Ramification, Galois Module Structure (and Hopf Algebras)

Nigel Byott

University of Exeter, UK

Omaha - 27 May 2013

Ramification (Number Fields)

Let N/K be a Galois extension of number fields (finite extensions of $\mathbb{Q}$), with Galois group $\Gamma = \mathrm{Gal}(N/K)$.

Their rings of algebraic integers, O_N and O_K, have unique factorisation of *ideals* into prime *ideals*.

If $\mathfrak{p}$ is a prime ideal of O_K, then

$$\mathfrak{p}O_N = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$$

where

- $\mathfrak{P}_1, \cdots, \mathfrak{P}_g$ are prime ideals of O_N above $\mathfrak{p}$,
- $e = e_{\mathfrak{p}}(N/K)$ is the *ramification index* of $\mathfrak{p}$ in N/K;
- $[N : K] = |\Gamma| = efg$, where f is the residue field extension degree:

$$f = \left[\frac{O_N}{\mathfrak{P}_i} : \frac{O_K}{\mathfrak{p}_i} \right] \text{ for each } i.$$

We say N/K is

- *unramified* at $\mathfrak{p}$ if $e = 1$;
- (at most) *tamely ramified* at $\mathfrak{p}$ if $p \nmid e$, where $p \in \mathbb{Z}$ is the unique rational prime number in $\mathfrak{p}$;
- *wildly ramified* at $\mathfrak{p}$ if $p \mid e$.

We can describe the wild ramification more precisely as follows. Fix a prime $\mathfrak{P}$ of O_N above $\mathfrak{p}$, and for $i \geq 0$ set

$$\Gamma_i(\mathfrak{P}) = \{\gamma \in \Gamma : \gamma(x) - x \in \mathfrak{P}^{i+1} \text{ for all } x \in O_N\}.$$

If we know the sequence of these higher ramification groups for each $\mathfrak{P}$, we can calculate a lot of arithmetic information about N/K, for example $\mathrm{Tr}_{N/K}(I)$ for any ideal I of O_N.

Galois Module Structure (Number Fields)

Theorem (Hilbert-Speiser)

Let N be an abelian extension of $\mathbb{Q}$ and let $\Gamma = \mathrm{Gal}(N/\mathbb{Q})$. If $N/\mathbb{Q}$ is tame (i.e., at most tamely ramified at all primes p), then there is some $x \in O_N$ so that $\{\gamma(x) : \gamma \in \Gamma\}$ is a $\mathbb{Z}$-basis of O_N. Equivalently, O_N is a free module (of rank 1) over the group ring $\mathbb{Z}[\Gamma]$.

If $N/\mathbb{Q}$ is wildly ramified, O_N cannot be free over $\mathbb{Z}[G]$, but we have the following generalisation:

Theorem (Leopoldt)

Let $N/\mathbb{Q}$ be an abelian extension of $\mathbb{Q}$ (possibly wildly ramified), and let $\Gamma = \mathrm{Gal}(N/\mathbb{Q})$. Let

$$\mathcal{A} = \{\alpha \in \mathbb{Q}[\Gamma] : \alpha \cdot a \in O_N \text{ for all } a \in O_N\},$$

the associated order of O_N in $\mathbb{Q}[\Gamma]$. Then O_N is a free $\mathcal{A}$-module.

What if the base field $K \neq \mathbb{Q}$?

Theorem (Noether's Criterion)

Let N/K be a Galois extension of number fields (not necessarily abelian). Then O_N is locally free *over $O_K[\Gamma]$ if and only if N/K is tame (i.e. at most tamely ramified at all primes $\mathfrak{p}$ of O_K.*

O_N is *locally free* means that, for each $\mathfrak{p}$, the completion $O_{N,\mathfrak{p}}$ is free over $O_{K,\mathfrak{p}}[\Gamma]$.

For a tame extension N/K, the failure of the locally free $O_K[\Gamma]$-module O_N to be (globally) free is measured by its class in the *locally free classgroup* $\mathrm{Cl}(O_K[\Gamma])$. There are deep results in this *tame, global* theory, e.g.

- restricting scalars to $\mathbb{Z}[G]$, the class of O_N in $\mathrm{Cl}(\mathbb{Z}[\Gamma])$ is determined by Artin L-functions (Fröhlich, Taylor);
- realisable Galois module classes in $\mathrm{Cl}(O_K[\Gamma])$ (McCulloh, Sodaïgui).

Our focus, however, is on the *wild, local* theory.

Take completions of O_N, O_K at $\mathfrak{P}$, $\mathfrak{p}$ (and replace Γ by the decomposition group of $\mathfrak{P}$). Changing notation, we arrive at the following situation:

Ramification (Local Fields)

K is a finite extension of $\mathbb{Q}_p$ (for some rational prime number $p \in \mathbb{Z}$). In particular, K has characteristic 0. It has valuation ring ("ring of integers") O_K, which is a PID, with unique maximal ideal $\mathfrak{P}_K$. The residue field $O_K/\mathfrak{P}_K$ is a finite field $\mathbb{F}_q$, $q = p^d$, of characteristic p. The K is complete with respect to the discrete valuation $v_K : K \longrightarrow \mathbb{Z} \cup \{\infty\}$ with

$$v_K(x) \geq j \Leftrightarrow x \in \mathfrak{P}_K^j.$$

N/K is a finite Galois extension, and $v_N \mid_K = e v_K$, where $e = e_{N/K}$ is the ramification index.

We can also consider the parallel characteristic p situation where K has the form $K = \mathbb{F}_q((T))$ with $v_K(T) = 1$.

In either case, writing $\Gamma = \mathrm{Gal}(N/K)$, we have the ramification groups

$$\Gamma_i = \{\gamma \in \Gamma : (\gamma - 1) \cdot O_N \subseteq \mathfrak{P}^{i+1}\}.$$

Galois Module Structure (Local Fields)

We can consider O_N as a module over its associated order

$$\mathcal{A} := \mathcal{A}_{N/K} := \{\alpha \in K[\Gamma] : \alpha \cdot a \in O_N \text{ for all } a \in O_N\},$$

or, more generally, for $h \in \mathbb{Z}$, consider $\mathfrak{P}_N^h$ as a module over its associated order

$$\mathcal{A}_{N/K}(\mathfrak{P}^h) := \{\alpha \in K[\Gamma] : \alpha \cdot a \in \mathfrak{P}_N^h \text{ for all } a \in \mathfrak{P}_N^h\}.$$

Questions: When is O_N (or $\mathfrak{P}_N^h$) free over its associated order? If not, "how complicated" is this module? "How complicated" is the associated order?

$\mathcal{A} = O_K[\Gamma]$ if and only if N/K is tame, and in that case O_N is free over $\mathcal{A}$.

Since our questions are about "wild" phenomena, for the rest of this talk we assume:

K is a local field of residue characteristic p. and N/K is a totally ramified abelian Galois extension of degree p^m.

We have the ramification groups $\Gamma = \Gamma_1 \geq \Gamma_2 \geq \cdots \geq \Gamma_n = \{1\}$ for large enough n.

Let $b_1 \leq \cdots \leq b_m$ be the ramification breaks, i.e. the b with $\Gamma_b \neq \Gamma_{b+1}$ (counted with multiplicity).

Write e for the absolute ramification index of the base field K:

$$pO_K = \mathfrak{P}_N^e \text{ (with } e = \infty \text{ if } K \text{ has characteristic } p.)$$

Then either

- $b_1 = ep/(p-1)$ (characteristic 0 only), or
- $p \nmid b_1$ and $1 \leq b_1 < ep/(p-1)$.

Also,

$$b_i \equiv b_{i+1} \bmod p^i \text{ for all } i$$

(This is the Hasse-Arf theorem; it does not necessarily hold for non-abelian extensions, but the congruence does hold mod p.)

Our question is now:

If we know the ramification filtration of N/K (or just the ramification breaks b_i), what can we say about the Galois module structure of O_N or its fractional ideals [and conversely]?

There are some cases where we can give some sort of answer:

Some examples: (1) degree p

$\Gamma = C_p$, and we have one ramification break b_1.

Let $s = (b_1 \bmod p)$, i.e. $s \equiv b_1 \bmod p$ with $0 \leq s \leq p-1$.

(Characteristic 0): If N/K is not "almost maximally ramified" (i.e. if $b_1 < [ep/(p-1)] - 1$) then

$$O_N \text{ is free over its associated order } \Leftrightarrow s \mid (p-1).$$

(Bertrandias & Ferton, 1972).

Idea: if $\Gamma = \langle \gamma \rangle$ then for all $x \in N$ with $p \nmid v_N(x)$ we have

$$v_N((\gamma - 1)(x)) = v_N(x) + b_1.$$

Similar results in characteristic p (Aiba, 2003; de Smit & Thomas, 2007)

In characteristic 0, Ferton (1972) gave result for arbitrary ideals in terms of continued fraction expansion of s/p.

Some examples: (2) Miyata's cyclic extensions

(Characteristic 0 only)

Suppose K contains a primitive p^m-th root of unity and consider a cyclic Kummer extension N of K of degree p^m, of the form

$$N = K(\sqrt[p^m]{a})$$

where $a \in O_K$ and $p \nmid v_K(a-1)$.

For these special Kummer extensions,

$$b_1 = \frac{ep}{p-1} - v_K(a-1),$$

$$b_{i+1} = b_i + p^i e \equiv b_1 \pmod{p^m} \text{ for } 2 \leq i < m.$$

Miyata (1998) gave a necessary and sufficient condition for O_N to be free over its associated order.

After some reformulation (NB, 2008), it follows that:

- if $m = 2$ then O_N is free $\Leftrightarrow (b_1 \bmod p^2) \mid (p^2 - 1)$, analogously to Bertrandias-Ferton for $m = 1$;
- if $m \geq 3$ then O_N is free if $(b_1 \bmod p^m) \mid (p^d - 1)$ for some $d \in \{1, 2, \ldots, m\}$ but the converse is not always true.

Some examples: (3) Almost one-dimensional extensions

These are a class of elementary abelian extensions in characteristic p, and include all totally and weakly ramified p-extensions. They were constructed by Elder (2009).

It turns out that Miyata's necessary and sufficient condition for O_N to be free over its associated order applies to these extensions as well.

This is surprising as both the characteristic and the Galois group are different. It suggests that these results might be part of a bigger picture.

What does Galois module structure say about ramification numbers?

Suppose that N/K is as above, and that **Vostokov's condition** holds:

$$p^m \nmid \mathcal{D}_{N/K},$$

where $\mathcal{D}_{N/K}$ is the different.

(This is automatic unless Γ is cyclic or $p = 2$, and guarantees that the associated order of every ideal is a local ring.)

Then the inverse different $\mathcal{D}_{N/K}^{-1}$ cannot be free over its associated order unless $b_i \equiv -1 \pmod{p^m}$ for all i. (NB, 1997).

Thus, when $\mathcal{D}_{N.K}^{-1}$ is free, we have $\mathcal{D}_{N/K}^{-1} = cO_N$ for some $c \in K$, and O_N is free as well.

More generally, Bondarko (2007) shows that, under some (fairly mild) restrictions on the ramification breaks, if there exists *some* ideal of O_N which is free over its associated order, then all the ramification breaks must be congruent mod p^m.

Hopf orders and Galois Module Structure

The associated orders $\mathcal{A}$ we have been considering are O_K orders in the group algebra $K[\Gamma]$, which is a Hopf algebra over K.

A particularly nice situation is when $\mathcal{A}$ inherits from $K[\Gamma]$ the structure of a Hopf order over O_K, i.e. when $\mathcal{A}$ is a Hopf order in $K[\Gamma]$. This happens if

$$\Delta(\mathcal{A}) \subseteq \mathcal{A} \otimes_{O_K} \mathcal{A},$$

where $\Delta : K[\Gamma] \longrightarrow K[\Gamma] \otimes_K K[\Gamma]$ is the comultiplication on $K[\Gamma]$:

$$\Delta\left(\sum_{\gamma\in\Gamma} c_\gamma \gamma\right) = \sum_{\gamma\in\Gamma} c_\gamma \gamma \otimes \gamma.$$

If the associated order $\mathcal{A}$ of some ideal $\mathfrak{P}_N^h$ of N is a Hopf order then it is free over $\mathcal{A}$.

For the valuation ring O_N itself, if the associated order $\mathcal{A}$ of O_N is a Hopf order $\mathcal{A}$ and Vostokov's condition holds, then

$$\mathcal{D}_{N/K} = \mathfrak{i}(\mathcal{A})O_N \text{ and } \mathrm{Tr}_{N/K}(O_N) = \mathfrak{i}(\mathcal{A})$$

where $\mathfrak{i}(\mathcal{A})$ is the O_K-ideal defined by

$$\mathcal{A} \cap K\left(\sum_{\gamma\in\Gamma}\gamma\right) = \mathfrak{i}(\mathcal{A})^{-1}\left(\sum_{\gamma\in\Gamma}\gamma\right).$$

We also have the Childs-Hurley criterion: if $\mathcal{H}$ is a Hopf order in $K[\Gamma]$ such that $\mathcal{H}\cdot O_N \subseteq O_N$ and

$$\mathrm{Tr}_{N/K}(O_N) = \mathfrak{i}(\mathcal{H})$$

then O_N is free over $\mathcal{H}$, and $\mathcal{A} = \mathcal{H}$.

Hopf orders and formal groups

Let $\mathbf{F}, \mathbf{G} \in O_K[[X, Y]]$ be (one-dimensional) formal groups over O_K, and let $f(X) \in O_K[[X]]$ determine a homomorphism $\mathbf{F} \longrightarrow \mathbf{G}$.

i.e. the operations $+_{\mathbf{F}}$, $+_{\mathbf{G}}$ defined by

$$x +_{\mathbf{F}} y = \mathbf{F}(x, y), \quad x +_{\mathbf{G}} y = \mathbf{G}(x, y) \text{ for } x, y \in \mathfrak{P}_K$$

each make $\mathfrak{P}_K$ into an abelian group (with identity element 0), and we have

$$f(\mathbf{F}(X, Y)) = \mathbf{G}(f(X), f(Y)) \text{ in } O_K[[X, Y]].$$

Suppose that the quotient ring

$$\mathcal{H} = \frac{O_K[[X]]}{(f(X))}$$

is finitely generated as an O_K-module (i.e. f is an isogeny). Then $\mathcal{H}$ is an O_K-Hopf algebra representing the group scheme $\mathbb{K} = \ker(f)$.

Consider the finite group

$$\Gamma = \mathbb{K}(K^c) = \{x \in \mathfrak{P}_{O_{K^c}} : f(x) = 0\},$$

where K^c is the algebraic closure of K.

Suppose that the elements of Γ are all in $\mathfrak{P}_K$. (We could arrange this by taking **F**, **G** and f to be defined over some smaller field E and taking K to be the field we get by adjoining the elements of Γ to E.)

Then we may identify $\mathcal{H}$ as a Hopf order in the Hopf algebra $\mathrm{Map}(\Gamma, K)$, and its dual Hopf order $\mathcal{A} = \mathcal{H}^D$ as a Hopf order in $K[\Gamma]$.

Choose $w \in O_K$ with $v_K(w) = 1$ and adjoin to K the roots of $f(Z) = w$. This gives a totally ramified extension N of K which is Galois with group Γ, and the associated order of O_N is the Hopf order $\mathcal{A}$. Thus O_N is free over $\mathcal{A}$.

Bondarko (2000) showed that we have a totally ramified, p-power degree abelian extension N/K such that O_N is free over its associated order $\mathcal{A}$, and $\mathcal{D}_{N/K} = cO_N$ for some $c \in O_K$, then $\mathcal{A}$ is a Hopf order and arises from this construction.

Now suppose $\Gamma \not\subseteq \mathfrak{P}_K$. The above construction still works, but $\mathcal{A}$ is a Hopf order in some Hopf algebra $A \neq K[\Gamma]$. So we have a Hopf-Galois structure on the extension N/K which does not come from classical Galois theory. In this new Hopf-Galois structure, O_N is free over its associated order **in the Hopf algebra** A. The extension N/K might still be Galois, and, if so, O_N might or might not be free over its associated order in $K[\Gamma]$.

Questions

This raises a number of questions (at least some of which will come up later in this conference!)

- What Hopf orders are there in a given group algebra $K[\Gamma]$ (or a more general Hopf algebra)? Which of them can arise as associated orders of valuation rings?
- What Hopf-Galois structures are there on a given field extension?
- Can we compare Galois module structure results for different Hopf-Galois structures on *the same* field extension?
- If we have a Hopf algebra H acting on a field extension L/K which is **not** a Galois extension (i.e. not normal and/or inseparable) can we give say anything about freeness over associated orders in H? What should replace the ramification breaks?