Constructing Number Fields and Function Fields with Prescribed Class Group Properties

Allison M. Pacelli
Williams College

October 31, 2006

Preliminaries

$q =$ a power of an odd prime

$\mathbb{F}_q =$ the finite field with q elements.

$T =$ any transcendental element over $\mathbb{F}_q$

$$A = \mathbb{F}_q[T] \longleftrightarrow \mathbb{Z}$$

$$k = \mathbb{F}_q(T) \longleftrightarrow \mathbb{Q}$$

$k =$ the *rational function field*

If K is any finite extension of k, then K is called a *global function field.*

Just like in the integers, there is one more prime in k in addition to the "finite" primes or monic, irreducible polynomials.

Prime at Infinity:

$$\infty = \text{localization of } \mathbb{F}_q\left[\frac{1}{T}\right] \text{ at } \frac{1}{T}$$

$$\begin{aligned} \mathrm{ord}_\infty\left(\frac{f}{g}\right) &= \deg(g) - \deg(f) \\ |f|_\infty &= q^{\deg(f)} \\ A_\infty &= \left\{\frac{f}{g} \;\middle|\; \deg(g) \geq \deg(f)\right\} \end{aligned}$$

The Ideal Class Group

$$\begin{array}{ccccccc} \mathcal{O}_K & \subset & K & \qquad & \mathcal{O}_K & \subset & K \\ | & & | & & | & & | \\ \mathbb{Z} & \subset & \mathbb{Q} & & \mathbb{F}_q[T] & \subset & k = \mathbb{F}_q(T) \end{array}$$

$\mathcal{O}_K$ = the ring of integers of K

= the integral closure of $\mathbb{Z}$ or $\mathbb{F}_q[T]$ in K

$Cl_K =$ the ideal class group of $\mathcal{O}_K$

Main Question: Can we construct number fields and function fields (preferably infinitely many) whose class groups have certain properties?

- class number 1?
- class number divisible by n?
- class number indivisible by n?
- class group G?
- class group with subgroup G?

In particular, we are interested in the n**-rank** of Cl_K for a given integer n, that is, the greatest integer r with the property that

$$(\mathbb{Z}/n\mathbb{Z})^r \subset Cl_K.$$

Gauss

- $\mathbb{Q}(\sqrt{d})$ has even class number if and only if d is divisible by at least two distinct primes

- $\mathbb{Q}(\sqrt{d})$ has 2-rank $r-1$ if r is the number of distinct primes dividing d

Class Number Divisible by n

Theorem. Infinitely many imaginary quadratic number fields have class number divisible by n.

Nagell (1922), Ankeny & Chowla (1955)

Theorem. Infinitely many real quadratic number fields have class number divisible by n.

Yamamoto (1970), Weinberger (1973)

Theorem. Infinitely many quadratic function fields have ideal class number divisible by n.

Friesen (1991)

Cohen - Lenstra Heuristics (1983)

A finite abelian group G seems to occur as the class group of an imaginary quadratic field with a frequency inversely proportional to the size of the automorphism group of G.

Conjecture: The number of imaginary quadratic number fields with class number divisible by an odd prime p is

$$1 - \prod_{i=1}^{\infty} \left(1 - \frac{1}{p^i}\right).$$

Conjecture: The number of real quadratic number fields with class number divisible by an odd prime p is

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

Cohen - Lenstra Heuristics

-generalized to number fields of any degree and over any base field by Cohen and Martinet (1987)

-function field analogue by Friedman and Washington (1989)

The only known results are for quadratic number fields with class number divisible by 3 (Davenport & Heilbronn, 1971) and for function fields (Achter, 2006).

Progress

In the past several years, several quantitative results have appeared which give lower bounds on the number of fields with bounded discriminant and class number divisible by $n \geq 3$.

Murty (1999):

(i) The number of imaginary quadratic number fields whose absolute discriminant is $\leq x$ and whose class number is divisible by n is $\gg x^{\frac{1}{2}+\frac{1}{n}}$.

(ii) If n is odd or $2 \parallel n$, then the number of real quadratic fields with discriminant $\leq x$ and class number divisible by n is $\gg x^{\frac{1}{2n}-\epsilon}$ for any $\epsilon > 0$.

(Ankeny & Chowla's results gave lower bound of $x^{1/2}$ for the imaginary case.)

Function Field Analogue

Cardon & Murty (2001):

Let q be a power of an odd prime, $n \geq 3$. The number of quadratic function fields $\mathbb{F}_q(T)(\sqrt{D})$ with $\deg(D) \leq x$ and class number divisible by n is $q^{x(\frac{1}{2}+\frac{1}{n})}$.

Improved Bounds

Imaginary Quadratic Number Fields

$4 \mid n$: $x^{\frac{1}{2}+\frac{2}{n}-\epsilon}$ for all $\epsilon > 0$

$4 \mid (n-2)$: $x^{\frac{1}{2}+\frac{3}{n+2}-\epsilon}$ (Soundararajan, 2000)

Real Quadratic Number Fields

n odd: $x^{\frac{1}{n}-\epsilon}$ for all $\epsilon > 0$ (Yu, 2002)

$n = 3$: $x^{5/6}$ (Chakraborty & Murty, 2003)

$n = 3$: $x^{7/8}$ (Byeon & Koh, 2003)

Real Quadratic Function Fields

n odd: $\frac{q^{x/n}}{x^2}$

n even: $q^{x/2n}$ (Chakraborty & Mukhopadhyay, 2006)

Higher Degree Extensions

Theorem. (Bilu & Luca, 2005)

Given positive integers m and n, $m \geq 3$, there exist positive numbers $X_0(m, n)$ and $c(m, n)$ such that for any $X > X_0(m, n)$ there are at least $c(m, n)X^{\mu}$ pairwise non-isomorphic totally real number fields of degree m, with discriminant not exceeding X, and with class number divisible by n, where $\mu = \frac{1}{2(m-1)n}$.

For $m = 2$, we get a lower bound of $x^{\frac{1}{2n}}$.

Higher Degree Extensions - function fields

Let l be a prime dividing $q-1$. If n is a fixed positive integer that satisfies

1) $n > l^2 - l$,

2) n has no prime divisors less than l, and

3) $\frac{1}{l} - \frac{1}{n} > \frac{\log 2}{\log q}$,

then there are $\gg q^{x(\frac{1}{l}+\frac{1}{n})}$ cyclic extensions $K = \mathbb{F}_q(T)(\sqrt[l]{D})$ of $\mathbb{F}_q(T)$ with $\deg(D) \le x$ and class number divisible by n.

If $q > 2^l$, but n is an integer that fails to satisfy one of the three conditions above:

$$q^{x(\frac{1}{l}+\frac{1}{nt})}, t > 1$$

Idea of Proof

Take monic $f, g \in \mathbb{F}_q[T]$ with $\deg(g^l) > \deg(f^n)$, and $a \in \mathbb{F}_q^\times$ with $-a$ not an l-th power. Let

$$D = g^l - af^n.$$

- Construct an element of order n in Cl_K for $K = \mathbb{F}_q(T, \sqrt{D})$.
- Use sieve methods to find a lower bound on the number of f and g for which D is l-th power-free.
- Check for duplication.

Constructing an Element of Order n in Cl_K

Let $\zeta \in \mathbb{F}_q$ be a primitive l-th root of unity.

$$D = g^l - af^n$$

$$(f^n) = (g^l - D) = (g - \sqrt[l]{D})(g - \zeta\sqrt[l]{D}) \cdots (g - \zeta^{l-1}\sqrt[l]{D})$$

Constructing an Element of Order n in Cl_K

Let $\zeta \in \mathbb{F}_q$ be a primitive l-th root of unity.

$$D = g^l - af^n$$

$$(f^n) = (g^l - D) = (g - \sqrt[l]{D})(g - \zeta\sqrt[l]{D}) \cdots (g - \zeta^{l-1}\sqrt[l]{D})$$

The ideals on the right are pairwise relatively prime, so there exists an ideal $\mathfrak{a}$ with

$$\mathfrak{a}^n = (g - \sqrt[l]{D}).$$

Let r be the order of $\mathfrak{a}$ in Cl_K. We will show that

$$r = n.$$

Choose $v \in \mathcal{O}_K$ with

$$\mathfrak{a}^r = (v).$$

Constructing an Element of Order n in Cl_K

For ideals $\mathfrak{b} \subset \mathcal{O}_K$, define

$$|\mathfrak{b}| = |\mathcal{O}_K/\mathfrak{b}|.$$

$$(f^n) = (g^l - D) = (g - \sqrt[l]{D})(g - \zeta\sqrt[l]{D}) \cdots (g - \zeta^{l-1}\sqrt[l]{D})$$

Then

$$|\mathfrak{a}^n|^l = |(f^n)| = q^{nl \deg(f)},$$

so

$$|(v)| = |\mathfrak{a}^r| = q^{r \deg(f)}.$$

We can show that

$$\deg(N(v)) \geq \frac{1}{l-1} \deg(D).$$

Then

$$\begin{aligned} q^{r \deg(f)} &= |\mathfrak{a}|^r = |(v)| = |N(v)| = q^{\deg(N(v))} \\ &\geq q^{\frac{\deg(D)}{l-1}} \\ &= q^{\frac{\deg(g^l - af^n)}{l-1}} \\ &= q^{\frac{n \deg(f)}{l-1}}, \end{aligned}$$

which implies that

$$\frac{n}{r} \leq l - 1.$$

But $\frac{n}{r}$ is an integer dividing n, so by the hypothesis we must have that $n = r$, as desired.

n-Rank in Quadratic Number Fields

Cohen-Lenstra: Probability that odd part of class group of an imaginary quadratic field is cyclic $> 97\%$

Probability that p-rank $= r$ ($p > 2$):

$$\frac{1}{p^{r^2}} \prod_{i=1}^{\infty} \left(1 - \frac{1}{p^i}\right) \prod_{1 \le i \le r} \left(1 - \frac{1}{p^i}\right)^{-2}$$

Infinitely many imaginary quadratic number fields have n-rank ≥ 2. (Yamamoto, 1970)

Infinitely many imaginary quadratic number fields have 3-rank at least 3. (Craig, 1973)

Algorithm for generating quadratic fields with 3-rank at least 2. (Diaz y Diaz, 1978)

Current record: 3 imaginary quadratic fields with 3-rank 6. (Llorente & Quer, 1987)

Infinitely many real and imaginary quadratic number fields with 5-rank ≥ 3. (Mestre, 1992)

3-Rank in Quadratic Number Fields

Theorem (with Erickson, Kaplan, Mendoza, and Shayler). Let $w \equiv \pm 1 \pmod 6$, and let c be any integer with $c \equiv w \pmod 6$. If $d =$

$$c\,(w^2+18cw+108c^2)(4w^3-27cw^2-486c^2w-2916c^3),$$

then $\mathbb{Q}(\sqrt{d})$ has 3-rank at least 2.

-Proven by the 2005 Algebraic Number Theory group at the SMALL REU at Williams College.

More Generally

Theorem. (with F. Luca)

Choose integers a and b such that

$$(a,b) \equiv (1,11),\ (11,1) \pmod{30}.$$

Choose positive integers α and β such that

$$\alpha \equiv 6, 24 \pmod{30}, \beta \equiv 7, 13, 17, 23 \pmod{30},$$

$$\mathrm{gcd}(\alpha, a - 18b\beta^2) = 1, \mathrm{gcd}(a, \beta) = 1,$$

$$\mathrm{gcd}(a, b(\alpha^2 - \beta^2)) = 1.$$

If $d = 8b\beta^2(a^2 + 18ac + 108c^2)*$

$(4a^3 - 216b\beta^2(a^2 + 18ac + 108c^2))$,

then $K = \mathbb{Q}[\sqrt{d}]$ has 3-rank at least 2.

Idea of Proof

Recall that the Hilbert Class Field H of K is the maximal, unramified, abelian extension of K, and that

$$\text{Gal}(H/K) \cong Cl_K.$$

$$\begin{array}{c} H \\ | \\ L \\ | \\ K \\ | \\ \mathbb{Q} \end{array}$$

$3|h_K \Leftrightarrow K$ admits a cyclic, unramified degree 3 extension.

In fact, the 3-rank of K is equal to n if and only if there are exactly $\dfrac{3^n - 1}{2}$ cyclic, unramified extensions of K degree 3.

Kishi and Miyake's Result

Theorem (Kishi/Miyake, 2000). Choose $u, w \in \mathbb{Z}$ and let $g(Z) = Z^3 - uwZ - u^2$. If

(i) $d = 4uw^3 - 27u^2$ is not a square in $\mathbb{Z}$;

(ii) u and w are relatively prime;

(iii) $g(Z)$ is irreducible;

(iv) One of the following conditions holds:

$$\begin{aligned} I.\ & 3 \nmid w; \\ II.\ & 3 \mid w, \quad uw \not\equiv 3 \pmod 9, \quad u \equiv w \pm 1 \pmod 9; \\ III.\ & 3 \mid w, \quad uw \equiv 3 \pmod 9, \quad u \equiv w \pm 1 \pmod{27}, \end{aligned}$$

then $K = \mathbb{Q}(\sqrt{d})$ has class number divisible by 3. Conversely, every quadratic number field K with class number divisible by 3 and every unramified cyclic cubic extension of K is given by a suitable choice of integers u and w.

The Parameterizations

Let

$$
\begin{aligned}
u &= 8b\beta^2(a^2 + 18ac + 108c^2), \\
v &= a, \\
x &= 8b\alpha^2(a^2 + 18ac + 108c^2), \\
y &= a + 18c.
\end{aligned}
$$

Claim: The pairs (u, w) and (x, y) satisfy the hypotheses for Kishi and Miyake's theorem.

Thus, $\mathbb{Q}(\sqrt{4w^3 - 27u})$ and $\mathbb{Q}(\sqrt{4y^3 - 27x})$ each admit cyclic, cubic, unramified extensions.

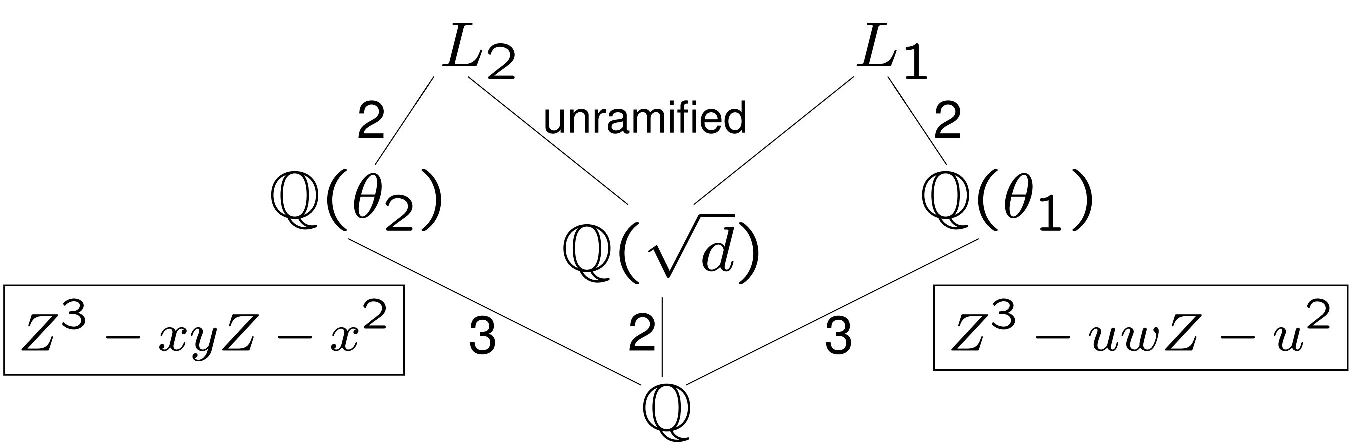
$$\theta_1 = \text{root of } Z^3 - uwZ - u^2$$

$$\theta_2 = \text{root of } Z^3 - xyZ - x^2.$$

Then the cubic fields $\mathbb{Q}(\theta_1)$ and $\mathbb{Q}(\theta_2)$ have discriminants which differ by a square factor, so

So $\mathbb{Q}(\sqrt{4w^3 - 27u}) = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{4y^3 - 27x})$.

Thus $\mathbb{Q}(\sqrt{d})$ has two cyclic, unramified cubic extensions L_1 and L_2, where L_i is the normal closure of $\mathbb{Q}(\theta_i)$. So $\mathbb{Q}(\sqrt{d})$ has 3-rank at least 2.



Quantitative Results

Theorem. (with F. Luca)

For every $\varepsilon > 0$, there exists $x_0 = x_0(\varepsilon)$ such that if $x > x_0$, then there are $\geq x^{1/3-\varepsilon}$ real quadratic number fields K with $\Delta_K \leq x$ whose class group has 3-rank at least 2. The same result is true for complex quadratic number fields with $|\Delta_K| \leq x$.

This lower bound agrees with Byeon's result (2006) on the number of imaginary quadratic number fields with n-rank ≥ 2.

n-Rank in Quadratic Function Fields

Function field analogue of theorem above. (current work)

Algorithm for generating quadratic function fields with 3-rank $\geq 2, 3$ (other results as well). (Bauer, Jacobson, Lee, Scheidler)

Infinitely many real and imaginary quadratic function fields have n-rank ≥ 2. (with Spencer)

Higher Degree Extensions

Theorem (Azuhata, Ichimura, 1982). For any positive integers m and n with $m > 1$, there are infinitely many number fields K of degree $m = r_1 + 2r_2$ such that

1) $r_2 \geq 1$, and

2) Cl_K contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{r_2}$.

$$n\text{-rank} + \text{unit rank} \geq m - 1$$

Higher Degree Extensions

Theorem (Azuhata, Ichimura, 1982). For any positive integers m and n with $m > 1$, there are infinitely many number fields K of degree $m = r_1 + 2r_2$ such that

1) $r_2 \geq 1$, and

2) Cl_K contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{r_2}$.

Theorem (Nakano, 1986). For any positive integers m and n with $m > 1$, and any non-negative integers r_1 and r_2 with $r_1 + 2r_2 = m$, there are infinitely many number fields K of degree m over $\mathbb{Q}$ such that

1) r_1 is the number of real embeddings of K into $\mathbb{C}$,

2) Cl_K contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{r_2+1}$.

$$n\text{-rank} + \text{unit rank} \geq m$$

Real vs. Imaginary Function Fields

Number Fields: Rank of Units $= r_1 + r_2 - 1$

Function Fields: Rank $=$ ($\#$ of primes over ∞) -1

Real vs. Imaginary Function Fields

Number Fields: Rank of Units $= r_1 + r_2 - 1$

Function Fields: Rank $=$ ($\#$ of primes over ∞) -1

	Number Fields	Function Fields
Max. Unit Rank	Real	∞ splits completely
Min. Unit Rank	Imaginary	∞ totally ramified/inert

So we say a function field K/k is *real* is the prime at infinity in k splits completely in K and *imaginary* if the prime at infinity in k is totally ramified or inert in K.

Function Fields - Imaginary Case

Theorem. For any relatively prime integers m and n, not divisible by the characteristic of $\mathbb{F}_q(T)$, with $m, n > 1$, there exist infinitely many function fields K of degree m over $k = \mathbb{F}_q(T)$ such that

1) the prime at infinity is totally ramified in K , and

2) Cl_K contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{m-1}$.

Infinity inert (with Y. Lee): Same rank under certain conditions on n, m, and q

$$n\text{-rank} + \text{unit rank} \geq m - 1.$$

Function Fields - Real Case

Theorem. For any relatively prime integers m and n, not divisible by the characteristic of $\mathbb{F}_q(T)$, with $m, n > 1$, there exist infinitely many function fields K of degree m over $k = \mathbb{F}_q(T)$ such that

1) the prime at infinity splits completely in K, and

2) Cl_K contains a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

$$n\text{-rank} + \text{unit rank} \geq m$$

General Case

Theorem. Let m and n be any positive integers, not divisible by the characteristic of $\mathbb{F}(T)$, with $n > 1$. If g is an integer with $2 \leq g \leq m - 1$, then there are infinitely many function fields K of degree m over k such that

1) the prime at infinity in k splits into exactly g primes in K, one with ramification index $m - g + 1$, the rest unramified, all with relative degree 1, and

2) Cl_K contains an abelian subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{m-g}$.

$$n\text{-rank} + \text{unit rank} \geq m - 1.$$

Improved to m (with Y. Lee) when infinity is inert, under certain conditions.

Improved to m by Y. Lee in certain cases.

Idea of Proof

$$f(X) = \prod_{i=0}^{m-1} (X - B_i) + D^n$$

$B_0, \cdots, B_{m-1}, D \in \mathbb{F}_q[T]$ and satisfy certain congruences and degree properties.

If θ is a root of $f(X)$, then $K = k(\theta)$ satisfies the theorem.

Since the class number is finite, the existence of one such field implies the existence of infinitely many.

Idea of Proof

W = roots of unity in K
E = group of units in K
$Cl_K[n] =$ elements of Cl_K with order dividing n

For all primes l dividing n:

$$(1) \to Cl_K\left[\frac{n}{l}\right] \xrightarrow{i} Cl_K[n] \xrightarrow{h} K^\times/EK^{\times l}$$

For all $\bar{\mathfrak{a}} \in Cl_K[n]$, $\mathfrak{a}^n = (\alpha)$. Set

$$h(\bar{\mathfrak{a}}) = [\alpha] \in K^\times/EK^{\times l}.$$

$$Cl_K[n]^{n/l} \cong Cl_K[n]/Cl_K\left[\frac{n}{l}\right] \cong Im(h)$$

Imaginary Case - Infinite Prime Totally Ramified

Since ∞ is totally ramified, $E = W$.

$$(1) \to Cl_K\left[\frac{n}{l}\right] \xrightarrow{i} Cl_K[n] \xrightarrow{h} K^\times/WK^{\times l}$$

$$Cl_K[n]^{n/l} \cong Cl_K[n]/Cl_K\left[\frac{n}{l}\right] \cong Im(h)$$

$\theta - B_1, \cdots, \theta - B_{m-1}$ linearly independent in $K^\times/WK^{\times l}$, and $[\theta - B_1], \cdots, [\theta - B_{m-1}] \in Im(h)$, so

$$\dim_{\mathbb{Z}/l\mathbb{Z}} Cl_K[n]^{n/l} = \dim_{\mathbb{Z}/l\mathbb{Z}} Im(h) \geq m - 1.$$

Thus Cl_K contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{m-1}$.

General Case

Exact Sequence:

$$(1) \to Cl_K\left[\frac{n}{l}\right] \xrightarrow{i} Cl_K[n] \xrightarrow{h} K^\times/EK^{\times l}$$

$\theta - B_1, \cdots, \theta - B_{m-1}$ linearly independent in $K^\times/WK^{\times l}$,

but $E \neq W$ in this case.

Now, since the prime at infinity splits into exactly g primes in K, we have that the unit rank of K is equal to $g - 1$.

General Case Continued

Exact Sequence:

$$(1) \to S \cap \; EK^{\times l}/WK^{\times l} \to S \to S' \to (1)$$

$S \subset K^{\times}/WK^{\times l}$: generated by $\theta - B_1, \ldots, \theta - B_{m-1}$

$S' \subset K^{\times}/EK^{\times l}$: image of S

$$\dim_{\mathbb{Z}/l\mathbb{Z}} S' = \dim_{\mathbb{Z}/l\mathbb{Z}} S - \dim_{\mathbb{Z}/l\mathbb{Z}} \; (S \; \cap \; EK^{\times l}/WK^{\times l})$$

$$\geq \dim_{\mathbb{Z}/l\mathbb{Z}} S - \dim_{\mathbb{Z}/l\mathbb{Z}}(E/W)$$

$$\geq m - 1 - (g - 1)$$

$$\geq m - g$$

Exact Sequence:

$$(1) \to Cl_K\left[\frac{n}{l}\right] \xrightarrow{i} Cl_K[n] \xrightarrow{h} K^\times/EK^{\times l}$$

Because $S' \subset Im(h)$, we get that

$$\begin{aligned}
\dim_{\mathbb{Z}/l\mathbb{Z}} Cl_K[n]^{n/l} &= \dim_{\mathbb{Z}/l\mathbb{Z}} Im(h) \\
&\geq \dim_{\mathbb{Z}/l\mathbb{Z}} S' \\
&\geq m - g.
\end{aligned}$$

Thus Cl_K contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{m-g}$.

Infinite Prime

With the exception of the case where the prime at infinity is inert, we use the Newton Polygon to prove the behavior of the prime at infinity.

A: any discrete, rank 1 valuation ring with quotient field K

$\overline{K}$: an algebraic closure of K

v: valuation on A and the unique extension of v to $\overline{K}$

If $f(X) = \sum_{i=0}^{d} a_i X^i \in \overline{K}[X]$, then the Newton polygon of f with respect to the valuation v is constructed by first considering the points $(i,\text{ord}_v(a_i))$ in the plane. Next, for each i, $0 \leq i \leq d$, draw the vertical half-line that starts at the point $(i,\text{ord}_v(a_i))$ and extends upward. The Newton polygon is the convex hull of the union of these lines and satisfies the following property.

Theorem. If $(i,\text{ord}_v(a_i))$ and $(j,\text{ord}_v(a_j))$, $j > i$, are endpoints of a segment of the boundary of the Newton polygon of f with respect to v, then f has $j - i$ roots θ_t in $\overline{K}$, counting multiplicity, each with

$$\text{ord}_v(\theta_t) = -\frac{\text{ord}_v(a_j) - \text{ord}_v(a_i)}{j - i}.$$

$$f(X) = \prod_{i=0}^{m-1} (X - B_i) + D^n$$

Infinity Totally Ramified:

$$\deg(D^n) > m \cdot \max \{\deg(B_i)\}_{i=0}^{m-1}$$

$$(m, \deg(D)) = 1$$

Newton Polygon consists of single line segment with slope

$$\frac{n \deg(D)}{m}.$$

Infinity Splits Completely:

$$\deg(B_0) < \cdots < \deg(B_{m-1})$$

$$\deg(B_0) + \cdots + \deg(B_{m-1}) = \deg(D^n)$$

Newton Polygon consists of m distinct line segments with distinct slopes $\deg(B_0), \deg(B_1), \ldots, \deg(B_{m-1})$.

General Case:

Prescribed Class Group

Can we construct infinitely many number fields or function fields with prescribed class group?

Every finite abelian p-group is isomorphic to the p-part of Cl_K for some number field K. (Yahagi, 1978)

Every cyclic group is isomorphic to the class group of infinitely many function fields. (Angles, 1998)

Every finite abelian group G is isomorphic to the S-class group of some number field K for some finite set of places S (the same is true for function fields). (Perret, 1999)

None of these fields give explicit constructions for the fields.

Indivisibility of Class Numbers

Constructing fields with class number indivisible by a given integer n is typically a more difficult problem.

e.g. Are there infinitely many regular primes?

- Infinitely many imaginary quadratic number fields have class number indivisible by 3. (Hartung, 1976) (check: not explicit)

- Infinitely many imaginary quadratic number fields have class number indivisible by p. (Horie & Onishi, Jochnowitz, Ono & Skinner)

- Quantitative results for imaginary quadratic number fields with $p \nmid h_K$. (Kohnen & Ono)

- Quantitative results for real quadratic number fields with $p \nmid h_K$. (Ono)

None of these results give explicit constructions of fields with the desired properties.

Higher Degree Function Fields

Theorem. Let m be any positive integer not divisible by 3. Let $q \not\equiv 1 \pmod 3$ be a power of an odd prime, $\gamma \in \mathbb{F}_q$. If $\gamma + 3\zeta_3$ is not a p-th power in $\mathbb{F}_q(\zeta_3)$ for all primes p dividing m and $\gamma + 3\zeta_3 \notin -4\mathbb{F}_{q^2}^4$, then there are infinitely many function fields of degree m with divisor class number not divisible by $n = 3$.

For any given m, there is a positive density of primes q satisfying the hypotheses.

Here we construct the fields explicitly. The proof relies on class field theory.