Student seminar notes week 4

Aleksandra Bogdanova after the talk of
Kasimir De Lataillade and Sandro Pfammatter

1 Characters of finite abelian groups

Definition 1.1. A charater χ for a finite abelian group, G, is a group homeomorphism

$$\chi : G \to \mathbb{C}^\times.$$

The product of two characters χ_1, χ_2 is defined for any $g \in G$ as

$$\chi_1 \cdot \chi_2(g) = \chi_1(g) \cdot \chi_2(g).$$

We denote $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^\times)$ and denote the neutral element χ_0, defined by $\chi_0(g) = 1$, for all $g \in G$.

Lemma 1.2. $G \cong \widehat{G}$.

Proof. As G is a finite abelian group we have $G = \bigoplus_n \mathbb{Z}/n\mathbb{Z}$, thus
$\hat{G} = \bigoplus_n \widehat{\mathbb{Z}/n\mathbb{Z}}$.
Any $\chi \in \widehat{\mathbb{Z}/n\mathbb{Z}}$ is uniquely determined by $\chi(1)$, thus $\chi \mapsto \chi(1)$ is an injective map from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{C}^\times$. We notice that set of $\chi(1)$'s correspond to the set of n-th roots of unity, which allows us to conclude that $\widehat{\mathbb{Z}/n\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}$, so $G \cong \widehat{G}$. □

Lemma 1.3. *There is a natural isomorphism* $G \cong \widehat{\widehat{G}}$.

Proof. We define the following map, for any $g \in G$:

$$\begin{aligned} \hat{g} \colon \widehat{G} &\to \mathbb{C}^\times \\ \chi &\mapsto \chi(g). \end{aligned}$$

It follows that the map

$$\begin{aligned} G &\to \widehat{\widehat{G}} \\ g &\to \hat{g} \end{aligned}$$

is clearly an homomorphism (it can be proven as an exercise). As $|G| = |\widehat{G}| = |\widehat{\widehat{G}}|$, we only need to show injectivity, to get that it is an isomorphism.
If $\hat{g}(\chi) = \chi(g) = 1$, for all $\chi \in \widehat{G}$, we look at the subgroup $H = \langle g \rangle$ of G. Then

it is immediate to see that elements of $\widehat{G}$ can be viewed as elements of $\widehat{G/H}$, by the first isomorphism theorem. This implies that $|\widehat{G/H}| = |\widehat{G}| = |G|$, thus $|H| = 1$, so the map is indeed injective, as the only elements sent to $id_{\widehat{\widehat{G}}}$ is 1.

□

We can thus naturally identify G with $\widehat{\widehat{G}}$.

Proposition 1.4. *For $H < G$, we define $H^\perp := \{\chi \in \widehat{G} : \chi(h) = 1 \quad \forall h \in H\}$.*

1. *if $H < G$, then $H^\perp \cong \widehat{G/H}$*
2. *if $H < G$, then $\widehat{H} \cong \widehat{G}/H^\perp$*
3. *$(H^\perp)^\perp = H$, under the identification $\widehat{\widehat{G}} \cong G$.*

Proof.

1. For any $\chi \in H^\perp$, we define $\psi \in \widehat{G/H}$ as $\psi(gH) = \chi(g)$, it is clearly well defined and is actually an isomorphism.
2. Clearly $\chi \mapsto \chi|_H$, is a homomorphism from $\widehat{G}$ to $\widehat{H}$, with kernel $H^\perp$. We also notice that $|H^\perp| = |\widehat{G/H}| = |G|/|H|$, so $|\widehat{H}| = |H| = |G|/|H^\perp| = |\widehat{G}|/|H^\perp| = |\widehat{G}/H^\perp|$, which allows us to conclude.
3. First we notice that $(H^\perp)^\perp = \{\hat{g} \in \widehat{\widehat{G}} | \hat{g}(\chi) = 1, \quad \forall \chi \in H^\perp\}$. We get for all $h \in H$, $\hat{h}(H^\perp) = \{1\}$, thus we deduce $\widehat{\widehat{H}} = H \subseteq (H^\perp)^\perp$.
   We also notice that, by our previous calculations
   $$|(H^\perp)^\perp| = |\widehat{G}/H^\perp| = |G|/|G/H| = |H|,$$
   which allows us to conclude.

□

Proposition 1.5 (Orthogonality relations)**.** *Let G be a finite abelian group.*

1. *Fix χ a character, then: $\sum_{g\in G} \chi(g) = \begin{cases} 0 & \text{if } \chi \neq \chi_0 \\ |G| & \text{if } \chi = \chi_0 \end{cases}$*
2. *Fix an element $g \in G$, then $\sum_{\chi\in\widehat{G}} \chi(g) = \begin{cases} 0 & \text{if } g \neq 1 \\ |G| & \text{if } g = 1 \end{cases}$*

Proof.

1. We have $\sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(hg) = \chi(h) \sum_{g\in G} \chi(g)$, for some $h \in G$. This gives us $\sum_{g\in G} \chi(g)(\chi(h) - 1) = 0$.
   Either $\chi(h) = 1$, and as we can take any $h \in G$ in the previous calculations, we get that $\chi = \chi_0$, and in particular $\sum_{g\in G} \chi_0(g) = |G|$.
   Or $\sum_{g\in G} \chi(g) = 0$, and we are done, in the case $\chi \neq \chi_0$.
2. Noticing that $\chi(g) = \hat{g}(\chi)$, we can conclude using point 1).

□

2 Dirichlet Characters

Definition 2.1 (Dirichlet character)**.** A Dirichlet character is a character of the group $(\mathbb{Z}/n\mathbb{Z})^\times$, for some $n \in \mathbb{N}$. For $\chi \in \widehat{\mathbb{Z}/n\mathbb{Z}}$, n is called the modulus of χ.

Example 2.2.
1. if p is an odd prime, the Legendre symbol is a Dirichlet character of modulus p, where the Legendre symbol is $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$, for $a \in \mathbb{Z}/p\mathbb{Z}$.
2. $\chi : (\mathbb{Z}/5\mathbb{Z}) \to \mathbb{C}^\times$, such that $\chi(1) = 1$, $\chi(2) = i$, $\chi(3) = -i$ and $\chi(4) = -1$.

We notice that for if $n|m$ we have a natural homomorphism

$$\varphi : (\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times.$$

We define $\tilde{\chi} = \chi \circ \varphi$, which is clearly in $\widehat{(\mathbb{Z}/m\mathbb{Z})^\times}$, for any $\chi \in \widehat{(\mathbb{Z}/n\mathbb{Z})^\times}$. In this case we say that $\tilde{\chi}$ is **induced** by χ.
We say that χ is **primitive** if it is not induced by any character of lower modulus. We define f_χ to be the minimal modulus of a Dirichlet character χ, i.e χ is not induced by a character of smaller modulus, and call f_χ the **conductor** of χ.

We notice that any Dirichlet character can be extended to a function $\mathbb{Z} \to \mathbb{C}$, by setting: $\chi(a) = \begin{cases} \chi(a \mod f_\chi) & \text{if } (a, f_\chi) = 1 \\ 0 & \text{if } (a, f_\chi) \neq 1 \end{cases}$.

If we take χ_1, χ_2 two primitive Dirichlet characters, with conductor n and m respectively. We notice that for $l = \text{lgm}(n, m)$, we get a character:

$$\begin{aligned} \eta\colon (\mathbb{Z}/n\mathbb{Z})^\times &\to \mathbb{C}^\times \\ a &\mapsto \chi_1(a)\chi_2(a). \end{aligned}$$

This character need not be irreducible, but we can define $\chi_1\chi_2$ as the irreducible character which induces η. This enables us to define a closed product on the set of primitive Dirichlet characters, that is clearly associative, commutative and with identity χ_0.

Example 2.3.

We take $\chi : (\mathbb{Z}/12\mathbb{Z})^\times \to \mathbb{C}^\times$, defined by $\chi(1) = 1$, $\chi(5) = -1$, $\chi(7) = -1$ and $\chi(11) = 1$, and $\varphi : (\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{C}^\times$, defined by $\varphi(1) = 1$, $\varphi(3) = -1$.
We get $\eta : (\mathbb{Z}/12\mathbb{Z})^\times \to \mathbb{C}^\times$, such that $\eta(1) = \chi(1)\varphi(1) = 1$, $\eta(5) = -1$, $\eta(7) = 1$, $\eta(11) = -1$, which is not primitive.
Indeed, we notice that the primitive character that induces η is:
$\chi\varphi : (\mathbb{Z}/3\mathbb{Z})^\times \to \mathbb{C}^\times$, such that $\chi\varphi(1) = 1$, $\chi\varphi(2) = -1$, so $f_{\chi\varphi} = 3$.

We notice that for any $n \in \mathbb{N}$, $\chi \in \widehat{(\mathbb{Z}/n\mathbb{Z})^\times}$, $\bar{\chi} = \chi^{-1}$, as the image of χ is contained in the set of n-th roots of unity. We also notice that $\bar{\chi}$ has to have

the same conductor as χ, and $\bar{\chi} \cdot \chi = \chi_0$. Combining this observation with the previous paragraph we get that the Dirichlet characters form a group, as any Dirichlet character can be represented by a primitive Dirichlet character and their product is well defined.
We call **order** of a Dirichlet character its order as a group element, and notice that it is always finite.

In particular we notice that $\chi(-1) = \pm 1$, if $\chi(-1) = 1$ we say that χ is **even** and if $\chi(-1) = -1$ we call χ **odd**. Actually, the set of even characters forms a subgroup of the group of Dirichlet characters.

We can easily notice that the Dirichlet characters with conductor dividing n form a finite subgroup, noticing for instance that the lcm of two of their conductors is always going to be smaller or equal to n.

We define ζ_n to be a primitive n-th root of unity, then we can identify $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ with $(\mathbb{Z}/n\mathbb{Z})^\times$. Let $\chi \in \widehat{G}$, and $K = \mathbb{Q}(\zeta_n)^{\ker(\chi)}$ (as clearly $\ker(\chi)$ is a subgroup of G), we call K the **the field associated to** χ.
More generally, we can consider $X < \widehat{G}$ (i.e X is a subgroup that contains characters such that the lcm of their conductors divides n). Let $H = \cap_{\chi \in X} \ker(\chi)$, then H is a subgroup of G, and we call the fixed field by H the **field associated to** X. Furthermore, under the identification $G \cong \widehat{\widehat{G}}$, we notice that $H = X^\perp$, as $\{\hat{g} \in \widehat{\widehat{G}} | \hat{g}(\chi) = 1, \forall \chi \in X\} \cong \{g \in G | \chi(g) = 1, \forall \chi \in X\}$.

Example 2.4. Let $\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q}) \to \mathbb{C}^\times$, defined by $\chi(\sigma_1) = 1$, $\chi(\sigma_5) = -1$, $\chi(\sigma_7) = 1$, $\chi(\sigma_{11}) = -1$, where $\sigma_i : \zeta_{12} \mapsto \zeta_{12}^i$. We notice that $\ker(\chi) = \{\sigma_1, \sigma_7\}$.

$$\begin{array}{cc} \mathbb{Q}(\zeta_{12}) & \{\sigma_1\} \\ | & | \\ \mathbb{Q}(\zeta_3) & \ker(\chi) = \langle \sigma_7 \rangle \\ | & | \\ \mathbb{Q} & G \end{array}$$

We notice that $\sigma_7(\zeta_3) = \zeta_3$, so $\ker(\chi)$ fixes elements of $\mathbb{Q}(\zeta_3)$. In particular by Galois theory, we can see that $\mathbb{Q}(\zeta_3)$ is the fixed field of $\mathbb{Q}(\zeta_{12})$ by $\ker(\chi)$, hence it is the field associated to χ. From this we get that χ is a character of $G/\ker(\chi) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^\times$, and $f_\chi = 3$.

Example 2.5. Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, and take X to be the subset of even characters in $\widehat{G}$. We actually have that X is a subgroup. We notice that X is a subgroup of index 2. We further have that for any $\chi \in X$, $\chi(-1) = 1$, so $\sigma_{-1} \in \ker(\chi)$, for all $\chi \in X$ (where σ_i is defined as in the previous example). As σ_{-1} is simply the complex conjugation, it allows us to deduce that the field fixed by X has to be real.

We know that $\{\sigma_1, \sigma_{-1}\} \subseteq \cap_{\chi \in X} \ker(\chi)$ and we will now show that it is actually an equality.
Assume we have $\sigma_r \in \cap_{\chi \in X} \ker(\chi)$, where $r \neq 1$. We get that for all $\chi \in X$, $\hat{\sigma}_r(\chi) = \chi(\sigma_r) = 1$ and as $\hat{\sigma}_r$ cannot be trivial, there exist $\psi \in \widehat{G}$, such that $\hat{\sigma}_r(\psi) = \psi(\sigma_r) \neq 1$ (where $\hat{\sigma}$ is defined in the proof of Lemma 1.3). By the definition of X, ψ has to be odd, which implies that ψ^2 is even, so $\psi^2(\sigma_r) = 1$ and thus $\psi(\sigma_r) = -1$.
As X has index 2, any odd character can be written as $\psi\chi$, for some $\chi \in X$. This implies that $\tilde{\sigma}_r$ sends any odd character to -1 and any even character to 1, but in that case $\sigma_r = \sigma_{-1}$, and it allows us to conclude. We will later prove that the field associated to X is actually $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, the maximal real field of this extension.

$$\begin{array}{cc} \mathbb{Q}(\zeta_n) & \{1\} \\ | & | \\ \mathbb{Q}(\zeta_n + \zeta_n^{-1}) & \{\sigma_1, \sigma_{-1}\} \\ | & | \\ \mathbb{Q} & G \end{array}$$

We will use the following theorem without proof.

Theorem 2.6 (Conductor discriminant formula)**.** *Let X be a finite group of Dirichlet characters and K its associated number field, then*

$$d_{K/\mathbb{Q}} = (-1)^{r_2} \prod_{\chi \in X} f_\chi,$$

where r_2 is the number of pairs of imaginary embeddings.

3 Enhanced Galois correspondence

Let $K/\mathbb{Q}$ be an abelian extension. Denote $G = \mathrm{Gal}(K/\mathbb{Q})$. We recall the usual Galois correspondence:

$$\begin{array}{cc} K & \{1\} \\ | & | \\ L = K^H & H = \mathrm{Gal}(K/L) \\ | & | \\ \mathbb{Q} & G \end{array} .$$

Let $X_K := \widehat{\mathrm{Gal}(K/\mathbb{Q})}$.

Remark 3.1. Let $K/\mathbb{Q}$ be an abelian extension.
By Kronecker–Weber theorem, there exists a $n \in \mathbb{N}$, such that $K \subseteq \mathbb{Q}(\zeta_n)$.

From Galois theory we know that $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(\zeta_n)/K)$, in particular $K = \mathbb{Q}(\zeta_n)^{\mathrm{Gal}(\mathbb{Q}(\zeta_n)/K)}$.

We get the following new correspondence (where we identify $\mathrm{Gal}(K/\mathbb{Q})$, with $\widehat{\widehat{\mathrm{Gal}(K/\mathbb{Q})}}$):

$$\{\text{Subgroups of } X_K\} \to \{\text{Subfields of K}\}$$
$$Y \mapsto \text{fixed field of } Y^\perp, \text{ denoted } K^{Y^\perp}$$
$$\mathrm{Gal}(K/L)^\perp = X_L \hookleftarrow L$$

To prove the correspondence we first notice that:
$X_L = \widehat{\mathrm{Gal}(L/\mathbb{Q})} = \mathrm{Gal}(\widehat{K/\mathbb{Q})/\mathrm{Gal}(K/L)} = \mathrm{Gal}(K/L)^\perp$.

Let $Y \leq X_K$, and set $L = K^{Y^\perp}$, by usual Galois correspondence we get $Y^\perp = \mathrm{Gal}(K/L)$. This allows us to conclude one direction as $X_L = \mathrm{Gal}(K/L)^\perp = (Y^\perp)^\perp = Y$.

For the other direction, let $\mathbb{Q} \subseteq L \subseteq K$. As $\left(\mathrm{Gal}(K/L)^\perp\right)^\perp = \mathrm{Gal}(K/L)$ we remark that $K^{\left(\mathrm{Gal}(K/L)^\perp\right)^\perp} = K^{\mathrm{Gal}(K/L)} = L$.
We thus get the following enhanced Galois correspondence:

$$\begin{array}{ccc} K & \{1\} & X_K = \widehat{G} \\ | & | & | \\ L = K^H & H = \mathrm{Gal}(K/L) & X_L = H^\perp = \widehat{G/H} \\ | & | & | \\ \mathbb{Q} & G & \{\chi_0\} = G^\perp \end{array}$$

Example 3.2. Let X be the group of even Dirichlet characters, of modulus n. We call K the associated field, and we already know that $K \subseteq \mathbb{Q}(\zeta_n)$ and that K is real.
Let $L \subseteq \mathbb{Q}(\zeta_n)$ be a real subfield, which implies that $\sigma_{-1}|_L = id_L$, i.e $\sigma_{-1} \in X_L^\perp$, or equivalently all elements in X_L are even. This tell us that $X_L \subseteq X$, an we can conclude that $L \subseteq K$ using our enhanced Galois correspondence. This implies that in particular K has to be the maximal real subfield of $\mathbb{Q}(\zeta_n)$.

Remark 3.3. Let X_1, X_2 be groups of Dirichlet characters associated to fields L_1, L_2, then the field associated to the group generated by X_1, X_2 is $L_1 L_2$.
The proof is left as an exercise.

3.1 Ramification via Dirichlet characters

Remark 3.4. We can decompose Dirichlet characters.
Let $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ and $n = \prod_{j=1}^n p_j^{a_j}$. From the Chinese reminder theorem

we get:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{j=1}^{n} \left(\mathbb{Z}/p_j^{a_j}\mathbb{Z}\right)^\times,$$

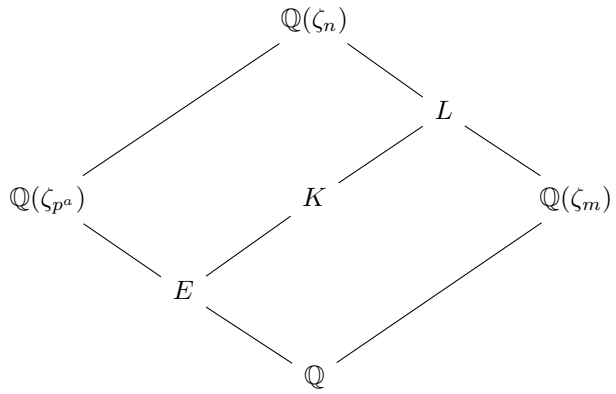
thus we can define χ, by giving a family of $\chi_{p_j} : (\mathbb{Z}/p_j^{a_j}\mathbb{Z})^\times \to \mathbb{C}^\times$.

Definition 3.5. Let X be a group of Dirichlet characters defined modulo n, where $n = \prod_{j=1}^{n} p_j^{a_j}$. We define $X_{p_j} = \{\chi_{p_j} | \chi \in X\}$.

Theorem 3.6. *Suppose X is a group of Dirichlet characters with associated field K. If $p \in \mathbb{Z}$ is prime, then the ramification index of p in $K/\mathbb{Q}$ is $e = |X_p|$.*

Proof. A reminder from algebraic number theory: let $F \subseteq L \subseteq K$ be an extension of number fields. Let $\mathfrak{p} \subseteq \mathcal{O}_F$, a non zero prime ideal, and take $\mathfrak{P}$ a prime ideal in $\mathcal{O}_L$, $\mathfrak{B}$ a prime ideal in $\mathcal{O}_K$ such that $\mathfrak{p} \cdot \mathcal{O}_L \subseteq \mathfrak{P}$ and $\mathfrak{p} \cdot \mathcal{O}_K \subseteq \mathfrak{B}$, then $e(\mathfrak{B}/\mathfrak{p}) = e(\mathfrak{B}/\mathfrak{P}) \cdot e(\mathfrak{P}/\mathfrak{p})$.
Moreover $d_{K/F} = N_{L/F}(d_{K/L}) \cdot d_{L/F}^{[K:L]}$.
Also recall that if $L_1 \cap L_2 = \mathbb{Q}$, where L_1, L_2 two number fields, then $d_{L_1L_2/\mathbb{Q}} = d_{L_1/\mathbb{Q}}^{[L_2:\mathbb{Q}]} \cdot d_{L_2/\mathbb{Q}}^{[L_1:\mathbb{Q}]}$.

We can now begin the proof of the theorem. Let $n = \mathrm{lcm}(f_\chi | \chi \in X)$, then $K \subseteq \mathbb{Q}(\zeta_n)$ and write $n = p^a m$, for some $p \nmid m$.
Let $L = K(\zeta_m)$, we clearly have the following field extension $\mathbb{Q}(\zeta_m) \subseteq L \subseteq \mathbb{Q}(\zeta_n)$.
We now look at $X_L = \widehat{\mathrm{Gal}(L/\mathbb{Q})}$. We notice that it is generated by elements from $\widehat{\mathrm{Gal}(K/\mathbb{Q})} = X$ and $\widehat{\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})}$. Since $(p, m) = 1$, $\widehat{\mathrm{Gal}(L/\mathbb{Q})} = X_p \times \widehat{\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})}$, in particular $L = E\mathbb{Q}(\zeta_n)$, where E is the field corresponding to X_p. Moreover $E \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$, i.e it is a composition of linearly disjoint fields. We get the following diagram:



We also get the following assertions:

- p is unramified in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, since $p \nmid m$.

- Let $\mathfrak{P}$ be a prime over p in $\mathcal{O}_E$, we know that $d_{L/\mathbb{Q}} = d_{E/\mathbb{Q}}^{[\mathbb{Q}(\zeta_m):\mathbb{Q}]} d_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}^{[E:\mathbb{Q}]}$. We also get $d_{L/\mathbb{Q}} = N_{E/\mathbb{Q}}(d_{L/E}) d_{E/\mathbb{Q}}^{[L:E]}$, thus as $[L:E] = [\mathbb{Q}(\zeta_m):\mathbb{Q}]$, we have $N_{E/\mathbb{Q}}(d_{L/E}) = d_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}^{[E:\mathbb{Q}]}$.
  We assume by contradiction that $\mathfrak{P}$ ramifies in L, which is equivalent to $\mathfrak{P}$ dividing $d_{L/E}$. Then, from the definition of the norm, and as $f(\mathfrak{P}/p) \neq 0$, $p | N_{E/\mathbb{Q}}(d_{L/E})$. Form the previous paragraph we get that $p | d_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}^{[E:\mathbb{Q}]}$, which yields a contradiction as p is not ramified in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ thus cannot divide $d_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}^{[E:\mathbb{Q}]}$.
  We recall that for any finite extensions $N \subseteq P \subseteq Q$, and primes $\mathfrak{n}, \mathfrak{p}, \mathfrak{q}$ in N, P, Q respectively, we have $e(\mathfrak{q}/\mathfrak{n}) = e(\mathfrak{q}/\mathfrak{p}) e(\mathfrak{p}/\mathfrak{n})$.
  We now notice that for any prime $\mathfrak{B}$ over $\mathfrak{P}$ in L, we get $e(\mathfrak{B}/\mathfrak{P}) = 1$, thus we also get that for any prime over $\mathfrak{P}$ in K the ramification index is 1. It allows us to conclude that the ramification index for p in $E/\mathbb{Q}$ is the same as the ramification index for p in $K/\mathbb{Q}$.

- p is totally ramified in $\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}$, so p is totally ramified in E.

Hence, the ramification index for p is $[E:\mathbb{Q}] = |\mathrm{Gal}(E/\mathbb{Q})| = |X_p|$. □

Corollary 3.6.1. *Let X be a group of Dirichlet characters, and K the associated field. Then p is unramified in $K/\mathbb{Q}$ if and only if $\chi(p) \neq 0$ for all $\chi \in X$.*

Proof. The prime p is unramified if and only if $|X_p| = 1$, or equivalently if there is no nontrivial character in X with conductor divisible by p, i.e $\chi(p) \neq 0$, for all $\chi \in X$. □

Theorem 3.7. *Let X be a group of Dirichlet characters, and K be the associated field. Let $p \in \mathbb{N}$ be prime. We define*

$$Y = \{\chi \in X : \chi(p) \neq 0\}$$
$$Y_1 = \{\chi \in X : \chi(p) = 1\},$$

and get that

X/Y is isomorphic to the inertia subgroup for p.
X/Y_1 is isomorphic to the decomposition group for p.
X/Y_1 is cyclic of order p.

Example 3.8. Le χ be the generator of $\widehat{\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})}$, let ψ be a generator of $\widehat{\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})}$.
Let K be associated to $\chi^2\psi$ and L to $\langle \chi^2, \psi \rangle$, where we view these characters as elements of $\widehat{\mathrm{Gal}(\mathbb{Q}(\zeta_{20})/\mathbb{Q})}$.
We notice that $\ker(\psi) = \langle \sigma_{13} \rangle$ and $\ker(\chi^2) = \langle \sigma_9, \sigma_{11} \rangle$, so L is the fixed field of $\langle \sigma_9 \rangle$. We also notice that $\ker(\psi\chi^2) = \langle \sigma_3 \rangle$, so $K = \mathbb{Q}(\zeta_{20})^{\langle \sigma_3 \rangle}$. We can compute, using for instance SageMath, that $L = \mathbb{Q}(\sqrt{5}, i)$ and $K = \mathbb{Q}(\sqrt{-5})$.
This implies that L/K is unramified at all primes other than 2 and 5, where we can deduce this result by looking at ramification indices for $L/\mathbb{Q}$ and $K/\mathbb{Q}$ as the extensions are abelian.

- For $K/\mathbb{Q}$, for $p = 2$ or 5, we have $X = \{\chi_0, \chi^2\psi\}$ and $Y = \{\chi_0\}$, thus $e_2 = e_5 = 2$.
- For $L/\mathbb{Q}$, $X = \{\chi_0, \chi^2, \psi, \chi^2\psi\}$.
  for $p = 2$, $Y = \{\chi_0, \chi^2\}$, thus $e_2 = 2$
  for $p = 5$, $Y = \{\chi_0, \psi\}$, thus $e_5 = 2$.

This implies that L/K is actually unramified at every prime: ramification on L/K is $e_{L/\mathbb{Q}}/e_{K/\mathbb{Q}} = 1$.