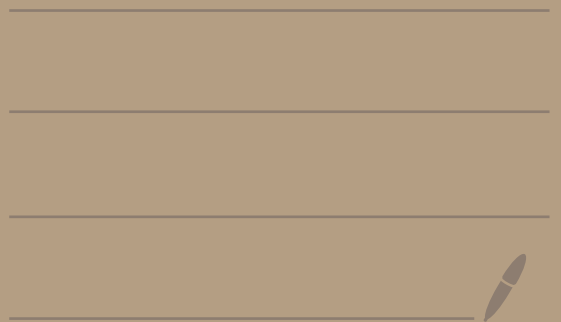


Quadratic Reciprocity in a Polynomial Ring

5/7/24



$K = \text{field}$ $K[t]$ Euclidean Domain

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

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

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

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

If K is infinite this isn't always true

$K = \text{number field}$ $q \in K[t]$ prime odd degree
fixed

When is

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

for all primes
 $p \neq q$.

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

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

$$q(t) = 2^2 (t - 2)$$

$$t^3 - 4 - 4 = (t - 2)(t^2 + 2t - 4)$$

$$2 - t \nmid (t^3 - 4)$$

$$t = 3 \quad \left(\frac{-1}{23} \right) = -1.$$

On the other hand

$$q = t^3 + 4 \text{ works.}$$

Gauss 2nd Proof of quadratic reciprocity: Inspiration

$n \in k[t]$ positive if leading coefficient
of n^* is in $k^{\times 2}$.

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

$$Q = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \rightarrow ax^2 + 2bxy + cy^2 \\ = (a, b, c)$$

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

$$d = b^2 - ac$$

$$M \in SL(2, K[t])$$

$$Q|_M = M Q M^t$$

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

Q_d = set of all such Q

$$(1, 0, -d) \in Q_d$$

Q_d splits into classes
set of classes = C_d .

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

Then the following holds

iff C_q is finite

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

Idea 1) C_d is a group under composition
abelian.

2) Count Element, of order 2.

$$(a, 0, c)$$

$$-ac = d$$

ambiguous forms vs

Define Genus characters.

"If" part similar to Gauss

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

C_2^2 = classes killed by all genus
characters.

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

Appl's Theorem of Milnor on Witt ring
of $K(t)$ which characterizes
it in terms of $F_p = K[t]/(p) \quad \forall p$

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, P. Confor.

Hilbert irreducibility Thm.

$$S^2 = t^3 - 4 \quad \text{rank } 1$$

$$S^2 = t^3 + 4 \quad \text{rank } 0$$

• Reier Riehart :

D fund discriminant

$$D = D_1 D_2 \quad D_i \text{ fund.}$$

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

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

Thm 2 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

$|d_2'|$ odd $\left(\frac{d_1}{p}\right) = 1$ $\nexists p \mid d_2$
and $\left(-\frac{d_2}{p}\right) = 1$ $\nexists p \mid d_1$

$$b^2 - ac = d$$

Sketch

Reduction

Unique

Theory

$$(a, b, c) = 4$$

disc d

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

a^* monic.

Composition also Dedekind

Steinberg Symbol — Hilbert Symbol

$$F_p = K[t]/(p)$$

$$a, b \in K[t]^*$$

$$(a, b) = t^{\nu_p(a)} \quad \nu_p(a) \quad \nu_p(b) \quad a^{\nu_p(b)} \quad b^{\nu_p(a)}$$

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

$$a = p^{\nu_p(a)} u$$

$$p \nmid u$$

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

Genus Character

$$Q(x, y) = n$$

n prime to p

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

$$Q\left(\frac{x}{z}, \frac{y}{z}\right) = 1$$

$$x, y, z \in k[t]$$

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