

(1)

4/11/11

## Reciprocity laws

The law of quadratic reciprocity has fascinated mathematicians for over 300 years. Its application & analogues plays central part in number theory. This is going to be an elementary introduction to "What is the general reciprocity problem"?

Let  $f = T^n + c_{n-1}T^{n-1} + \dots + T_0$ ,  $c_i \in \mathbb{Z}$  be a monic polynomial. Suppose that  $f$  is irreducible

e.g.  $T^2 + 1$ ,  $T^3 - T - 1$

In fact Selmer proved that  $T^n - T - 1$  is irred for every  $n > 1$ .

Let  $p$  be a prime &  $f_p(x) :=$  reducing coeff. of  $f(x)$  modulo  $p$ .

$\text{Spl}(f) = \{ p \mid f_p(x) \text{ splits into distinct linear factors} \}$

The general reciprocity problem we shall be considering "Given  $f(x)$  as above, describe the factorisation of  $f_p(x)$  as a function of the prime  $p$ ".

Ask for less: Give a rule to determine which primes belong to  $\text{Spl}(f)$ .

Let us see how "Quadratic reciprocity law" gives "reciprocity law" above.

Quadratic: For a quad. poly  $f(x)$ ,

- ①  $f_p(x) = l(x)$  where  $l(x)$  is linear
- ②  $f_p(x) = l_1(x)l_2(x)$  where  $l_i$ 's are linear
- ③  $f_p(x)$  remains irred modulo  $p$ .

②

We consider the poly. of the form  $x^2 - q$  where  $q$  is a prime. Then  $x^2 - q$  splits completely modulo  $p$  if  $\left(\frac{q}{p}\right) = +1$  & remains irreducible if  $\left(\frac{q}{p}\right) = -1$

$$\therefore p \in \text{Spl}(f) \Leftrightarrow \left(\frac{q}{p}\right) = +1$$

Since there are infinitely many primes, to describe  $\text{Spl}(f)$  we need infinite amount of work by above method. If somehow  $\left(\frac{q}{p}\right)$  is related to  $\left(\frac{p}{q}\right)$  then we are done since there are only finitely many residue classes modulo  $q$ . This is given by,

"Quadratic reciprocity law": (Legendre)

For  $p$ , an odd prime

$$1. \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$

$$2. \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

$$3. \text{ If } q \text{ is another odd prime, distinct from } p \text{ then } \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right)$$

Theorem: If  $q \equiv 1 \pmod{4}$  then  $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$

$$\text{ ' } q \equiv 3 \pmod{4} \text{ then } \begin{cases} \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \text{ if } p \equiv 1 \pmod{4} \\ \left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) \text{ if } p \equiv 3 \pmod{4} \end{cases}$$

$$\text{ e.g. } q=17 \text{ then } \text{Spl}(x^2-17) = \left\{ p \mid \left(\frac{p}{17}\right) = +1 \right\}$$

$$\text{ i.e. } p \equiv 1, 2, 4, 8, 9, 13, 15, 16 \pmod{17}$$

$\therefore$  Splitting of  $x^2 - a$  is given by congruence cond<sup>n</sup> (3) modulo a no. that is dependent on  $f(x)$ .

### Cyclotomic polynomials:

Suppose  $\zeta$ : a primitive  $n^{\text{th}}$  root of unity  
Then the minimal poly of  $\zeta$  can be written as  $\Phi_n(x)$  which is of deg  $\phi(n)$ . Also,

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

e.g.  $\Phi_1(x) = x - 1$ ,  $\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$

### Theorem (Cyclotomic reciprocity law)

The cyclotomic poly  $\Phi_n(x)$  factors into distinct linear factors modulo  $p \iff p \equiv 1 \pmod{n}$ .

$\therefore \text{Spl}(f)$  is given by congruence cond<sup>n</sup> depending upon  $f$ .

### Abelian polynomials

A nice description of  $\text{Spl}(f)$  is not always possible. But, one can characterise for which polynomials congruence cond<sup>n</sup> gives the result.

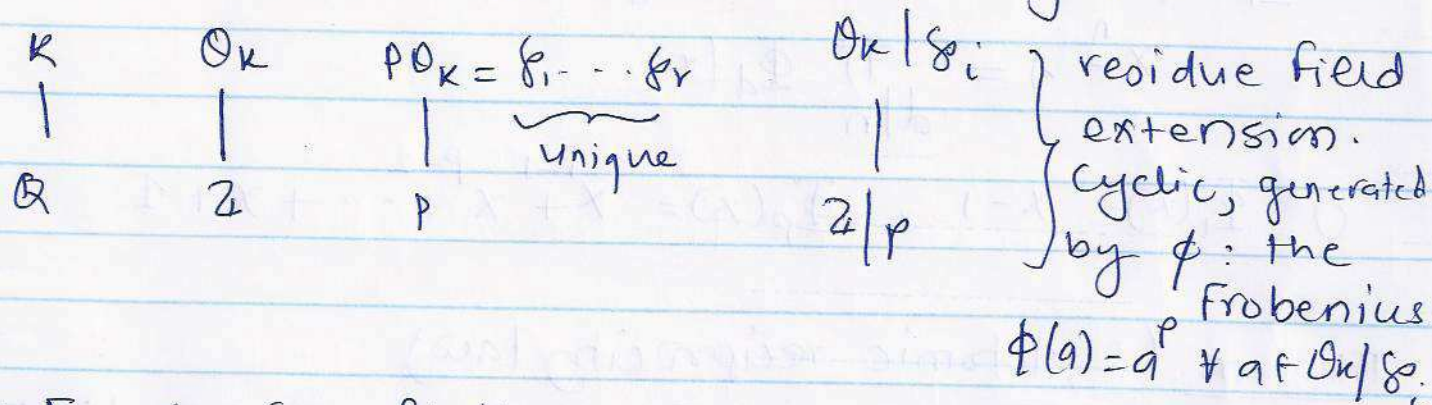
- Let  $K_f = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$  where  $\alpha_i \in \mathbb{C}$  are roots of  $f$   
We call it a root field (= splitting field of  $f$ )
- $f$  is abelian if  $\text{Gal}(K_f/\mathbb{Q})$  is abelian.

Abelian polynomial theorem: The set  $\text{Spl}(f)$  can be described by congruences w.r.t a modulus depending only on  $f \iff f(x)$  is an abelian polynomial.

(2)

Proof of this theorem involves almost all of class field theory over  $\mathbb{Q}$ .

Let me get to more useful statement by giving a sketch of how to prove the sufficiency part.



- Except for finitely many primes called (ramified primes) the  $\mathfrak{f}_i$ 's appearing in  $p\mathcal{O}_K$  are all distinct.

- If  $K/\mathbb{Q}$  is a Galois ext<sup>n</sup> &  $p$  is a prime that is not ramified then for each  $\mathfrak{f}_i$  there is a unique  $\sigma \in G$  s.t  $\sigma$  reduces to the Frobenius modulo  $\mathfrak{f}_i$ . We denote it by  $\sigma_{\mathfrak{f}_i}$ .

The Artin symbol corresponding to  $p$  is given by

$$\sigma_p(a) = a^f \pmod{\mathfrak{f}} \quad \forall a \in \mathcal{O}_K$$

- We know that all  $\sigma_p$ 's corresponding to a single  $p$  are conjugates.

- If  $\text{Gal}(K/\mathbb{Q})$  is abelian then the conj. class is represented by a unique member, called

Artin symbol of  $p$ ,  $\sigma_p \in G$

(5)

- let  $\Gamma \subseteq \mathbb{Q}^\times$  be the free abelian gp generated by the primes. Then Artin symbol gives a homomorphism  $\sigma: \Gamma \rightarrow G$  by extending  $\sigma_p = \cdot \sigma_p \cdot \sigma_q$  &  $\sigma_a = \sigma_p^{-1}$  for  $a = 1/p$ .

' $\sigma$ ' is called the Artin map.

- Ray group :  $\Gamma_a = \left\{ \frac{c}{d} \in \mathbb{Q}^\times \mid c \& d \text{ are primes } \& \right.$   
 $\left. c \equiv d \pmod{a} \right\}$   
 where  $a = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_s^{e_s}$ , where  $p_i$ 's are ramified primes &  $e_i$ 's  $\geq 1$ .

Artin reciprocity law: let  $K/\mathbb{Q}$  be a finite Galois abelian extn with the Galois group  $G$ . let  $\Gamma$  be the subgroup of  $\mathbb{Q}^\times$  as above. Then the Artin map  $\sigma: \Gamma \rightarrow G$  is surjective, whose kernel contains the ray group  $\Gamma_a$ , where  $a$  is an appropriate product of the ramified primes.

Artin reciprocity together with the following lemma will prove: If  $f(x)$  is an abelian poly, then  $\text{Spl}(f)$  can be described by congruence conditions.

Lemma: Suppose  $f(x)$  is an abelian poly. with root field  $K$ , Galois gp  $G$  & Artin map  $\sigma: \Gamma \rightarrow G$ . Then except for finitely many exceptional primes  $f(x)$  splits modulo  $p \iff \sigma_p$  is trivial.

$\therefore \text{Spl}(f)$  contains all primes  $p$  such that  $p \equiv 1 \pmod{a}$  with at most finitely many exceptions.

### General polynomial

If  $f(x)$  is an irred. poly in  $\mathbb{Z}[x]$  which is non-abelian then the best statement one can make is about the relative size of  $\text{Spl}(f)$

Let  $\pi :=$  set of all primes and

$$T \subseteq \pi, \quad x \in \mathbb{R} \quad \text{s.t.} \quad x \geq 1$$

$$\text{Let } \delta(T, x) = \frac{\#\{p \in T \mid p < x\}}{\#\{p \in \pi \mid p < x\}}$$

Defn: If  $\lim_{x \rightarrow \infty} \delta(T, x) = \delta(T)$  then  $T$  has density  $\delta(T)$

Dirichlet's theorem: If  $\frac{1}{m}$

Suppose  $m$  is a positive integer &  $a$  is any integer prime to  $m$  then the set of all primes congruent to  $a \pmod{m}$  has density equal to  $1/\phi(m)$

Weak Chebotarev theorem: let  $f(x)$  irred. poly in  $\mathbb{Z}[x]$  with root field  $K_f$  & suppose that  $[K_f : \mathbb{Q}] = n$ . Then  $\text{Spl}(f)$  has density  $= 1/n$

Check: This implies Dirichlet's theorem when  $f = \Phi_m$

- Let  $N_p(f) =$  no. of roots of  $f$  in  $\mathbb{F}_p$ .

The fundamental insight of Langlands was that there is a "formulae" for  $N_p(f)$  for every poly.  $f$  abelian or not.

① e.g (Serre)  $f = T^3 - T - 1$ ,  $\text{Gal}(K/\mathbb{Q}) \cong S_3$   
 $\therefore f$  is not abelian.

Then  $N_p(f) = 1 + a_p$  where  $a_n$ 's are coefficients of the formal power series

$$q \prod_{k=1}^{\infty} (1 - q^k) (1 - q^{23k}) = q - q^2 - q^3 + q^6 + q^8 - \dots$$

It follows that  $a_p \in \{-1, 0, 2\}$

We thus have a formula for  $N_p(T^3 - T - 1)$  which constitutes a "reciprocity law for  $T^3 - T - 1$ ".

② There are reciprocity laws even for  $f \in \mathbb{Z}[s, t]$  such as

$$f = s^2 + s - T^3 + T^2$$

fact:  $N_p(f) = p - a_p$  where  $a_n$ 's are coeff. of the formal power series

$$q \prod_{k=1}^{\infty} (1 - q^k)^2 (1 - q^{11k})^2 = 0 + 1 \cdot q + \sum_{n \geq 2} c_n q^n$$

By exploring properties of these  $a_p$ 's, Langlands, Wiles, and others (Diamond, Taylor,

- Conrad, ... ) have proved the equalities of Artin L-functions & Hecke L-functions for elliptic curves. This equality encapsulate the "reciprocity law". They proved that are valid

" Similar formulae for  $N_p(t)$ , such equality of L-functions are valid for each of the infinitely many  $f \in \mathbb{Z}[s, t]$  which defines an elliptic curve; there by setting a conjecture of Shimura, Taniyama & Weil.

Among all instances of Langlands' program at its most basic level, reciprocity law is a search for patterns in the sequence  $N_p(f)$  for fixed but arbitrary  $f$ .

Langlands predicted that there is a "reciprocity law" for  $f$  as soon as we can give an embedding  $\rho : Gal(K_f/a) \rightarrow GL_d(\mathbb{C})$

$\rightarrow d=1$  is a class field theory

Essentially the only known cases are  
 $d=2$  &  $\rho(G_f)$  is solvable (Langlands + Tunnell)  
 $d=2$  &  $\rho(G)$  is not of the form  $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$  for any  $a \in \mathbb{C}^*$  when  $c \in G_f$  sending  $x+iy \mapsto x-iy$ . (Khare + Wintenberger + Kisin)