581F: FINAL PROJECT
RAMIFICATION GROUP

EINA OOKA

In this paper, we will discuss about a sequence of subgroups of galois groups called ramification groups. In general, these ramification groups can be very complicated; however, in the case of cyclotomic extensions, they are subgroups of a finite cyclic group, which behaves relatively well. So, our goal in this paper is to look at a few properties about ramification groups in general, and then compute explicitly ramification groups of the cyclotomic extensions.

1. Definitions and Properties

Throughout this paper, let $K/\mathbb{Q}$ be a finite separable Galois extension of a number field K. Denote $G = Gal(K/\mathbb{Q})$. For a prime $p \in \mathbb{Z}$ and a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ over p, we have learned about the decomposition group and inertia group of $\mathfrak{p}$, which are both subgroups of G.

Definition 1. The*Decomposition group* of $\mathfrak{p}$ is defined by

$$D_{\mathfrak{p}} = \{\sigma \in G | \sigma(\mathfrak{p}) = \mathfrak{p}\}$$

. The *inertia group* is defined by

$$I_{\mathfrak{p}} = \{\sigma \in G | \sigma(a) \equiv a (\text{mod } \mathfrak{p}) \text{ for all } a \in \mathcal{O}_K\}$$

.

We have discussed in class the following properties:

(i) The sequence
$$1 \to I_{\mathfrak{p}} \to D_{\mathfrak{p}} \to Gal(k_{\mathfrak{p}}/\mathbb{F}_p) \to 1$$
is exact, i.e. $I_{\mathfrak{p}}$ is the kernel of a surjection $D_{\mathfrak{p}} \to Gal(k_{\mathfrak{p}}/\mathbb{F}_p)$

(ii) The order of $D_{\mathfrak{p}}$ is ef, and that of $I_{\mathfrak{p}}$ is e where e is the ramification index and f if the residue class degree of $\mathfrak{p}$.

Now, we can define a decreasing sequence of subgroups, called *ramification groups* by modifying the inertia group by looking at the residue field of prime powers.

Definition 2. The m-th *ramification group* is defined for $m = 0, 1, 2, ...$ by

$$G_m = \{\sigma \in G | \sigma(a) \equiv a (\text{mod } \mathfrak{p}^{m+1}) \text{ for all } a \in \mathcal{O}_K\}$$

.

We can see from the definition that $G_0 = I_{\mathfrak{p}}$, and is the largest subgroup of G that acts trivially on the residue field $\mathcal{O}_K/\mathfrak{p}$. Since $O_K/\mathfrak{p} \subseteq \mathcal{O}_K/\mathfrak{p}^2 \subseteq \mathcal{O}_K/\mathfrak{p}^3 \subseteq ...$, the ramification groups form a decreadng sequence $G_0 \supseteq G_1 \supseteq G_2 \supseteq ....$

Because $L/\mathbb{Q}$ is a finite Galois extension, G is finite. We have a decreasing sequence of subgroups of a finite group G, from which we can conclude that it must stabilize for some n. What we would like to do here is to show that $G_n = 1$ for some n.

In order to do this, we need to know certain properties of valuations. Since we have a dedekind domain, we can take the *exponential valuation*, $\nu_{\mathfrak{p}}$ for our map from $\mathcal{O}_K$ to $\mathbb{R}$, which is given by

$$(\alpha) = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\alpha)}$$

where the product is taken over all nonzero prime ideals. Moreover, there exists an element $\pi \in \mathcal{O}_K$ such that $\nu_{\mathfrak{p}}(\pi^i) = i$ for all $i \in \mathbb{Z}$. In the completion of $\mathcal{O}_K$, every element can be uniquely written as an infinite sum of linear combinations of π^is. Because $\pi^{n+1} \in \mathfrak{p}^{n+1}$, by passing to the quotient, every element in $\mathcal{O}_K/\mathfrak{p}$ can be expressed as a linear combinations of π^is for $i = 1, 2, .., n$ in the residue field $\mathcal{O}_K/\mathfrak{p}^{n+1}$.

Lemma 3. *With π defined as above, for $m = 1, 2, ...$*

$$G_m = \{\sigma \in G | \sigma(\pi) \equiv \pi \, (mod \; \mathfrak{p}^{m+1})\}$$

Proof. Clearly the left hand side of the equality is contained in the right hand side. Thus, we need to show the other containment. Let $\alpha \in \mathcal{O}_K$. Denote the fixed field of $I_{\mathfrak{p}}$ by T. There exit $\alpha_0, \alpha_1, ..., \alpha_m \in \mathcal{O}_T$ such that

$$\alpha \equiv \sum_{i=0}^{n} \alpha_i \pi^i (\text{mod } \mathfrak{p}^{n+1})$$

Now take $\sigma \in D_{\mathfrak{p}}$ such that $\sigma(\pi) = \pi$ (mod $\mathfrak{p}^{n+1}$). Since σ acts trivially on $\mathcal{O}_K/\mathfrak{p}$, σ acts trivially on elements of T, such as α_is. Then we have

$$\sigma(\alpha) \equiv \sum_{i=0}^{n} \alpha_i \sigma(\pi)^i \equiv \sum_{i=0}^{n} \alpha_i \pi^i \equiv \alpha (\text{mod } \mathfrak{p}^{n+1})$$

.

□

Proposition 4. *$G_n = 1$ for sufficiently large n.*

Proof. Let $\sigma \in G_m$ for all $m = 1, 2, ...$ We want to show that such σ is the identity. Since $\sigma(\pi) \equiv \pi$ (mod $\mathfrak{p}^{n+1}$) for all n, $\sigma(\pi) = \pi$. Because π is taken to be $\nu_{\mathfrak{p}}(\pi) = 1$, this imply that $T(\pi)$ contains $\mathfrak{p}$, where T is again the fixed field of $I_{\mathfrak{p}}$. Thus the ramification index of $T(\pi)/T$ must be e, where we also know that K/T is of degree e (discussed in class). Therefore $T(\pi) = K$. Because σ acts trivially on T and on π, σ fixes every element of K. □

2. Example: The Cyclotomic Field ($p = 7$)

Now I would like to compute the decomposition groups, inertia groups and ramification groups of the cyclotomic field $K = \mathbb{Q}(\zeta_7)$, which is a degree 6 extension of $\mathbb{Q}$, with the defining minimal polynomial $(x^7 - 1)/(x - 1)$. The ring of integers $\mathcal{O}_K$ is given by $\mathbb{Z}[\zeta_7]$.

The galois group $Gal(K/\mathbb{Q})$is a cyclic group of order 6, with a generator $(\zeta_7 \to (\zeta_7)^3)$. Because it is cyclic, we can find $D_{\mathfrak{p}}$ and $I_{\mathfrak{p}}$ easily by the order of the subgroup.

```
sage: K.<a> = NumberField((x^7-1)/(x-1))

sage: I= K.fractional_ideal(2); I.factor()
(Fractional ideal (a^5 + a^4 + 1) of Number Field in a with ...) *
(Fractional ideal (a^3 + a^2 + 1) of Number Field in a with ...)

sage: I= K.fractional_ideal(3); I.factor()
Fractional ideal (3) of Number Field in a with defining ...

sage: I= K.fractional_ideal(5); I.factor()
Fractional ideal (5) of Number Field in a with defining ...

sage: I= K.fractional_ideal(7); I.factor()
(Fractional ideal (a^5 + a^4 + a^3 + a^2 + a + 2) of Number ...)^6

sage: I= K.fractional_ideal(11); I.factor()
(Fractional ideal (-2*a^4 - 2*a^2 - 2*a + 1) of Number Field ...) *
(Fractional ideal (2*a^5 + 2*a^4 + 3*a^3 + 2) of Number Field ...)

sage: I= K.fractional_ideal(13); I.factor()
(Fractional ideal (a^5 - a^4 - a^3 + a^2 + 1) of Number Field ...) *
(Fractional ideal (2*a^4 + a^3 + a^2 + 2*a) of Number Field ...) *
(Fractional ideal (a^5 + 2*a^4 + 2*a^3 + a^2 + 2) of Number ...)

sage: I= K.fractional_ideal(17); I.factor()
Fractional ideal (17) of Number Field in a with defining ...

sage: I= K.fractional_ideal(19); I.factor()
Fractional ideal (19) of Number Field in a with defining ...

sage: I= K.fractional_ideal(23); I.factor()
(Fractional ideal (-2*a^5 - 5*a^2 - 2*a - 2) of Number Field ...) *
(Fractional ideal (2*a^5 + 2*a^4 + 5*a^3 + 2) of Number Field...)

sage: I= K.fractional_ideal(29); I.factor()
(Fractional ideal (-a^5 - a^4 - 2*a^3 - a^2 - 1) of Number  ...) *
(Fractional ideal (a^5 - a^4 + a) of Number Field in a with ...) *
(Fractional ideal (a^5 + a^4 + a^2 + a + 2) of Number Field ...) *
(Fractional ideal (-a^4 - a^3 - a^2 - a - 2) of Number Field ...) *
(Fractional ideal (a^3 + a^2 - a) of Number Field in a with ...) *
(Fractional ideal (-a^5 + a^3 - 1) of Number Field in a with ...)
```

In this example, (7) is the only prime in $\mathbb{Z}$ that factors in $\mathcal{O}_K$ to be have a nontrivial inertia group. We would like to compute the series of ramification groups for this $\mathfrak{p} = (\zeta_7^5 + \zeta_7^4 + \zeta_7^3 + \zeta_7^2 + \zeta_7 + 2)$ over 7.

As we've shown in Lemma 3, we only have to check which galois element acts trivially on $\pi \pmod{\mathfrak{p}^{n+1}}$, for $\pi \in \mathcal{O}_K$ such that $\nu_{\mathfrak{p}}(\pi) = 1$. Clearly we can take $\pi = \zeta_7^5 + \zeta_7^4 + \zeta_7^3 + \zeta_7^2 + \zeta_7 + 2$, which is the generator of $\mathfrak{p}$ itself. Also take the generator of the galois group to be $\sigma : \zeta_7 \to (\zeta_7)^3$.

In the following computation, $\mathfrak{p} = J$, $b = \sigma(\pi) - \pi$, $c = \sigma^2(\pi) - \pi$ and $d = \sigma^3(\pi) - \pi$. I am examining whether those elements are in $\mathfrak{p}^n$. If it is, then it means that $\sigma(\pi)^i = \pi \pmod{\mathfrak{p}^n}$ for $i = 1, 2, 3$. We have to check only for σ^i for $i = 1, 2, 3$, since these are generators of all the subgroups, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$, respectively.

```
sage: J = (K.fractional_ideal(a^5 + a^4 + a^3 + a^2 + a + 2))

sage: b = (21*a^15 - 14*a^12 + 21*a^9 + 7*a^3 + 7)-(21*a^5 - 14*a^4 + 21*a^3 + 7*a + 7)
sage: b in J
True
sage: b in J^2
True
...
sage: b in J^7
True
sage: b in J^8
False

sage: c=  (21*a^10 - 14*a^8 + 21*a^6 + 7*a^2 + 7)-(21*a^5 - 14*a^4 + 21*a^3 + 7*a + 7)
sage: c in J^7
True
sage: c in J^8
False

sage: d=  (21*a^30 - 14*a^24 + 21*a^18 + 7*a^6 + 7)-(21*a^5 - 14*a^4 + 21*a^3 + 7*a + 7)
sage: d in J^7
True
sage: d in J^8
False
```

This shows that ramification groups G_m is the whole galois group for $m = 0, 1, 2, ..., 6$, and is trivial for $m > 6$.

$$G_0 = (\mathbb{Z}/7\mathbb{Z})^\times \supseteq (\mathbb{Z}/7\mathbb{Z})^\times \supseteq (\mathbb{Z}/7\mathbb{Z})^\times \supseteq (\mathbb{Z}/7\mathbb{Z})^\times \supseteq (\mathbb{Z}/7\mathbb{Z})^\times \supseteq (\mathbb{Z}/7\mathbb{Z})^\times \supseteq (\mathbb{Z}/7\mathbb{Z})^\times \supseteq \{e\} = G_7$$

As we have observed above, 7 factors into a prime to the power of 6, creating interesting sequence of ramification groups. This is in fact true for any prime p in the cyclotomic extension by ζ_p, i.e., p always factor as a prime to the power of p-1 in $\mathcal{O}_K$ [2].

```
sage: K.<a> = NumberField((x^7-1)/(x-1))
sage: I= K.fractional_ideal(7); I.factor()
(Fractional ideal (a^5 + a^4 + a^3 + a^2 + a + 2) of Number ...)^6

sage: K.<a> = NumberField((x^13-1)/(x-1))
sage:  I= K.fractional_ideal(13); I.factor()
(Fractional ideal (-a^4 + 1) of Number Field in a with ...)^12

sage: K.<a> = NumberField((x^19-1)/(x-1))
sage:  I= K.fractional_ideal(19); I.factor()
(Fractional ideal (-a^15 + a^12) of Number Field in a ...)^18
```

Granting this fact, the next proposition follows easily by noting that the order of $I_{\mathfrak{p}} \subset D_{\mathfrak{p}}$ is e.

Proposition 5. *For any prime p with the cyclotomic field $\mathbb{Q}(\zeta_p)$, the decomposition group and the inertia group of primes over p are always the Galois group itself.*

By observing that the G_m for 7 in $\mathbb{Q}(\zeta_7)$ was the whole galois group for $m = 1, 2, ...6$, and trivial otherwise, we might want to guess that G_m is the whole galois group for $m = 1, 2, ..., p-1$ and trivial for $m > 6$. This is actually not true in general. Consider the following counter-example when $p = 5$ with the generator of the galois group $(\zeta_5 \to (\zeta_5)^2)$.

```
sage: K.<a> = NumberField((x^5-1)/(x-1))

sage:  I= K.fractional_ideal(5); I.factor()
(Fractional ideal (a^3 + 2*a^2 + a + 1) of Number Field in a ...)^4

sage: J = (K.fractional_ideal(a^3 + 2*a^2 + a + 1))

sage: b = (a^6 + 2*a^4 + a^2 + 1) - (a^3 + 2*a^2 + a + 1)
sage: b in J
True
sage: b in J^2
False

sage: c = (a^12 + 2*a^8 + a^4 + 1) - (a^3 + 2*a^2 + a + 1)
sage: c in J
True
sage: c in J^2
False
```

Therefore the series of ramification group for this case is:

$$I_{\mathfrak{p}} = (\mathbb{Z}/5\mathbb{Z})^{\times} \supseteq \{e\} = G_1$$

References

[1] Helmut Koch, Number Theory - Algebraic Numbers and Function, Graduate Studies in Mathematics Volume 24 (2000), pp171- 176.
[2] P. Stevenhagen, Voortgezette Getaltheorie, Thomas Stieltjes Institute (2002), p46