Lecture 11 The Legendre symbol

Defn Given an odd prime p, the Legendre symbol is the map

$$\mathbb{Z} \longrightarrow \{-1, 0, 1\}$$

$$x \longmapsto \left(\frac{x}{p}\right) := \begin{cases} 1, & \text{if } \exists\, y \in \mathbb{Z} \text{ s.t. } y^2 \equiv x \pmod p \\ & \text{\& } x \not\equiv 0 \pmod p \\ -1, & \text{if } \nexists\, y \in \mathbb{Z} \text{ s.t. } y^2 \equiv x \pmod p \\ & \text{\& } x \not\equiv 0 \pmod p \\ 0 & \text{if } x \equiv 0 \pmod p \end{cases}$$

Prop 1 If K is a field and $G \leq K^\times$ is a finite subgroup, then G is cyclic.

Proof

As G is finite & abelian then* $G \cong C_{d_1} \times C_{d_2} \times \dots \times C_{d_s}$, where

$d_1 \mid d_2 \mid \dots \mid d_{s-1} \mid d_s$ and C_d denotes the cyclic group of order d.

Hence

$$\forall x \in G : x^{d_s} = 1.$$

i.e. $G \subseteq \{x \in K : f(x) = 0\}$, where $f(X) := X^{d_s} - 1$. Therefore

$|G| = d_1 \cdot d_2 \cdot \dots \cdot d_s \leq \deg f = d_s$, so $d_1 = d_2 = \dots d_{s-1} = 1$

and thus $G \cong C_{d_s}$ □

* Gen: F.G. torsion R-module, where R is a PID.

Prop 2 Let $F = \mathbb{F}_{p^d}$, p odd. We have a group homomorphism

$$F^\times \xrightarrow{\psi} F^\times$$

$$x \longmapsto x^{\frac{p^d-1}{2}}.$$

such that

(i) $\mathrm{Im}(\psi) = \{-1, 1\}$

(ii) $\mathrm{Ker}(\psi) = (F^\times)^2$

and $\forall\ a \in \mathbb{F}_p{}^\times$ we have $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$.

Proof

For $a \in F^\times$ $\exists\, \alpha \in E$ s.t. $\alpha^2 = a$, so (α : $\star$)

$$a \in (F^\times)^2 \iff \alpha \in F^\times \iff \alpha^{p^d - 1} = 1$$

But each $a \in F^\times$ is a zero of the polynomial

$$X^{p^d-1} - 1 = \left(X^{\frac{p^d-1}{2}} - 1\right)\left(X^{\frac{p^d-1}{2}} + 1\right) \qquad *$$

$$\alpha^{p^d-1} \overset{(\star)}{=} \underbrace{a^{\frac{p^d-1}{2}}}_{=:\psi(a)} \overset{(*)}{=} \pm 1,$$

so $\mathrm{Im}(\psi) \subseteq \{-1, 1\}$ and also $\ker(\psi) = (F^\times)^2$.

But $F^\times$ is cyclic of even order. Hence $|F^\times/(F^\times)^2| = 2$,

so we have

$$\begin{array}{ccc} F^\times & \xrightarrow{\psi} & F^\times \\ & \overset{\hat{\psi}}{\nearrow} & \uparrow \\ \pi \downarrow & & \\ F^\times/(F^\times)^2 & \xrightarrow{\sim} & \{-1, 1\} \end{array}$$

and thus $\mathrm{Im}(\psi) = \{-1, 1\}$. In particular, for $F = \mathbb{F}_p$ we have $\forall\ a \in \mathbb{F}_p$

$$\left(\frac{a}{p}\right) = \psi(a) = a^{\frac{p-1}{2}} \qquad \square$$

Let p be an odd prime and pick a field F.

Let E be the splitting field of the polynomial $f_p(x) := X^p - 1$ over F and define

$$\mu_p := \{ x \in E : x^p = 1 \}$$

Assume that $\chi(F) \neq p$ so that μ_p has exactly p elements.

Example Let $F = \mathbb{Q}$. Then we may embed the s.f. $E \hookrightarrow \mathbb{C}$ and $\zeta = e^{2\pi i/p} \in \mathbb{C}$ generates μ_p.

More generally, as $\mu_p \subseteq E^\times$ and $|\mu_p| < \infty$, then Prop 1

$\Rightarrow \exists\, \zeta \in \mu_p$ s.t. $\mu_p = \{\zeta, \zeta^2, \dots, \zeta^{p-1}\}$. Define the Gauss sum

$$S_p := \sum_{k \in \mathbb{F}_p} \left(\frac{k}{p}\right) \zeta^k \in E.$$

Remark We'll use Gauss sums $/\mathbb{F}_\ell$, where ℓ is an odd prime $\neq p$.

Lemma 3 Notation as above $S_p^2 = \left(\frac{-1}{p}\right) p$

Proof

$$S_p^2 = \left(\sum_j \left(\frac{j}{p}\right)\zeta^j\right)\left(\sum_k \left(\frac{k}{p}\right)\zeta^k\right) = \sum_j \sum_k \left(\frac{j}{p}\right)\left(\frac{k}{p}\right)\zeta^j\zeta^k =$$

perm. $(k \mapsto jk)$

$$\sum_j \sum_k \left(\frac{jk}{p}\right)\zeta^{j+k} = \sum_j \sum_k \left(\frac{j\,jk}{p}\right)\zeta^{j+jk} =$$

$$\sum_j \sum_k \left(\frac{j^2 k}{p}\right)\zeta^{j(1+k)} = \sum_j \sum_k \left(\frac{k}{p}\right)\zeta^{j(1+k)}$$

Hence

$$S_r = \sum_j \sum_k \left(\frac{k}{p}\right) \zeta^{j(1+k)} =$$

$$\sum_j \sum_{k \neq -1} \left(\frac{k}{p}\right) \zeta^{j(1+k)} + \sum_j \left(\frac{-1}{p}\right) \zeta^0 =$$

$$\sum_{k \neq -1} \left(\frac{k}{p}\right) \underbrace{\sum_j \left(\zeta^{1+k}\right)^j}_{\| \; 0} + \sum_j \left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right) \sum_j 1 = \left(\frac{-1}{p}\right) r$$

[use Viète's formula.]

□

Lemma 4 Fix a prime $\ell \neq p$ and consider the Gauss sum S_p over $\mathbb{F}_\ell$. Then

$$S_p^{\ell} = \left(\frac{\ell}{p}\right) S_p$$

Proof

$(k = r\ell^{-1})$

$$S_p^{\ell} = \left(\sum_{k \in \mathbb{F}_p} \left(\frac{k}{p}\right) \zeta^k\right)^{\ell} = \sum_k \left(\frac{k}{p}\right) \zeta^{k\ell} = \sum_r \left(\frac{r\ell^{-1}}{p}\right) \zeta^r =$$

$$\sum_r \left(\frac{r}{p}\right)\left(\frac{\ell^{-1}}{p}\right) \zeta^r = \sum_r \left(\frac{r}{p}\right)\left(\frac{\ell}{p}\right)^{-1} \zeta^r = \left(\frac{\ell}{p}\right) S_p \quad \square$$

Thm 5 (Gauss) If p and l are distinct, odd primes then

$$\left(\frac{p}{l}\right)\left(\frac{l}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{l-1}{2}}$$

Proof

$$\left(\frac{l}{p}\right) = \left(S_p^2\right)^{\frac{l-1}{2}} = \left(\left(\frac{-1}{p}\right)p\right)^{\frac{l-1}{2}} = \left(\frac{-1}{p}\right)^{\frac{l-1}{2}} p^{\frac{l-1}{2}} = \left((-1)^{\frac{p-1}{2}}\right)^{\frac{l-1}{2}} \left(\frac{p}{l}\right)$$

By Lemma 4 ↑

By Lemma 3 ↓

By Prop 2 ↓

$$= (-1)^{\frac{p-1}{2}\cdot\frac{l-1}{2}} \left(\frac{p}{l}\right)$$

□

Let l be a prime number > 2 and let $E := sf\, f(X) / \mathbb{F}_l$, where $f(X) = X^8 - 1$. Recall that

$$\mu_8 := \{ x \in E : x^8 = 1 \}$$

is a cyclic subgroup of $E^\times$. So let $\zeta \in \mu_8$ be a generator of μ_8.

We'll prove the following.

Propn 6 The element $\alpha := \zeta + \zeta^{-1}$ is s.t. $\alpha^2 = 2$.

Proof

Note that $f(X) = (X^4-1)(X^4+1)$. So the roots of the first factor are the elements of μ_4. So the primitivity of ζ implies that ζ is a root of the second factor $\Phi_8(X) = X^4+1$,

thus

$$\zeta^{-2}(\zeta^4+1) = 0$$

$$\zeta^2 + \zeta^{-2} = 0$$

and then

$$\alpha^2 = (\zeta+\zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = 2 \qquad \square$$

Prop 7 If we further assume that $\ell \equiv \pm 1 \pmod 8$, then

(a) $$\alpha^\ell = \alpha$$

(b) $$\left(\frac{2}{\ell}\right) = 1$$

Proof

Note that $\ell \equiv \pm 1 \pmod 8 \Rightarrow \zeta^\ell = \zeta^{8k \pm 1} = \zeta^{8k}\zeta^{\pm 1}$

$= (\zeta^8)^k \zeta^{\pm 1} = 1^k \zeta^{\pm 1} = \zeta^{\pm 1}$. Therefore

$$\alpha^\ell = \left(\zeta + \zeta^{-1}\right)^\ell = \zeta^\ell + \zeta^{-\ell} = \zeta^{\pm 1} + \zeta^{\mp 1} = \alpha$$

if $\ell \equiv \pm 1 \pmod 8$. Therefore

$$\left(\frac{2}{\ell}\right) \equiv \left(\alpha^2\right)^{\frac{\ell-1}{2}} = \alpha^{\ell-1} = 1 \qquad \square$$

Prop 8 If $\ell \equiv \pm 3 \pmod 8$, then

(a) $$\alpha^{\ell} = -\alpha$$

(b) $$\left(\frac{2}{\ell}\right) = -1$$

Proof

[Ex]

Corollary For each odd prime ℓ we have $\left(\frac{2}{\ell}\right) = (-1)^{\frac{\ell^2-1}{8}}$.

Remark. The above formula is known as the Second Supplement to the Quadratic Reciprocity Law.

$$\left(\frac{359}{691}\right) = (-1)^{\frac{358}{2}\cdot\frac{690}{2}}\left(\frac{691}{359}\right) = -\left(\frac{332}{359}\right) = -\left(\frac{2^2}{359}\right)\left(\frac{83}{359}\right)$$

$$= -\left(\frac{83}{359}\right) = -(-1)^{\frac{82}{2}\cdot\frac{358}{2}}\left(\frac{359}{83}\right) = \left(\frac{27}{83}\right) = \left(\frac{3}{83}\right)$$

$$= (-1)^{\frac{2}{2}\cdot\frac{82}{2}}\left(\frac{83}{3}\right) = -\left(\frac{2}{3}\right) = -(-1)^{\frac{3^2-1}{8}} = 1$$