beta^2 = H(\alpha)\big\}$.

On Monday, we will count how many points there are in this for finite fields. There is no class on Wednesday.

26 - -Monday, 6.3.2019

On Friday, we talk about zeta functions.

Recall: Let F be a perfect field with characteristic not 2, and $R = F[T]$. Take $H \in R$ square free with degree $1 + 2g$. Take

$$V(m) := \Big\{a + b\sqrt{H} : a, b \in R,\ \deg(a^2 - b^2 H) \leq m\Big\} \tag{440}$$

and rank$V(m) = m + 1 - g$ for all m large. (This is contained in Riemann-Roch.)

For $\mathcal{O}_K = R \oplus R\sqrt{H}$, we've shown that every element of $C(\mathcal{O}_K)$ is represented by $J \subseteq \mathcal{O}_K$ has $\deg(J) =$ rank$_F(\mathcal{O}_K/J) \leq g$.

Remark 304. The $g = 1$ case (which we do not prove but is very important) is connected to the Weierstrass $\wp$-function.

Today onwards, we take $F = \mathbb{F}_p$ or $\mathbb{F}_q,\ q = p^k$.

Recall that we asked what points in the fields are there on the circle $x^2 + y^2 = 1$.

We now have $H \in F_p[T]$ with degree $1 + 2g$, squarefree and $\mathbb{F}_q \supseteq \mathbb{F}_p,\ q = p^k$. We consider the set

$$X(\mathbb{F}_q) := \big\{(a, b) \in \mathbb{F}_q^2 : b^2 = H(a)\big\} \tag{441}$$

Now the first naive analogue of the Riemann hypothesis is the following:

Proposition 305 (André Weil, 40's.).

$$|\#X(\mathbb{F}_q) - q| \leq 2g\sqrt{q} \tag{442}$$

E. Bombieri and W. Schmidt gave an elementary proof of this fact (improving on the result by Stepanov.)

Remark 306. In books, they often have $|\#X(\mathbb{F}_q) - q - 1|$. But the above formula is fine because we are ignoring the point at infinity.

We also restrict to the case when k is even and large.

Today we want an upper bound for $\#X(\mathbb{F}_{q^2})$ and $q \to \infty$. We have the basis for $V(m)$ given by

$$1, 0, T, 0, T^2, ..., 0, T^g, \sqrt{H}, T^{g+1}, T\sqrt{H}, T^{g+2}, ... \tag{443}$$

where the ith one is written e_{i-1} (so $e_0 = 1,\ e_2 = T,\ e_{2g} = T^g$ etc).

There are two observations:

Proposition 307.

$$V(q-1) \otimes_{\mathbb{F}_p} V(m) \to V(q-1+qm) \tag{444}$$

$$\sum_i a_i \otimes b_i \mapsto \sum_i a_i b_i^q \tag{445}$$

is one-to-one.

This is like a decimal expansion.

Proposition 308.

$$\sum_i a_i \otimes b_i \mapsto \sum_i a_i^q b_i \tag{446}$$

is *not* one-to-one if m large.

These are simplified versions of Bombieri's argument.

Remark 309. The m of $V(m)$ is looking at the order of the pole at infinity.

PROOF 310 (Second Statement.). If $b \in V(m)$, then $b^q \in V(nq)$. Then

$$\text{rank}(V(q-1) \otimes V(n)) = (q-1+g)(m+1-g) > q(q-1) + m + 1 - g = \text{rank}V(q(q-1)+m) \tag{447}$$

for large m. Now if we choose

$$\sum_i a_i \otimes b_i \in V(q-1) \otimes V(m) \tag{448}$$

nonzero such that

$$\sum_i a_i^q b_i = 0 \tag{449}$$

then we have

$$f = \sum_i a_i b_i^q \neq 0 \tag{450}$$

We then have

$$0 = \left(\sum_i a_i^q b_i \right)^q \tag{451}$$

for $a_i, b_i \in \mathcal{O}_K$. Now let $(\alpha, \beta \in X(\mathbb{F}_{q^2})$ then

$$\sum_i a_i(\alpha,\beta)^{q^2} b_i(\alpha,\beta)^q = \sum_i a_i(\alpha,\beta) b_i(\alpha,\beta)^q = f(\alpha,\beta) \tag{452}$$

In other words, $f(\alpha,\beta) = 0$ which is interesting.

Now $f \in V(q-1+mq)$, thus $\#(\mathbb{F}_{q^2}) \leq q-1+mq$ (by regarding $f \in \mathbb{F}_p[T] \otimes \mathbb{F}_p[T]\sqrt{H}$). It remains to minimize m. We have

$$(q-1+1-1-g)(m+1-g) > q(q-1) \tag{453}$$

$$m+1-g > \frac{q(q-1)}{q-1-g} = q + \frac{qg}{q-1-g} \tag{454}$$

Now note that

$$\frac{qg}{q-1-g} = g + \epsilon \tag{455}$$

where q is sufficiently large where $|\epsilon| < 1$.

Now $m - g \geq q + g$, thus

$$m+1-g \geq q+g+1 > q+g+\epsilon \tag{456}$$

Thus we take $m - g = q + g$, i.e. $m = q + 2g$, and

$$\#X(F_{p^2})q^2 + (2g+1)q - 1 \leq q-1+qm = q-1+q(q+2g) \tag{457}$$

□

Proposition 311 (Bombieri-Stepanov-Schmidt).

$$\#X(\mathbb{F}_{q^2}) \leq q^2 + (2g+1)q - 1 \tag{458}$$

of $q = p^k$ and $k \geq c$ for some constant c.

Remark 312. Now considering the valuation $v(\cdot)$, $v(e_i) = -i$ is the order of vanishing at infinity. We then see that $v(a_i) \geq -(q-1)$ and $v(e_i^q) = -qi$.

27 Zeta Functions. - -Friday, 6.7.2019

The Riemann zeta function is given by

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\text{:prime}} \left(1 - \frac{1}{p^s}\right)^{-1} \tag{459}$$

Dedekind defined the analogous function for the number field K and ring of integers $\mathcal{O}_K$:

$$\zeta_K(s) = \sum_{I \subseteq \mathcal{O}_K} \frac{1}{N(I)^s} = \prod_{\mathfrak{p} \subseteq \mathcal{O}_K \text{ prime}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} \tag{460}$$

Now in the last few part of the course, we discussed

$$K = \mathbb{F}_p(T)[\sqrt{H}] \qquad \deg H = 2g+1 \tag{461}$$

with $H \in \mathbb{F}_p[T]$ squarefree and

$$\mathcal{O}_K = \mathbb{F}_[T] \oplus \mathbb{F}_p[T]\sqrt{H} \tag{462}$$

and the curve

$$X(\mathbb{F}_p) = \left\{(\alpha, \beta) \in \mathbb{F}_{p^k}^2 : \beta^2 = H(\alpha)\right\} \tag{463}$$

Emil Artin then considered

$$\zeta_{\mathcal{O}_K}(s) = \sum_{I \subseteq \mathcal{O}_K} \frac{1}{N(I)^s} = \sum_{I \subseteq \mathcal{O}_K} \frac{1}{p^{s \deg I}} \tag{464}$$

where we recall that $N(I) = |\mathcal{O}_K/I| = p^{\deg I}$ since $\mathcal{O}_K/I$ is an $\mathbb{F}_p$ vector space.

The conventional notation is taking $t := p^{-s}$,

$$Z_X(t) = \sum_{I \subseteq \mathcal{O}_K} t^{\deg I} \in \mathbb{Z}[[t]] \tag{465}$$

where we think of t small.

Proposition 313.

$$Z_X(t) = \prod_{P \subseteq \mathcal{O}_K \text{ prime}} (1 - t^{\deg P})^{-1} \tag{466}$$

PROOF 314. Using the fact that ideals are a product of primes, we can rewrite the RHS as

$$\prod_{P \subseteq \mathcal{O}_K \text{ prime}} (1 + t^{\deg P} + t^{2\deg P} + t^{3\deg P} + ...) = \prod_{P \subseteq \mathcal{O}_K \text{ prime}} (1 + t^{\deg P} + t^{\deg P^2} + t^{\deg P^3} + ...) \tag{467}$$

Now from unique prime factorization of ideals, we get we see that the Euler product is equal to the series. □

Proposition 315.

$$\log Z_X(t) = \sum_{N=1}^{\infty} \#X(\mathbb{F}_{p^N}) \cdot \frac{t^N}{N} \tag{468}$$

Note that we can take logarithms formally via power series.

PROOF 316. From the previous proposition,

$$\begin{aligned}
\log Z_X(t) &= \sum_P (-\log(1 - t^{\deg P})) \\
&= \sum_{n=1}^{\infty} \sum_P \frac{t^Z n \deg P}{n} \\
&= \sum_n \sum_P \frac{t^{n \deg P}}{n \deg P} \cdot \deg P
\end{aligned}$$

We then have the following lemma:

Lemma. For all natural number N,

$$\#(\mathbb{F}_{p^N}) = \sum \{\deg P : P \subseteq \mathcal{O}_K \text{ prime}, \ \deg P | N\} \tag{469}$$

Taking $N = n \deg P$ implies the proposition.

Proof of Lemma. Consider

$$\mathcal{O}_K = \mathbb{F}_[T, Y]/(Y^2 - H(T)) \tag{470}$$

Now we consider the universal property of polynomial rings: consider the collection of all ring homomorphisms $\mathcal{O}_K \to \mathbb{F}_{p^N}$. This is equivalent to all ring homomorphism $\phi : \mathbb{F}_p[T, Y] \to \mathbb{F}_{p^N}$ with $\phi(Y^2 - H(T)) = 0$.

We then have a one-to-one correspondence between the ring homomorphisms $\phi : \mathbb{F}_p[T, Y] \to \mathbb{F}_{p^N}$ and $(\alpha, \beta) \in \mathbb{F}_{p^N}$, i.e. given (α, β), we can take

$$\phi(f(T, Y)) = f(\alpha, \beta) \tag{471}$$

These are ring homomorphisms that take $Y^2 - H(T)$ to zero and so $\beta^2 - H(a) = 0$.

Now $X(\mathbb{F}_{p^N})$ is in bijection with the ring homomorphisms $\psi : \mathcal{O}_K \to \mathbb{F}_{p^N}$. Now given ψ, we can let $P := \ker\psi$, and

$$\begin{tikzcd}
\mathcal{O}_K \arrow[r, "\psi"] \arrow[d] & \mathbb{F}_{p^N} \\
\mathcal{O}_K/P \arrow[ur] &
\end{tikzcd}$$

If $\deg P = k$, then $\mathcal{O}_K/P \cong \mathbb{F}_{p^k}$. Then necessarily $k|N$.

So far, we found (via $\psi \mapsto \ker\psi$)

$$X(\mathbb{F}_{p^N}) \xrightarrow{\theta} \{P \subseteq \mathcal{O}_K,\ \deg P|N\} \tag{472}$$

The claim is that θ is onto, and $\#\theta^{-1}(P) = \deg P$.

Let's prove the claim. Assume $\deg P = k|N$. We want to prove that there is the map $\mathcal{O}_K/P \to \mathbb{F}_{p^N}$ in the previous diagram. But we have existence and we also see that it is not unique since we can compose the map with powers of Frobenius automorphisms. This proves the claim.

□

So in order to count the number of points in $X(\mathbb{F}_{p^N})$, it suffices to compute $\log Z_X(t)$ from the above proposition. But in order to do that we have to look at the original zeta function.

Proposition 317.

$$(1 - pt)Z_X(t) \in \mathbb{Z}[t] \tag{473}$$

i.e., $Z_X(t)$ is a rational function.

Definition 318. Given fractional ideal J,

$$Z_J(t) := \sum_{\substack{0 \neq I \subseteq \mathcal{O}_K \\ I \sim J \text{ in } \mathrm{Cl}(\mathcal{O}_K)}} t^{\deg I} \tag{474}$$

PROOF 319. Let $J_1, ..., J_h$ be representatives of the class group. We see that

$$Z_X(t) = \sum_{i=1}^{h} Z_{J_i}(t) \tag{475}$$

We've shown that every ideal $\sim$ to an ideal $J \subseteq \mathcal{O}_K$ such that $\deg J \leq g$ (i.e. a finite set).

Now observe that

$$Z_{\mathcal{O}_X}(t) = \sum_{0 \neq \alpha \in \mathcal{O}_K} t^{\deg \alpha} \tag{476}$$

where we are summing over all principal ideals (so in particular, α is equivalent to $\lambda\alpha$ for $\lambda \in \mathbb{F}_p^\times$).

Recall that

$$V(m) = \{\alpha \in \mathcal{O}_K : \deg(\alpha) \leq m\} \tag{477}$$

is a $\mathbb{F}_p$-vector space with rank $m+1-g$ if m large.

Now

$$Z_{\mathcal{O}_K}(t) = \sum_{m=0}^{\infty} t^m \left(\frac{\#\{\alpha : \deg \alpha = m\}}{p-1} \right) \tag{478}$$

Now

$$\#\{\alpha : \deg(\alpha) = m\} = \#(V(m) - V(m-1)) = p^{m+1-g} - p^{m-g} \tag{479}$$

for large m.

Therefore, $(1-pt)Z_X(t)$ is a polynomial of degree at most $2g$.

Definition 320. For $J \subseteq \mathcal{O}_K$,

$$Z_{J^{-1}}(t) = \sum_{\substack{I \subseteq \mathcal{O}_K \\ IJ \text{ principal}}} t^{\deg I} = \sum_{\substack{I \subseteq \mathcal{O}_K \\ IJ \text{ principal}}} t^{\deg(IJ) - \deg J} \tag{480}$$

Using this, we have

$$\begin{aligned} Z_{J^{-1}}(t) &= t^{-\deg J} \sum_{\substack{0 \neq \alpha \in J \\ \alpha \sim \lambda\alpha,\ \lambda \in \mathbb{F}_p^\times}} t^{\deg \alpha} \\ &= t^{-\deg J} \sum_{\substack{0 \neq \alpha \in J \\ \alpha \sim \lambda\alpha,\ \lambda \in \mathbb{F}_p^\times}} t^m a_m \end{aligned}$$

for

$$a_m = \frac{1}{p-1} \left(\#(V(m) \cap J) - \#(V(m-1) \cap J) \right) \tag{481}$$

for which we still get $pa_m = a_{m+1}$ for all m large.

This implies that

$$(1-pt)Z_J(t) \in \mathbb{Z}[t] \tag{482}$$

□

We skipped a few details. In a more careful treatment, we'd need to consider:

Proposition 321.

$$f(t) = 1 - a_1 t + a_2 t^2 + ... + (-1)^{2g} a_{2g} t^{2g} = \prod_{i=1}^{2g} (1 - \lambda_i t) \tag{483}$$

with $a_i a_{2g-i} = p^g$ and $\lambda_i \in \mathbb{C}$. In fact, λ_i are algebraic integers for which

$$(\lambda_1, ..., \lambda_{2g}) \tag{484}$$

is a permutation of

$$\left(\frac{p}{\lambda_1}, ..., \frac{p}{\lambda_{2g}} \right) \tag{485}$$

It follows that

Proposition 322.

$$\#X(\mathbb{F}_{p^N}) = p^N + (-1)^N \left(\sum_{i=1}^{2g} \lambda_i^N \right) \tag{486}$$

Remark 323. Once again, we are ignoring the one point at infinity.

Proposition 324 (Weil Conjecture for Curves, Proved by Weil.). All λ_i have absolute value $p^{1/2}$.

This implies that

$$\left| \#X(\mathbb{F}_{p^N}) - p^N \right| \leq p^{1/2} \cdot (2g) \tag{487}$$