I. Preliminaries

1 Exact sequences

Def: Let $S: E_1 \xrightarrow{f_1} E_2 \xrightarrow{f_2} E_3 \to \dots \to E_i \xrightarrow{f_i} E_{i+1} \to \dots$ a sequence of groups / rings / R-modules and homomorphisms in the corresponding category.

The sequence S is semi-exact if $\forall i$, $\mathrm{Im}(f_i) \subseteq \mathrm{Ker}(f_{i+1})$.

The sequence S is exact if $\forall i$, $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$.

The sequence S is exact if $\forall i$, $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$.

A short exact sequence is an exact sequence of the form

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

(we replace 0 by 1 if the category is groups).

This means: f is injective, $\mathrm{Im}(f) = \mathrm{Ker}(g)$, g surjective.

· Examples:

a) L/K Galois extension

$$\begin{tikzcd} L \arrow[d, dash] \arrow[dr, dash, "\text{Galois}"] & \\ K \arrow[r, dash] & K' \end{tikzcd} \Rightarrow \mathrm{Gal}(L|K') \leq \mathrm{Gal}(L/K).$$

K'/K is Galois $\iff \mathrm{Gal}(L/K') \trianglelefteq \mathrm{Gal}(L/K)$ in this case

$$1 \to \mathrm{Gal}(L/K') \hookrightarrow \mathrm{Gal}(L/K) \xrightarrow{\pi} \mathrm{Gal}(L/K)/\mathrm{Gal}(L/K') \simeq \mathrm{Gal}(K'/K) \to 1.$$

b) Let L_1/K and L_2/K be Galois $\Rightarrow L_1L_2/K$ is Galois and also $L_1 \cap L_2$. Moreover $\mathrm{Gal}(L_1L_2|K) \simeq \mathrm{Gal}(L_1|K) \times \mathrm{Gal}(L_2|K)$ and

$$\begin{tikzcd} 1 \arrow[r] & \mathrm{Gal}(L_1/L_1\cap L_2) \times \mathrm{Gal}(L_2|L_1\cap L_2) \arrow[r] & \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) \simeq \mathrm{Gal}(L_1L_2|K) \arrow[d] \\ & & \mathrm{Gal}(L_1\cap L_2|K) \arrow[d] \\ & & 1. \end{tikzcd}$$

c) A Dedekind domain, e.g. $\mathcal{O}_K$ or $K[X,Y]/I(V)$, V affine variety. $I(A)$ = group of fractional ideals.

$$1 \longrightarrow \underbrace{A^*}_{\text{inv. elements}} \xhookrightarrow{\text{inc}} K^* \hookrightarrow I(A) \longrightarrow Cl(A) = I(A)/K^* \to 1 \quad \text{exact.}$$

$$\gamma \longmapsto \gamma A$$

Recall: $\zeta \in \overline{\mathbb{Q}}$ n-th primitive root of 1 $\Rightarrow$ $\mathbb{Q}(\zeta)|\mathbb{Q}$ Galois:
$\forall \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$, $\sigma(\zeta)$ is also primitive, $\sigma(\zeta) = \zeta^{\chi(\sigma)}$, $\chi(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^*$

$\Rightarrow$ $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \xrightarrow[\sim]{\chi} (\mathbb{Z}/n\mathbb{Z})^*$ $\Rightarrow$ $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ is abelian, hence Galois.

if $n = p^r n'$, $r \geq 0$, $n' \geq 1$, $(p, n') = 1$ $\Rightarrow$ $\zeta^{n'}$ primitive p^r-th root of 1,

$\mathbb{Q} \subseteq \mathbb{Q}(\zeta^{n'}) \subseteq \mathbb{Q}(\zeta)$,

$$\begin{tikzcd} \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \arrow[r, "\sim"] \arrow[d, "\mathrm{Res}"'] \arrow[dr, phantom, "G"] & (\mathbb{Z}/n\mathbb{Z})^* \arrow[d, "\mathrm{Red}"] \\ \mathrm{Gal}(\mathbb{Q}(\zeta^{n'})|\mathbb{Q}) \arrow[r, "\sim"] & (\mathbb{Z}/p^r\mathbb{Z})^* \end{tikzcd}$$

Since $\mathbb{Q}(\zeta^{n'})$, $\mathbb{Q}(\zeta^{p^r})$ are linearly disjoint (apply b)

$\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta^{n'})|\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta^{p^r})|\mathbb{Q})$.

Goal: (Kr-W)
Let $K|\mathbb{Q}$ be abelian and finite $\Rightarrow$ $\exists \zeta$ primitive root of 1 s.t
$K \subseteq \mathbb{Q}(\zeta)$:

$$\begin{tikzcd} \mathbb{Q}(\zeta) \arrow[dr, dash, "H \triangleleft (\mathbb{Z}/n\mathbb{Z})^*"] \arrow[dd, dash, "(\mathbb{Z}/n\mathbb{Z})^*"'] & \\ & K \\ \mathbb{Q} \arrow[ur, dash, "(\mathbb{Z}/n\mathbb{Z})^*/H"'] & \end{tikzcd}$$

2. Gaussian periods

p odd prime, ζ p-th root of unity, $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \simeq \mathbb{F}_p^*$ cyclic of order $p-1$. There's a 1-1 correspondence between subextensions of $\mathbb{Q}(\zeta)|\mathbb{Q}$ and positive divisors $d | p-1$.

Goal: to give a primitive element for each subextension.

Fix g | $\langle g \rangle = \mathbb{F}_p^*$. σ | $\sigma(\zeta) = \zeta^g$, $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) = \langle \sigma \rangle$

Lem set $\zeta_i = \zeta^{g^i}$ $i \geq 0$. Then $\zeta_i = \zeta_j \Leftrightarrow i \equiv j \bmod p-1$ and
$\sigma^j(\zeta_i) = \zeta_{i+j}$ #

Def: Let $n \mid p-1$, $d = \frac{p-1}{n}$. For each $i \in \{0,1,\dots,n-1\}$, The i-th Gaussian n-period relative to g is $\eta_i = \sum_{j=0}^{d-1} \sigma^{dn}(\zeta_i) = \sum_{j=0}^{d-1} \zeta_{i+jn}$

① **Prop:** $\{\eta_0, \eta_1, \dots, \eta_{n-1}\}$ does not depend on g or on ζ. Moreover, η_0 doesn't depend on g and the η_i's are the η_0's associated to all the primitive roots of unity.

Lem (exerc.) Let $L|K$ be Galois, $\theta \in L$ primitive element $\Rightarrow \forall\, \underset{K}{\underset{\cup\!\shortmid}{K}} \subseteq L$, K is obtained adjoining to K, the coefficients of $\mathrm{Irr}(\theta, K)$.

Now, $K|\mathbb{Q}$ subext of $\mathbb{Q}(\zeta)|\mathbb{Q}$, $n := [K:\mathbb{Q}] \mid p-1$, $K = \mathbb{Q}(\zeta)^H$, $H \leq \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ of index n $\Rightarrow$ K generated by the coeffs of $\mathrm{Irr}(\zeta, K)$.

If $H = \langle \sigma^n \rangle$, $\mathrm{Irr}(\zeta, K) = \prod_{\tau \in H} (x - \tau(\zeta)) = \prod_{j=0}^{d-1} (x - \sigma^{jn}(\zeta))$.

The coeffs are the symmetric polys on $x_j = \sigma^{jn}(\zeta)$, $0 \leq j \leq d-1$. These generate $K \Rightarrow$ so generate the Newton symmetric polys $\left\{ \sum_{j=0}^{d-1} x_j^k \,,\ 0 \leq k \leq n-1 \right\}$

But for $k = g^i$, $\Rightarrow \sum_{j=0}^{d-1} x_j^k = \sum_{j=0}^{d-1} \sigma^{jn}(\zeta)^{g^i} = \sum_{j=0}^{d-1} \sigma^{jn}(\zeta_i) = \eta_i$

$\Rightarrow$ These are the n-th Gaussian periods #

② **Cor:** p odd prime, ζ primitive root of 1, $K \leq \mathbb{Q}(\zeta)$, $n := [K:\mathbb{Q}]$ $\Rightarrow \forall i \in \{0,\dots,n-1\}$, $K = \mathbb{Q}(\eta_i)$. Moreover $\{\eta_0, \eta_1, \dots \eta_{n-1}\}$ are all conjugated.

3. Dirichlet characters

G finite abelian group, $\widehat{G} := \mathrm{Hom}(G, \mathbb{C}^*)$ the complex dual of G.

$\forall\, \chi \in \widehat{G}$, $\mathrm{Im}(\chi) \subseteq \mu_n$ where n is the exponent of G.

(3) <u>Thm</u>: a) $G \simeq \widehat{G}$ non-canonically

b) $G \simeq \widehat{\widehat{G}}$ canonically.

(4) <u>Prop</u> (orthogonality relations). Let G finite abelian of $\mathrm{ord}(G) = g \Rightarrow$

a) $\forall\, \chi \in \widehat{G}$, $\displaystyle\sum_{\sigma \in G} \chi(\sigma) = \begin{cases} g & \text{if } \chi = 1 \\ 0 & \text{othw} \end{cases}$

b) $\forall\, \sigma \in G$, $\displaystyle\sum_{\chi \in \widehat{G}} \chi(\sigma) = \begin{cases} g & \text{if } \sigma = 1 \\ 0 & \text{othw.} \end{cases}$

(5) <u>Prop</u>: Let $0 \to G' \to G \to G'' \to 0$ be an exact seq^n of finite abelian groups $\Rightarrow$ $0 \to \widehat{G''} \to \widehat{G} \to \widehat{G'} \to 0$ exact.

<u>Not</u>: $G(n) := (\mathbb{Z}/n\mathbb{Z})^*$, $\widehat{G(n)} \equiv$ ~~set~~ group of Dirichlet characters modulo n.

(6) <u>Prop</u>: Let $\chi \in \widehat{G(n)}$ be a Dirichlet char. If $\exists\, d_1, d_2 \mid n$ s.t. $\chi: G(n) \xrightarrow{\text{Red}} G(d_i) \xrightarrow{\chi_i} \mathbb{C}^*$

$d := (d_1, d_2) \Rightarrow \exists\, \chi' \in G(d)$ s.t. $\chi: G(n) \xrightarrow{\text{Red}} G(d) \xrightarrow{\chi_d} \mathbb{C}^*$. (Proof pending)

(7) <u>Cor</u>: There exists the smallest $f \geq 1$ s.t. $\chi: G(n) \to G(f) \xrightarrow{\chi_f} \mathbb{C}^*$. such

f is called the <u>conductor</u>.

The characters $\chi \in \widehat{G(n)}$ s.t. $f_\chi = n$ are called "primitive".

- If $\chi \in \widehat{G(n)}$ Dirichlet, can extend: $\chi: \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$

$$a \longmapsto \begin{cases} \chi(a) & \text{if } (a,n) = 1 \\ 0 & \text{othw.} \end{cases}$$

Also: $\chi: \mathbb{Z} \to \mathbb{C}^*$

$$a \longmapsto \chi([a]_n).$$

$\chi_1 \equiv$ trivial character (conductor 1).

If χ_i Dirichlet character of conductor f_i we define $\chi_1\chi_2$:

$\omega: G([f_1,f_2]) \to \mathbb{C}^*$ Consider $\chi_1\chi_2 \equiv$ the primitive Dirichlet

$a \longmapsto \chi_1(a)\chi_2(a)$ character associated to ω.

$\Rightarrow$ We can give the set of all Dirichlet characters the structure of a group with neutrum 1 and $\chi^{-1} = \overline{\chi}$.

• The legendre symbol:

p odd prime. homomorphism $\Rightarrow \left(\frac{*}{p}\right) \in \widehat{G(p)}$

Def: $\left(\frac{*}{p}\right): \mathbb{F}_p^* \to \{\pm 1\}$

$a \longmapsto \left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a = x_0^2 \\ -1 & \text{other} \end{cases}$

it's a quadratic character of conductor p.

8) **Prop**: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$; $\left(\frac{a^2}{p}\right) = 1$; $\left(\frac{a}{p}\right) = 0 \ \forall p|a$, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$.

9) **Prop**: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

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

in part if p or $q \equiv 1 \pmod 4$ $\Rightarrow \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$

4. Gauss sums

χ primitive Dirichlet character mod n, ζ n-th primitive root of 1, $N \geq 1$.

Def: The N-th Gauss sum for χ relative to ζ is

$$G(\chi, N) = \sum_{a \in \mathbb{Z}/n\mathbb{Z}} \chi(a)\zeta^{aN}.$$

($g(\chi, N)$ is for $\zeta = e^{\frac{2\pi i}{n}}$).

10) **Prop**. χ Dirichlet character modulo n, ζ n-th root of unity $\Rightarrow \forall N$,

$$G(\chi, N) = \overline{\chi(N)}\, G(\chi, 1).$$

Proof: supp $(n, N) = 1$. $G(\chi, N) = \sum_{a \bmod n} \chi(aNN')\zeta^{aN} = \overline{\chi(N)}\, G(\chi, 1)$.

$\chi(aNN') = \overline{\chi(N)}\chi(aN)$

otherw, $d := (N, n) > 1$, $N = N'd$, $n = n'd$, $(N', n') = 1$.

Since $\chi(N)=0 \overset{?}{\Longrightarrow} G(\chi,N)=0$:

$$G(\chi,N)=\sum_{a \bmod n} \chi(a)\zeta^{adN'} \underset{\substack{\uparrow \\ 0\le a<n,\ a=n'q+r,\ 0\le r<n',\ 0\le q<d}}{=} \sum_{r \bmod n'} \sum_{q \bmod d} \chi(r+n'q)\zeta^{rdN'} =$$

$$= \sum_{r \bmod n'} \zeta^{rdN'} \sum_{q \bmod d} \chi(n'q+r)$$

χ primitive mod $n \Rightarrow \mathrm{Ker}\left[G(n) \xrightarrow{\mathrm{Red}} G(n')\right]$ cannot be included in $\mathrm{Ker}(\chi)$ (exercise)

$\Rightarrow \exists c \in G(n)$, $c \equiv 1 \bmod n'$ | $\chi(c) \neq 1$.

$\Rightarrow \forall$ fixed r, the subset of $G(n)$ of the elements $cn'q+cr$, $0\le q<d$ is the same as $\{n'q+r\}$ $\Rightarrow \sum_{q \bmod d} \chi(n'q+r) = \sum_{q} \chi(c)\chi(n'q+r)$

$\Longrightarrow G(\chi,N) = \underset{\substack{\neq \\ 1}}{\chi(c)}\, G(\chi,N) \Rightarrow G(\chi,N)=0$ #.

(11) <u>Prop</u>: $|G(\chi,N)|=\sqrt{n}$. (if $((N,n)=1)$)

<u>Proof</u>: $|G(\chi,1)|=|G(\chi,N)|$ hence enough to assume $N=1$.

$$|G(\chi,1)|^2 = G(\chi,1)\overline{G(\chi,1)} = G(\chi,1)\sum_{a \bmod n}\overline{\chi(a)}\zeta^{-a} = \sum_a G(\chi,a)\zeta^{-a} = \sum_a\sum_b \chi(b)\zeta^{a(b-1)}$$

$$= \sum_b \chi(b)\sum_a \zeta^{a(b-1)} \underset{\uparrow}{=} \chi(1).n = n. \ \#$$

If $b \not\equiv 1 \bmod n \Rightarrow \sum_a \zeta^{a(b-1)} = 0$ If $b\equiv 1 \bmod n$, $\zeta^{a(b-1)}=1$

(12) <u>Cor</u>: χ quadratic Dirichlet, primitive mod $n \Rightarrow G(\chi,1)^2 = \chi(-1)n$.

<u>Proof</u>: $$G(\chi,1)^2 = G(\chi,1)\sum_a \chi(a)\zeta^a \underset{\substack{\uparrow \\ \chi(a)=\overline{\chi}(a)}}{=} \sum_a G(\chi,a)\zeta^a = \sum_a\sum_b \chi(b)\zeta^{a(b+1)} =$$

$$= \sum_b \chi(b)\sum_a \zeta^{a(b+1)} = \chi(-1).n \ \#$$