Quadratic Reciprocity in a Polynomial Ring

5/7/24

K = field $\quad K[t] \quad$ Euclidean Domain

$p, q \in K[t] \quad p$ prime

$\left(\frac{q}{p}\right) = 1$ means q is a square mod p

K finite $\quad$ Artin: $\quad \left(\frac{q}{p}\right) = 1$ iff $\left(\frac{p^*}{q}\right) = 1$

$p^* = (-1)^{|p|} p \qquad |p| = \deg p \qquad p \neq q$ primes

If K is infinite this isnt always true

K = number field $\qquad q \in K[t]$ prime odd degree fixed

When is

$$\left(\frac{q}{p}\right) = 1 \implies \left(\frac{p^*}{q}\right) = \underline{1}$$

for <u>all</u> <u>primes</u> $p \neq q$.

$k = \mathbb{Q}$ not all q work

$q = t^3 - 4 \qquad p = t - 2$

$q(t) \equiv 2^2 (t-2) \qquad t^3 - 4 - 4 = (t-2)(t^2+2t-4)$

$2 \cdot t \not\equiv \square \; (t^3-4) \qquad t = 3 \qquad \left(\frac{-1}{23}\right) = -1.$

On the other hand

$q = t^3 + 4$ works.

Gauss $\underline{2^{nd}}$ Proof of quadratic reciprocity: Inspiration

$n \in k[t]$ positive if leading coefficient

of n^* is in $k^{\cdot 2}$.

$n < 0$ means $-n > 0$

$Q = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \longrightarrow ax^2 + 2bxy + cy^2$

$= (a, b, c)$

$a, b, c \in K[t]$

$d = b^2 - ac$

$M \in SL(2, K[t])$ $\quad Q|M = MQM^t$

Suppose $d < 0$ monic $\quad$ $\underline{a > 0}$

square-free

Q_d = set of all such Q

$(1, 0, -d) \in Q_d$ $\quad$ Q_d splits into classes

Set of classes $= C_d$.

Thm 1 $\quad q \in \mathbb{K}[t]$ fixed prime odd degree

Then the following holds

iff C_q is finite

$$\left(\frac{q}{p}\right) = 1 \implies \left(\frac{p^*}{q}\right) = 1 \quad \forall p \neq q$$

Ideas 1) C_d is a group under composition abelian.

2) Count Elements of order 2.

$(a, 0, c) \qquad -ac = d$

ambiguous forms vs

Define Genus characters.

"If" part similar to Gauss

"Only If" Part uses analogue of Gauss's Principal Genus Theorem.

C_d^2 = classes killed by all genus characters.

$b^2 - ac$ Property: finitely many $n \in \mathbb{Z}$ $|n| \leq N$

Apply Theorem of Milnor on with ring of $K(t)$ which characterizes it in terms of $F_p = K[t]/(p)$ $\forall p$

Other Part:

If C_d is infinite there exists a $c \in C_d$ not a square.

True since C_d is finitely generated by Mordell-Weil.

Show C_d is isomorphic to the Divisor Class group of hyperelliptic curve determined by $s^2 = d(t)$.

Jacobi, Mumford, D. Cantor.

Hilbert irreducibility Thm.

$s^2 = t^3 - 4$ rank 1

$s^2 = t^3 + 4$ rank 0

- Redei Richert :

D fund discriminant

$D = D_1 D_2$ $\qquad D_i$ fund.

$\left(\frac{D_1}{p}\right) = 1 \quad \forall p \mid D_2$

$\left(\frac{D_2}{p}\right) = 1 \quad \forall p \mid D_1$

<u>Thm 2</u> K number field $d \in K[t]$
square-free odd degree.

T = torsion group of Jacobian
of $s^2 = d(t)$.

e_4 = # cyclic factors order 2^n $n \geq 2$
in decomposition of T. Then

2^{e_4} is the number of decompositions
$d = d_1 d_2$ d_1, d_2 monic
$(\deg d_2)$ odd $\left(\frac{d_1}{p}\right) = 1$ $\forall p \mid d_2$
and $\left(\frac{-d_2}{p}\right) = 1$ $\forall p \mid d_1$

$$b^2 - ac = d$$

Sketch

Reduction Theory

Unique $(a,b,c) = \varphi$ disc d

$$|b| < |a| < \tfrac{1}{2}|d|$$

a^* monic.

Composition ala Dedekind

Steinberg Symbol — Hilbert symbol

$$F_p = K[t]/(p) \qquad a, b \in K(t)^*$$

$$(a,b) = (-1)^{v_p(a)\, v_p(b)} \quad a^{v_p(b)} \quad b^{v_p(a)}$$

$$\in F_p^* / F_p^{*2}$$

$$a = p^{v_p(a)}\, u$$

$$p \nmid u$$

$$(a,b)_\infty \quad " \quad "$$

Genus Character

$$Q(x,y) = n \qquad n \text{ prime to } p$$

$$\chi_p(Q) = (n,d)_p$$

$$Q\left(\frac{x}{z}, \frac{y}{z}\right) = 1 \qquad x, y, z \in k[t]$$

$$Q(x, y) = z^2$$