AN INTRODUCTION TO GALOIS MODULE STRUCTURE

Nigel Byott

University of Exeter

Omaha, May 2019

Galois Theory: A Quick Summary

An extension N/K of fields of (finite) degree $n = [N : K]$ is **Galois** if it is normal and separable.

Galois Theory: A Quick Summary

An extension N/K of fields of (finite) degree $n = [N : K]$ is **Galois** if it is normal and separable.

Its **Galois group** is

$$\mathrm{Gal}(N/K) := \{\text{field automorphisms } \sigma : N \to N \text{ with } \sigma(k) = k \ \forall k \in K\}.$$

Then $\mathrm{Gal}(N/K)$ is a group of order n.

Galois Theory: A Quick Summary

An extension N/K of fields of (finite) degree $n = [N : K]$ is **Galois** if it is normal and separable.

Its **Galois group** is

$$\mathrm{Gal}(N/K) := \{\text{field automorphisms } \sigma : N \to N \text{ with } \sigma(k) = k \; \forall k \in K\}.$$

Then $\mathrm{Gal}(N/K)$ is a group of order n.

The **Fundamental Theorem of Galois Theory** says there is a bijection between subgroups of $\mathrm{Gal}(N/K)$ and fields E with $K \subseteq E \subseteq N$.

Galois Theory: A Quick Summary

An extension N/K of fields of (finite) degree $n = [N : K]$ is **Galois** if it is normal and separable.

Its **Galois group** is

$$\mathrm{Gal}(N/K) := \{\text{field automorphisms } \sigma : N \to N \text{ with } \sigma(k) = k \ \forall k \in K\}.$$

Then $\mathrm{Gal}(N/K)$ is a group of order n.

The **Fundamental Theorem of Galois Theory** says there is a bijection between subgroups of $\mathrm{Gal}(N/K)$ and fields E with $K \subseteq E \subseteq N$.

The **Nomal Basis Theorem** says there is an element $\alpha \in N$ (called a **normal basis generaor**) such that

$$\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(N/K)\}$$

is a basis for N as a K-vector space.

Galois Theory: A Quick Summary

An extension N/K of fields of (finite) degree $n = [N : K]$ is **Galois** if it is normal and separable.

Its **Galois group** is

$$\mathrm{Gal}(N/K) := \{\text{field automorphisms } \sigma : N \to N \text{ with } \sigma(k) = k \; \forall k \in K\}.$$

Then $\mathrm{Gal}(N/K)$ is a group of order n.

The **Fundamental Theorem of Galois Theory** says there is a bijection between subgroups of $\mathrm{Gal}(N/K)$ and fields E with $K \subseteq E \subseteq N$.

The **Nomal Basis Theorem** says there is an element $\alpha \in N$ (called a **normal basis generaor**) such that

$$\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(N/K)\}$$

is a basis for N as a K-vector space.
Thus every $\beta \in N$ can be written in a unique way as

$$\beta = \sum_{\sigma} c_\sigma \sigma(\alpha), \qquad c_\sigma \in K.$$

Reinterpreting the Normal Basis Theorem

Write $G = \mathrm{Gal}(N/K)$ and let

$$K[G] = \left\{ \sum_{\sigma \in G} c_\sigma \sigma : c_\sigma \in K \right\},$$

a K-vector space over K of dimension n.

Reinterpreting the Normal Basis Theorem

Write $G = \mathrm{Gal}(N/K)$ and let

$$K[G] = \left\{ \sum_{\sigma \in G} c_\sigma \sigma : c_\sigma \in K \right\},$$

a K-vector space over K of dimension n.

Then $K[G]$ is a ring with multiplication

$$\left(\sum_\sigma c_\sigma \sigma \right) \left(\sum_\tau d_\tau \tau \right) = \sum_{\sigma,\tau} c_\sigma d_\tau \sigma\tau = \sum_\rho \left(\sum_\sigma c_\sigma d_{\sigma^{-1}\rho} \right) \rho.$$

Reinterpreting the Normal Basis Theorem

Write $G = \mathrm{Gal}(N/K)$ and let

$$K[G] = \left\{ \sum_{\sigma \in G} c_\sigma \sigma : c_\sigma \in K \right\},$$

a K-vector space over K of dimension n.

Then $K[G]$ is a ring with multiplication

$$\left(\sum_\sigma c_\sigma \sigma \right) \left(\sum_\tau d_\tau \tau \right) = \sum_{\sigma,\tau} c_\sigma d_\tau \sigma\tau = \sum_\rho \left(\sum_\sigma c_\sigma d_{\sigma^{-1}\rho} \right) \rho.$$

We call $K[G]$ the **group algebra** of G over K.

Reinterpreting the Normal Basis Theorem

Write $G = \mathrm{Gal}(N/K)$ and let

$$K[G] = \left\{ \sum_{\sigma \in G} c_\sigma \sigma : c_\sigma \in K \right\},$$

a K-vector space over K of dimension n.

Then $K[G]$ is a ring with multiplication

$$\left(\sum_\sigma c_\sigma \sigma \right) \left(\sum_\tau d_\tau \tau \right) = \sum_{\sigma,\tau} c_\sigma d_\tau \sigma\tau = \sum_\rho \left(\sum_\sigma c_\sigma d_{\sigma^{-1}\rho} \right) \rho.$$

We call $K[G]$ the **group algebra** of G over K.

Then $K[G]$ acts on N; for $\beta \in N$ we have

$$\left(\sum_\sigma c_\sigma \sigma \right) \cdot \beta = \sum_\sigma c_\sigma \sigma(\beta) \in N.$$

Reinterpreting the Normal Basis Theorem

Write $G = \mathrm{Gal}(N/K)$ and let

$$K[G] = \left\{ \sum_{\sigma \in G} c_\sigma \sigma : c_\sigma \in K \right\},$$

a K-vector space over K of dimension n.

Then $K[G]$ is a ring with multiplication

$$\left(\sum_\sigma c_\sigma \sigma \right) \left(\sum_\tau d_\tau \tau \right) = \sum_{\sigma,\tau} c_\sigma d_\tau \sigma\tau = \sum_\rho \left(\sum_\sigma c_\sigma d_{\sigma^{-1}\rho} \right) \rho.$$

We call $K[G]$ the **group algebra** of G over K.

Then $K[G]$ acts on N; for $\beta \in N$ we have

$$\left(\sum_\sigma c_\sigma \sigma \right) \cdot \beta = \sum_\sigma c_\sigma \sigma(\beta) \in N.$$

Thus N becomes a module over the ring $K[G]$.

Now if $\alpha \in N$ is a normal basis generator for N/K, then, for each $\beta \in N$, there is a unique $\lambda \in K[G]$ with $\beta = \lambda \cdot \alpha$.

Now if $\alpha \in N$ is a normal basis generator for N/K, then, for each $\beta \in N$, there is a unique $\lambda \in K[G]$ with $\beta = \lambda \cdot \alpha$.

This means that N is a **free** $K[G]$-module of rank 1.

Now if $\alpha \in N$ is a normal basis generator for N/K, then, for each $\beta \in N$, there is a unique $\lambda \in K[G]$ with $\beta = \lambda \cdot \alpha$.

This means that N is a **free** $K[G]$-module of rank 1.

[Note that, unlike vector spaces over a field, modules over a ring do not always have a basis, i.e. are not always free. Thus the Normal Basis Theorem gives non-trivial information about the structure of N as a $K[G]$-module.]

Now if $\alpha \in N$ is a normal basis generator for N/K, then, for each $\beta \in N$, there is a unique $\lambda \in K[G]$ with $\beta = \lambda \cdot \alpha$.

This means that N is a **free** $K[G]$-module of rank 1.

[Note that, unlike vector spaces over a field, modules over a ring do not always have a basis, i.e. are not always free. Thus the Normal Basis Theorem gives non-trivial information about the structure of N as a $K[G]$-module.]

The main question of Galois module structure is:

Can we find an analogue of the Normal Basis Theorem at the level of integers?

Rings of algebraic integers

Let's take $K = \mathbb{Q}$. Inside $\mathbb{Q}$ we have the ring of integers $\mathbb{Z}$.

Rings of algebraic integers

Let's take $K = \mathbb{Q}$. Inside $\mathbb{Q}$ we have the ring of integers $\mathbb{Z}$.

Let N is a finite extension of $\mathbb{Q}$ (i.e. a number field) with $[N : \mathbb{Q}] = n$.

Rings of algebraic integers

Let's take $K = \mathbb{Q}$. Inside $\mathbb{Q}$ we have the ring of integers $\mathbb{Z}$.

Let N is a finite extension of $\mathbb{Q}$ (i.e. a number field) with $[N : \mathbb{Q}] = n$.

We have an analogue of $\mathbb{Z}$ inside N:

$$O_N = \{\alpha \in N : \alpha \text{ is the root of some monic } f(X) \in \mathbb{Z}[X]\}.$$

Rings of algebraic integers

Let's take $K = \mathbb{Q}$. Inside $\mathbb{Q}$ we have the ring of integers $\mathbb{Z}$.

Let N is a finite extension of $\mathbb{Q}$ (i.e. a number field) with $[N : \mathbb{Q}] = n$.

We have an analogue of $\mathbb{Z}$ inside N:

$$O_N = \{\alpha \in N : \alpha \text{ is the root of some monic } f(X) \in \mathbb{Z}[X]\}.$$

O_N is a ring, it contains $\mathbb{Z}$, and it has a basis over $\mathbb{Z}$ of size n.

Rings of algebraic integers

Let's take $K = \mathbb{Q}$. Inside $\mathbb{Q}$ we have the ring of integers $\mathbb{Z}$.

Let N is a finite extension of $\mathbb{Q}$ (i.e. a number field) with $[N : \mathbb{Q}] = n$.

We have an analogue of $\mathbb{Z}$ inside N:

$$O_N = \{\alpha \in N : \alpha \text{ is the root of some monic } f(X) \in \mathbb{Z}[X]\}.$$

O_N is a ring, it contains $\mathbb{Z}$, and it has a basis over $\mathbb{Z}$ of size n.

We call O_N the **ring of algebraic integers** of N.

Example: Quadratic Fields

Let $N = \mathbb{Q}(\sqrt{d})$ with d a squarefree integer.

Example: Quadratic Fields

Let $N = \mathbb{Q}(\sqrt{d})$ with d a squarefree integer.

Any element $\alpha = u + v\sqrt{d}$ of N with u, $v \in \mathbb{Z}$ will be an algebraic integer: it is a root of

$$\left(X - (u + v\sqrt{d})\right)\left(X - (u - v\sqrt{d})\right) = X^2 - 2uX + (u^2 + v^2 d) \in \mathbb{Z}[X].$$

Example: Quadratic Fields

Let $N = \mathbb{Q}(\sqrt{d})$ with d a squarefree integer.

Any element $\alpha = u + v\sqrt{d}$ of N with u, $v \in \mathbb{Z}$ will be an algebraic integer: it is a root of

$$\left(X - (u + v\sqrt{d})\right)\left(X - (u - v\sqrt{d})\right) = X^2 - 2uX + (u^2 + v^2 d) \in \mathbb{Z}[X].$$

However, these might not be all the algebraic integers:

Example: Quadratic Fields

Let $N = \mathbb{Q}(\sqrt{d})$ with d a squarefree integer.

Any element $\alpha = u + v\sqrt{d}$ of N with u, $v \in \mathbb{Z}$ will be an algebraic integer: it is a root of

$$\left(X - (u + v\sqrt{d})\right)\left(X - (u - v\sqrt{d})\right) = X^2 - 2uX + (u^2 + v^2 d) \in \mathbb{Z}[X].$$

However, these might not be all the algebraic integers:

$\alpha = \frac{1}{2}(1 + \sqrt{d})$ is a root of

$$\left(X - \frac{1}{2}(1 + \sqrt{d})\right)\left(X - \frac{1}{2}(1 - \sqrt{d})\right) = X^2 - X + \frac{1}{4}(1 - d)$$

so

$$\alpha \in O_N \Leftrightarrow d \equiv 1 \pmod{4}.$$

Theorem

Let d be a squarefree integer and $N = \mathbb{Q}(\sqrt{d})$. Then

$$O_N = \begin{cases} \mathbb{Z}[\sqrt{d}] = \{u + v\sqrt{d} : u, v \in \mathbb{Z}\} & \textit{if } d \equiv 2, 3 \pmod 4; \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{u + v\left(\frac{1+\sqrt{d}}{2}\right) : u, v \in \mathbb{Z}\right\} & \textit{if } d \equiv 1 \pmod 4. \end{cases}$$

Theorem

Let d be a squarefree integer and $N = \mathbb{Q}(\sqrt{d})$. Then

$$O_N = \begin{cases} \mathbb{Z}[\sqrt{d}] = \{u + v\sqrt{d} : u, v \in \mathbb{Z}\} & \textit{if } d \equiv 2, 3 \pmod 4; \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{u + v\left(\frac{1+\sqrt{d}}{2}\right) : u, v \in \mathbb{Z}\right\} & \textit{if } d \equiv 1 \pmod 4. \end{cases}$$

Notice that $\mathrm{Tr}_{N/\mathbb{Q}}(O_N) = \begin{cases} 2\mathbb{Z} & \text{if } d \equiv 2, 3 \pmod 4, \\ \mathbb{Z} & \text{if } d \equiv 1 \pmod 4. \end{cases}$

Theorem

Let d be a squarefree integer and $N = \mathbb{Q}(\sqrt{d})$. Then

$$O_N = \begin{cases} \mathbb{Z}[\sqrt{d}] = \{u + v\sqrt{d} : u, v \in \mathbb{Z}\} & \text{if } d \equiv 2, 3 \pmod 4; \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{u + v\left(\frac{1+\sqrt{d}}{2}\right) : u, v \in \mathbb{Z}\right\} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Notice that $\mathrm{Tr}_{N/\mathbb{Q}}(O_N) = \begin{cases} 2\mathbb{Z} & \text{if } d \equiv 2, 3 \pmod 4, \\ \mathbb{Z} & \text{if } d \equiv 1 \pmod 4. \end{cases}$

Example (Cyclotomic Fields)

Let $N = \mathbb{Q}(\zeta_m)$ with $\zeta_m = e^{2\pi i/m}$, a primitive nth root of unity. Then $O_N = \mathbb{Z}[\zeta_m]$.

Theorem

Let d be a squarefree integer and $N = \mathbb{Q}(\sqrt{d})$. Then

$$O_N = \begin{cases} \mathbb{Z}[\sqrt{d}] = \{u + v\sqrt{d} : u, v \in \mathbb{Z}\} & \textit{if } d \equiv 2, 3 \pmod 4; \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{u + v\left(\frac{1+\sqrt{d}}{2}\right) : u, v \in \mathbb{Z}\right\} & \textit{if } d \equiv 1 \pmod 4. \end{cases}$$

Notice that $\mathrm{Tr}_{N/\mathbb{Q}}(O_N) = \begin{cases} 2\mathbb{Z} & \text{if } d \equiv 2, 3 \pmod 4, \\ \mathbb{Z} & \text{if } d \equiv 1 \pmod 4. \end{cases}$

Example (Cyclotomic Fields)

Let $N = \mathbb{Q}(\zeta_m)$ with $\zeta_m = e^{2\pi i/m}$, a primitive nth root of unity. Then $O_N = \mathbb{Z}[\zeta_m]$.

We can now ask the question:

Theorem

Let d be a squarefree integer and $N = \mathbb{Q}(\sqrt{d})$. Then

$$O_N = \begin{cases} \mathbb{Z}[\sqrt{d}] = \{u + v\sqrt{d} : u, v \in \mathbb{Z}\} & \text{if } d \equiv 2, 3 \pmod 4; \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{u + v\left(\frac{1+\sqrt{d}}{2}\right) : u, v \in \mathbb{Z}\right\} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Notice that $\mathrm{Tr}_{N/\mathbb{Q}}(O_N) = \begin{cases} 2\mathbb{Z} & \text{if } d \equiv 2, 3 \pmod 4, \\ \mathbb{Z} & \text{if } d \equiv 1 \pmod 4. \end{cases}$

Example (Cyclotomic Fields)

Let $N = \mathbb{Q}(\zeta_m)$ with $\zeta_m = e^{2\pi i/m}$, a primitive nth root of unity. Then $O_N = \mathbb{Z}[\zeta_m]$.

We can now ask the question:

If $N/\mathbb{Q}$ is a Galois extension, does it have a **normal integral basis**, i.e. does there exist $\alpha \in O_N$ such that each $\beta \in O_N$ can be written uniquely as $\beta = \lambda \cdot \alpha$ for some λ in the **integral group ring** $\mathbb{Z}[G]$?

Example (Quadratic Fields)

If $N = \mathbb{Q}(\sqrt{d})$ with $d \equiv 1 \pmod 4$, the answer is **Yes**.

Example (Quadratic Fields)

If $N = \mathbb{Q}(\sqrt{d})$ *with* $d \equiv 1 \pmod 4$, *the answer is* **Yes**.

Take $\alpha = \frac{1}{2}(1+\sqrt{d})$. *Here* $G = \{\mathrm{id}, \sigma\}$ *with* $\sigma(\sqrt{d}) = -\sqrt{d}$.

$$\forall a, b \in \mathbb{Z}: \qquad a + b\left(\frac{1+\sqrt{d}}{2}\right) = (a + b + a\sigma) \cdot \left(\frac{1+\sqrt{d}}{2}\right).$$

Example (Quadratic Fields)

If $N = \mathbb{Q}(\sqrt{d})$ *with* $d \equiv 1 \pmod 4$, *the answer is* **Yes**.

Take $\alpha = \frac{1}{2}(1+\sqrt{d})$. *Here* $G = \{\mathrm{id}, \sigma\}$ *with* $\sigma(\sqrt{d}) = -\sqrt{d}$.

$$\forall a, b \in \mathbb{Z}: \qquad a + b\left(\frac{1+\sqrt{d}}{2}\right) = (a + b + a\sigma) \cdot \left(\frac{1+\sqrt{d}}{2}\right).$$

However, if $d \equiv 2, 3 \pmod 4$, *the answer is* **No**.

Example (Quadratic Fields)

If $N = \mathbb{Q}(\sqrt{d})$ *with* $d \equiv 1 \pmod 4$, *the answer is* **Yes**.

Take $\alpha = \frac{1}{2}(1+\sqrt{d})$. *Here* $G = \{\mathrm{id}, \sigma\}$ *with* $\sigma(\sqrt{d}) = -\sqrt{d}$.

$$\forall a, b \in \mathbb{Z} : \qquad a + b\left(\frac{1+\sqrt{d}}{2}\right) = (a + b + a\sigma) \cdot \left(\frac{1+\sqrt{d}}{2}\right).$$

However, if $d \equiv 2, 3 \pmod 4$, *the answer is* **No**.

If we have α *with* $\mathbb{Z}[G] \cdot \alpha = O_N$, *then*

$$(1+\sigma) \cdot \alpha = \mathrm{Tr}_{N/\mathbb{Q}}(\alpha) = \pm 1,$$

but we have seen that $\mathrm{Tr}_{N/\mathbb{Q}}(O_N) = 2\mathbb{Z}$.

Example (Quadratic Fields)

If $N = \mathbb{Q}(\sqrt{d})$ with $d \equiv 1 \pmod 4$, the answer is **Yes**.

Take $\alpha = \frac{1}{2}(1+\sqrt{d})$. Here $G = \{\mathrm{id}, \sigma\}$ with $\sigma(\sqrt{d}) = -\sqrt{d}$.

$$\forall a, b \in \mathbb{Z} : \qquad a + b\left(\frac{1+\sqrt{d}}{2}\right) = (a + b + a\sigma) \cdot \left(\frac{1+\sqrt{d}}{2}\right).$$

However, if $d \equiv 2, 3 \pmod 4$, the answer is **No**.

If we have α with $\mathbb{Z}[G] \cdot \alpha = O_N$, then

$$(1+\sigma) \cdot \alpha = \mathrm{Tr}_{N/\mathbb{Q}}(\alpha) = \pm 1,$$

but we have seen that $\mathrm{Tr}_{N/\mathbb{Q}}(O_N) = 2\mathbb{Z}$.

Example (Cyclotomic fields with prime conductor)

If $N = \mathbb{Q}(\zeta_p)$ with p prime, then $G = \{\sigma_1, \sigma_2, \ldots, \sigma_{p-1}\} \cong \mathbb{F}_p^\times$, where $\sigma_a(\zeta_p) = \zeta_p^a$, and we have $O_N = \mathbb{Z}[G] \cdot \zeta_p$.

Tame and wild extensions

We call an extension N/K of number fields **tame** if $\mathrm{Tr}_{N/K}(O_N) = O_K$; otherwise it is **wild**.

Tame and wild extensions

We call an extension N/K of number fields **tame** if $\mathrm{Tr}_{N/K}(O_N) = O_K$; otherwise it is **wild**.

As in our quadratic example, if N/K is a wild Galois extension then there cannot be a normal integral basis for N/K.

Tame and wild extensions

We call an extension N/K of number fields **tame** if $\mathrm{Tr}_{N/K}(O_N) = O_K$; otherwise it is **wild**.

As in our quadratic example, if N/K is a wild Galois extension then there cannot be a normal integral basis for N/K.

So the tame/wild distinction is fundamental for Galois module structure.

Tame and wild extensions

We call an extension N/K of number fields **tame** if $\mathrm{Tr}_{N/K}(O_N) = O_K$; otherwise it is **wild**.

As in our quadratic example, if N/K is a wild Galois extension then there cannot be a normal integral basis for N/K.

So the tame/wild distinction is fundamental for Galois module structure.

The first general result of integral Galois module structure was:

Tame and wild extensions

We call an extension N/K of number fields **tame** if $\mathrm{Tr}_{N/K}(O_N) = O_K$; otherwise it is **wild**.

As in our quadratic example, if N/K is a wild Galois extension then there cannot be a normal integral basis for N/K.

So the tame/wild distinction is fundamental for Galois module structure.

The first general result of integral Galois module structure was:

Theorem (Hilbert 1897; Speiser 1916)

If N is a tame Galois extension of $\mathbb{Q}$ whose Galois group is abelian, then $N/\mathbb{Q}$ does have a normal integral basis.

Tame and wild extensions

We call an extension N/K of number fields **tame** if $\mathrm{Tr}_{N/K}(O_N) = O_K$; otherwise it is **wild**.

As in our quadratic example, if N/K is a wild Galois extension then there cannot be a normal integral basis for N/K.

So the tame/wild distinction is fundamental for Galois module structure.

The first general result of integral Galois module structure was:

Theorem (Hilbert 1897; Speiser 1916)

If N is a tame Galois extension of $\mathbb{Q}$ whose Galois group is abelian, then $N/\mathbb{Q}$ does have a normal integral basis.

The key idea is that $N \subseteq \mathbb{Q}(\zeta_m)$ for some squarefree m.

Wild abelian extensions of $\mathbb{Q}$

If $N/\mathbb{Q}$ is a wild abelian extension, then O_N cannot be a free $\mathbb{Z}[G]$-module.

Wild abelian extensions of $\mathbb{Q}$

If $N/\mathbb{Q}$ is a wild abelian extension, then O_N cannot be a free $\mathbb{Z}[G]$-module.

But we could try replacing $\mathbb{Z}[G]$ with a bigger ring.

Wild abelian extensions of $\mathbb{Q}$

If $N/\mathbb{Q}$ is a wild abelian extension, then O_N cannot be a free $\mathbb{Z}[G]$-module.

But we could try replacing $\mathbb{Z}[G]$ with a bigger ring.

The **associated order** of O_N is

$$\mathcal{A}(N/\mathbb{Q}) = \{\lambda \in \mathbb{Q}[G] : \lambda \cdot O_N \subseteq O_N\}.$$

Wild abelian extensions of $\mathbb{Q}$

If $N/\mathbb{Q}$ is a wild abelian extension, then O_N cannot be a free $\mathbb{Z}[G]$-module.

But we could try replacing $\mathbb{Z}[G]$ with a bigger ring.

The **associated order** of O_N is

$$\mathcal{A}(N/\mathbb{Q}) = \{\lambda \in \mathbb{Q}[G] : \lambda \cdot O_N \subseteq O_N\}.$$

Then $\mathcal{A}(N/\mathbb{Q})$ is a subring of $\mathbb{Q}[G]$ containing $\mathbb{Z}[G]$, and O_N is an $\mathcal{A}(N/\mathbb{Q})$-module.

Wild abelian extensions of $\mathbb{Q}$

If $N/\mathbb{Q}$ is a wild abelian extension, then O_N cannot be a free $\mathbb{Z}[G]$-module.

But we could try replacing $\mathbb{Z}[G]$ with a bigger ring.

The **associated order** of O_N is

$$\mathcal{A}(N/\mathbb{Q}) = \{\lambda \in \mathbb{Q}[G] : \lambda \cdot O_N \subseteq O_N\}.$$

Then $\mathcal{A}(N/\mathbb{Q})$ is a subring of $\mathbb{Q}[G]$ containing $\mathbb{Z}[G]$, and O_N is an $\mathcal{A}(N/\mathbb{Q})$-module.
Also

$$\mathcal{A}(N/\mathbb{Q}) = \mathbb{Z}[G] \Leftrightarrow N/\mathbb{Q} \text{ is tame.}$$

Wild abelian extensions of $\mathbb{Q}$

If $N/\mathbb{Q}$ is a wild abelian extension, then O_N cannot be a free $\mathbb{Z}[G]$-module.

But we could try replacing $\mathbb{Z}[G]$ with a bigger ring.

The **associated order** of O_N is

$$\mathcal{A}(N/\mathbb{Q}) = \{\lambda \in \mathbb{Q}[G] : \lambda \cdot O_N \subseteq O_N\}.$$

Then $\mathcal{A}(N/\mathbb{Q})$ is a subring of $\mathbb{Q}[G]$ containing $\mathbb{Z}[G]$, and O_N is an $\mathcal{A}(N/\mathbb{Q})$-module.
Also

$$\mathcal{A}(N/\mathbb{Q}) = \mathbb{Z}[G] \Leftrightarrow N/\mathbb{Q} \text{ is tame.}$$

Theorem (Leopoldt, 1959)

If N is a wild Galois extension of $\mathbb{Q}$ whose Galois group is abelian, then O_N is a free module over $\mathcal{A}(N/\mathbb{Q})$.

Wild abelian extensions of $\mathbb{Q}$

If $N/\mathbb{Q}$ is a wild abelian extension, then O_N cannot be a free $\mathbb{Z}[G]$-module.

But we could try replacing $\mathbb{Z}[G]$ with a bigger ring.

The **associated order** of O_N is

$$\mathcal{A}(N/\mathbb{Q}) = \{\lambda \in \mathbb{Q}[G] : \lambda \cdot O_N \subseteq O_N\}.$$

Then $\mathcal{A}(N/\mathbb{Q})$ is a subring of $\mathbb{Q}[G]$ containing $\mathbb{Z}[G]$, and O_N is an $\mathcal{A}(N/\mathbb{Q})$-module.
Also

$$\mathcal{A}(N/\mathbb{Q}) = \mathbb{Z}[G] \Leftrightarrow N/\mathbb{Q} \text{ is tame.}$$

Theorem (Leopoldt, 1959)

If N is a wild Galois extension of $\mathbb{Q}$ whose Galois group is abelian, then O_N is a free module over $\mathcal{A}(N/\mathbb{Q})$.

The key idea is that $N \subseteq \mathbb{Q}(\zeta_m)$ for some m.

Example (Wild quadratic extensions)

If $N = \mathbb{Q}(\sqrt{d})$ *with* $d \equiv 2, 3 \pmod 4$ *then*

$$\mathcal{A}(N/\mathbb{Q}) = \mathbb{Z} \cdot \left(\frac{1+\sigma}{2}\right) + \mathbb{Z} \cdot \left(\frac{1-\sigma}{2}\right).$$

Example (Wild quadratic extensions)

If $N = \mathbb{Q}(\sqrt{d})$ *with* $d \equiv 2, 3 \pmod 4$ *then*

$$\mathcal{A}(N/\mathbb{Q}) = \mathbb{Z} \cdot \left(\frac{1+\sigma}{2}\right) + \mathbb{Z} \cdot \left(\frac{1-\sigma}{2}\right).$$

This is the maximal order in $\mathbb{Q}[C_2]$*. We have*

$$O_N = \mathcal{A}(N/\mathbb{Q}) \cdot (1 + \sqrt{d}).$$

Example (Wild quadratic extensions)

If $N = \mathbb{Q}(\sqrt{d})$ *with* $d \equiv 2, 3 \pmod 4$ *then*

$$\mathcal{A}(N/\mathbb{Q}) = \mathbb{Z} \cdot \left(\frac{1+\sigma}{2}\right) + \mathbb{Z} \cdot \left(\frac{1-\sigma}{2}\right).$$

This is the maximal order in $\mathbb{Q}[C_2]$. *We have*

$$O_N = \mathcal{A}(N/\mathbb{Q}) \cdot (1 + \sqrt{d}).$$

The Hilbert-Speiser Theorem and Leopoldt's Theorem mean we have a good understanding of Galois module structure for abelian extensions of $\mathbb{Q}$.

Example (Wild quadratic extensions)

If $N = \mathbb{Q}(\sqrt{d})$ *with* $d \equiv 2, 3 \pmod 4$ *then*

$$\mathcal{A}(N/\mathbb{Q}) = \mathbb{Z} \cdot \left(\frac{1+\sigma}{2}\right) + \mathbb{Z} \cdot \left(\frac{1-\sigma}{2}\right).$$

This is the maximal order in $\mathbb{Q}[C_2]$*. We have*

$$O_N = \mathcal{A}(N/\mathbb{Q}) \cdot (1 + \sqrt{d}).$$

The Hilbert-Speiser Theorem and Leopoldt's Theorem mean we have a good understanding of Galois module structure for abelian extensions of $\mathbb{Q}$.

We would like to generalise in two directions:

Example (Wild quadratic extensions)

If $N = \mathbb{Q}(\sqrt{d})$ with $d \equiv 2, 3 \pmod 4$ then

$$\mathcal{A}(N/\mathbb{Q}) = \mathbb{Z} \cdot \left(\frac{1+\sigma}{2}\right) + \mathbb{Z} \cdot \left(\frac{1-\sigma}{2}\right).$$

This is the maximal order in $\mathbb{Q}[C_2]$. We have

$$O_N = \mathcal{A}(N/\mathbb{Q}) \cdot (1 + \sqrt{d}).$$

The Hilbert-Speiser Theorem and Leopoldt's Theorem mean we have a good understanding of Galois module structure for abelian extensions of $\mathbb{Q}$.

We would like to generalise in two directions:

- non-abelian Galois groups;

Example (Wild quadratic extensions)

If $N = \mathbb{Q}(\sqrt{d})$ *with* $d \equiv 2, 3 \pmod 4$ *then*

$$\mathcal{A}(N/\mathbb{Q}) = \mathbb{Z} \cdot \left(\frac{1+\sigma}{2}\right) + \mathbb{Z} \cdot \left(\frac{1-\sigma}{2}\right).$$

This is the maximal order in $\mathbb{Q}[C_2]$. *We have*

$$O_N = \mathcal{A}(N/\mathbb{Q}) \cdot (1 + \sqrt{d}).$$

The Hilbert-Speiser Theorem and Leopoldt's Theorem mean we have a good understanding of Galois module structure for abelian extensions of $\mathbb{Q}$.

We would like to generalise in two directions:

- non-abelian Galois groups;
- base fields $K \supset \mathbb{Q}$;

Example (Wild quadratic extensions)

If $N = \mathbb{Q}(\sqrt{d})$ *with* $d \equiv 2, 3 \pmod 4$ *then*

$$\mathcal{A}(N/\mathbb{Q}) = \mathbb{Z} \cdot \left(\frac{1+\sigma}{2}\right) + \mathbb{Z} \cdot \left(\frac{1-\sigma}{2}\right).$$

This is the maximal order in $\mathbb{Q}[C_2]$*. We have*

$$O_N = \mathcal{A}(N/\mathbb{Q}) \cdot (1 + \sqrt{d}).$$

The Hilbert-Speiser Theorem and Leopoldt's Theorem mean we have a good understanding of Galois module structure for abelian extensions of $\mathbb{Q}$.

We would like to generalise in two directions:

- non-abelian Galois groups;
- base fields $K \supset \mathbb{Q}$;

(both for tame and wild extensions).

A tame non-abelian case

For tame Galois extensions $N/\mathbb{Q}$ with $\mathrm{Gal}(N/\mathbb{Q}) \cong Q_8$ (the quaternion group of order 8), calculations of Martinet (1971) showed that there is a normal integral basis in some cases, but not in others.

A tame non-abelian case

For tame Galois extensions $N/\mathbb{Q}$ with $\mathrm{Gal}(N/\mathbb{Q}) \cong Q_8$ (the quaternion group of order 8), calculations of Martinet (1971) showed that there is a normal integral basis in some cases, but not in others.

So being tame does not guarantee the existence of a normal integral basis.

A tame non-abelian case

For tame Galois extensions $N/\mathbb{Q}$ with $\mathrm{Gal}(N/\mathbb{Q}) \cong Q_8$ (the quaternion group of order 8), calculations of Martinet (1971) showed that there is a normal integral basis in some cases, but not in others.

So being tame does not guarantee the existence of a normal integral basis.

Question: What determines which tame Q_8-extensions do have a normal integral basis?

Digression: irreducible characters and L-functions

Attached to a finite group G are certain functions $\chi : G \to \mathbb{C}$ called **irreducible characters.** Some of these may be **symplectic**.

Digression: irreducible characters and L-functions

Attached to a finite group G are certain functions $\chi : G \to \mathbb{C}$ called **irreducible characters.** Some of these may be **symplectic**.

There are no irreducible symplectic characters if G is abelian or $|G|$ is odd.

Digression: irreducible characters and L-functions

Attached to a finite group G are certain functions $\chi : G \to \mathbb{C}$ called **irreducible characters.** Some of these may be **symplectic**.

There are no irreducible symplectic characters if G is abelian or $|G|$ is odd.

The group Q_8 has just one irreducible symplectic character.

Digression: irreducible characters and L-functions

Attached to a finite group G are certain functions $\chi : G \to \mathbb{C}$ called **irreducible characters.** Some of these may be **symplectic**.

There are no irreducible symplectic characters if G is abelian or $|G|$ is odd.

The group Q_8 has just one irreducible symplectic character.

If N/K is a Galois extension of number fields with Galois group G, then for each irreducible character χ of G there is a complex function $L(s, N/K, \chi)$ called the Artin L-function.

The **simplest possible example** is when $N = K = \mathbb{Q}$, so $G = \{e\}$, with just one irreducible character, χ_0.

The **simplest possible example** is when $N = K = \mathbb{Q}$, so $G = \{e\}$, with just one irreducible character, χ_0. Then

$$L(s, \mathbb{Q}/\mathbb{Q}, \chi_0) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}},$$

where $n^s = e^{s \log(n)}$ for $s \in \mathbb{C}$.

The **simplest possible example** is when $N = K = \mathbb{Q}$, so $G = \{e\}$, with just one irreducible character, χ_0. Then

$$L(s, \mathbb{Q}/\mathbb{Q}, \chi_0) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}},$$

where $n^s = e^{s \log(n)}$ for $s \in \mathbb{C}$.

This is the famous **Riemann Zeta Function** $\zeta(s)$.

The **simplest possible example** is when $N = K = \mathbb{Q}$, so $G = \{e\}$, with just one irreducible character, χ_0. Then

$$L(s, \mathbb{Q}/\mathbb{Q}, \chi_0) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}},$$

where $n^s = e^{s \log(n)}$ for $s \in \mathbb{C}$.

This is the famous **Riemann Zeta Function** $\zeta(s)$.

The series (and the product) converge for $\mathrm{Re}(s) > 1$.

The **simplest possible example** is when $N = K = \mathbb{Q}$, so $G = \{e\}$, with just one irreducible character, χ_0. Then

$$L(s, \mathbb{Q}/\mathbb{Q}, \chi_0) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}},$$

where $n^s = e^{s \log(n)}$ for $s \in \mathbb{C}$.

This is the famous **Riemann Zeta Function** $\zeta(s)$.

The series (and the product) converge for $\mathrm{Re}(s) > 1$.

However, $\zeta(s)$ is defined for all $s \in \mathbb{C}$ (except for a pole at $s = 1$) by analytic continuation, and it has a functional equation relating $\zeta(s)$ to $\zeta(1 - s)$.

The **simplest possible example** is when $N = K = \mathbb{Q}$, so $G = \{e\}$, with just one irreducible character, χ_0. Then

$$L(s, \mathbb{Q}/\mathbb{Q}, \chi_0) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}},$$

where $n^s = e^{s \log(n)}$ for $s \in \mathbb{C}$.

This is the famous **Riemann Zeta Function** $\zeta(s)$.

The series (and the product) converge for $\mathrm{Re}(s) > 1$.

However, $\zeta(s)$ is defined for all $s \in \mathbb{C}$ (except for a pole at $s = 1$) by analytic continuation, and it has a functional equation relating $\zeta(s)$ to $\zeta(1 - s)$.

In general, each Artin L-function $L(s, N/K, \chi)$ is a meromorphic function on the whole of $\mathbb{C}$, and has a functional equation.

The **simplest possible example** is when $N = K = \mathbb{Q}$, so $G = \{e\}$, with just one irreducible character, χ_0. Then

$$L(s, \mathbb{Q}/\mathbb{Q}, \chi_0) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}},$$

where $n^s = e^{s \log(n)}$ for $s \in \mathbb{C}$.

This is the famous **Riemann Zeta Function** $\zeta(s)$.

The series (and the product) converge for $\mathrm{Re}(s) > 1$.

However, $\zeta(s)$ is defined for all $s \in \mathbb{C}$ (except for a pole at $s = 1$) by analytic continuation, and it has a functional equation relating $\zeta(s)$ to $\zeta(1 - s)$.

In general, each Artin L-function $L(s, N/K, \chi)$ is a meromorphic function on the whole of $\mathbb{C}$, and has a functional equation.

The functional equation for $L(s, N/K, \chi)$ involves a number $W(N/K, \chi)$ called the root number.

The **simplest possible example** is when $N = K = \mathbb{Q}$, so $G = \{e\}$, with just one irreducible character, χ_0. Then

$$L(s, \mathbb{Q}/\mathbb{Q}, \chi_0) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}},$$

where $n^s = e^{s \log(n)}$ for $s \in \mathbb{C}$.

This is the famous **Riemann Zeta Function** $\zeta(s)$.

The series (and the product) converge for $\mathrm{Re}(s) > 1$.

However, $\zeta(s)$ is defined for all $s \in \mathbb{C}$ (except for a pole at $s = 1$) by analytic continuation, and it has a functional equation relating $\zeta(s)$ to $\zeta(1 - s)$.

In general, each Artin L-function $L(s, N/K, \chi)$ is a meromorphic function on the whole of $\mathbb{C}$, and has a functional equation.

The functional equation for $L(s, N/K, \chi)$ involves a number $W(N/K, \chi)$ called the root number.

If χ is an irreducible symplectic character then $W(N/K, \chi) = \pm 1$.

Back to quaternion extensions:

Back to quaternion extensions:

Theorem (Conjectured Serre 1971; proved Fröhlich, 1972)

Let $N/\mathbb{Q}$ be a tame Galois extension with Galois group Q_8, and let χ be the irreducible symplectic character of Q_8. Then

$$O_N \text{ is free over } \mathbb{Z}[Q_8] \Leftrightarrow W(N/\mathbb{Q}, \chi) = +1.$$

Back to quaternion extensions:

Theorem (Conjectured Serre 1971; proved Fröhlich, 1972)

Let $N/\mathbb{Q}$ be a tame Galois extension with Galois group Q_8, and let χ be the irreducible symplectic character of Q_8. Then

$$O_N \text{ is free over } \mathbb{Z}[Q_8] \Leftrightarrow W(N/\mathbb{Q}, \chi) = +1.$$

This shows an unexpected connection between algebraic information (whether N has a normal integral basis) and anayltic information (root numbers of L-functions).

Back to quaternion extensions:

Theorem (Conjectured Serre 1971; proved Fröhlich, 1972)

Let $N/\mathbb{Q}$ be a tame Galois extension with Galois group Q_8, and let χ be the irreducible symplectic character of Q_8. Then

$$O_N \text{ is free over } \mathbb{Z}[Q_8] \Leftrightarrow W(N/\mathbb{Q}, \chi) = +1.$$

This shows an unexpected connection between algebraic information (whether N has a normal integral basis) and anayltic information (root numbers of L-functions).

To fit this into a general theory, we need to understand the significance of tameness.

Locally free $\mathbb{Z}[G]$-modules

For each prime number p, we define the **localisation** of $\mathbb{Z}$ at p:

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : \quad a, b \in \mathbb{Z}, \quad p \nmid b \right\}.$$

Locally free $\mathbb{Z}[G]$-modules

For each prime number p, we define the **localisation** of $\mathbb{Z}$ at p:

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : \quad a, b \in \mathbb{Z}, \quad p \nmid b \right\}.$$

Then $\mathbb{Z}_{(p)}$ is a **local ring**, i.e. a ring with only one maximal ideal, namely $p\mathbb{Z}_{(p)}$. The field of fractions of $\mathbb{Z}_{(p)}$ is $\mathbb{Q}$.

Locally free $\mathbb{Z}[G]$-modules

For each prime number p, we define the **localisation** of $\mathbb{Z}$ at p:

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : \quad a, b \in \mathbb{Z}, \quad p \nmid b \right\}.$$

Then $\mathbb{Z}_{(p)}$ is a **local ring**, i.e. a ring with only one maximal ideal, namely $p\mathbb{Z}_{(p)}$. The field of fractions of $\mathbb{Z}_{(p)}$ is $\mathbb{Q}$.

The only prime number in $\mathbb{Z}$ which "survives" in $\mathbb{Z}_{(p)}$ is p itself; all other primes become units in $\mathbb{Z}_{(p)}$.

Locally free $\mathbb{Z}[G]$-modules

For each prime number p, we define the **localisation** of $\mathbb{Z}$ at p:

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : \quad a, b \in \mathbb{Z}, \quad p \nmid b \right\}.$$

Then $\mathbb{Z}_{(p)}$ is a **local ring**, i.e. a ring with only one maximal ideal, namely $p\mathbb{Z}_{(p)}$. The field of fractions of $\mathbb{Z}_{(p)}$ is $\mathbb{Q}$.

The only prime number in $\mathbb{Z}$ which "survives" in $\mathbb{Z}_{(p)}$ is p itself; all other primes become units in $\mathbb{Z}_{(p)}$.

(We could also take completions and work with the p-adic integers $\mathbb{Z}_p$ instead of $\mathbb{Z}_{(p)}$. The field of fractions of $\mathbb{Z}_p$ is the the field $\mathbb{Q}_p$ of p-adic numbers.)

For a Galois extension $N/\mathbb{Q}$ with $\mathrm{Gal}(N/\mathbb{Q}) = G$, we know that O_N is a $\mathbb{Z}[G]$-module. We can extend scalars from $\mathbb{Z}$ to $\mathbb{Z}_{(p)}$, so that $O_{N,(p)}$ is a $\mathbb{Z}_{(p)}[G]$-module.

For a Galois extension $N/\mathbb{Q}$ with $\mathrm{Gal}(N/\mathbb{Q}) = G$, we know that O_N is a $\mathbb{Z}[G]$-module. We can extend scalars from $\mathbb{Z}$ to $\mathbb{Z}_{(p)}$, so that $O_{N,(p)}$ is a $\mathbb{Z}_{(p)}[G]$-module.

Then

$$L/\mathbb{Q} \text{ is tame} \Leftrightarrow O_{N,(p)} \text{ is a free } \mathbb{Z}_{(p)}[G]\text{-module for each prime } p.$$

We then say O_N is a **locally free** $\mathbb{Z}[G]$-module.

For a Galois extension $N/\mathbb{Q}$ with $\mathrm{Gal}(N/\mathbb{Q}) = G$, we know that O_N is a $\mathbb{Z}[G]$-module. We can extend scalars from $\mathbb{Z}$ to $\mathbb{Z}_{(p)}$, so that $O_{N,(p)}$ is a $\mathbb{Z}_{(p)}[G]$-module.

Then

$$L/\mathbb{Q} \text{ is tame} \Leftrightarrow O_{N,(p)} \text{ is a free } \mathbb{Z}_{(p)}[G]\text{-module for each prime } p.$$

We then say O_N is a **locally free** $\mathbb{Z}[G]$-module.

So $N/\mathbb{Q}$ has a normal integral basis if and only if the locally free $\mathbb{Z}[G]$-module O_N is free.

For a Galois extension $N/\mathbb{Q}$ with $\mathrm{Gal}(N/\mathbb{Q}) = G$, we know that O_N is a $\mathbb{Z}[G]$-module. We can extend scalars from $\mathbb{Z}$ to $\mathbb{Z}_{(p)}$, so that $O_{N,(p)}$ is a $\mathbb{Z}_{(p)}[G]$-module.

Then

$$L/\mathbb{Q} \text{ is tame} \Leftrightarrow O_{N,(p)} \text{ is a free } \mathbb{Z}_{(p)}[G]\text{-module for each prime } p.$$

We then say O_N is a **locally free** $\mathbb{Z}[G]$-module.

So $N/\mathbb{Q}$ has a normal integral basis if and only if the locally free $\mathbb{Z}[G]$-module O_N is free.

Fröhlich constructed a finite abelian group $\mathrm{Cl}(\mathbb{Z}[G])$ which classifies locally free $\mathbb{Z}[G]$-modules (up to stable isomorphism).

For a Galois extension $N/\mathbb{Q}$ with $\mathrm{Gal}(N/\mathbb{Q}) = G$, we know that O_N is a $\mathbb{Z}[G]$-module. We can extend scalars from $\mathbb{Z}$ to $\mathbb{Z}_{(p)}$, so that $O_{N,(p)}$ is a $\mathbb{Z}_{(p)}[G]$-module.

Then

$$L/\mathbb{Q} \text{ is tame} \Leftrightarrow O_{N,(p)} \text{ is a free } \mathbb{Z}_{(p)}[G]\text{-module for each prime } p.$$

We then say O_N is a **locally free** $\mathbb{Z}[G]$-module.

So $N/\mathbb{Q}$ has a normal integral basis if and only if the locally free $\mathbb{Z}[G]$-module O_N is free.

Fröhlich constructed a finite abelian group $\mathrm{Cl}(\mathbb{Z}[G])$ which classifies locally free $\mathbb{Z}[G]$-modules (up to stable isomorphism).

We now consider tame Galois extensions N/K (with base field $K \supseteq \mathbb{Q}$), and consider O_N as a locally free $\mathbb{Z}[G]$-module of rank $[K : \mathbb{Q}]$.

The main theorem of tame Galois module structure

Theorem (Taylor, 1981)

For a tame Galois extension N/K of number fields, the class of O_N in $\mathrm{Cl}(\mathbb{Z}[G])$ is determined by the $W(N/K, \chi)$ for the irreducible symplectic characters χ of G. In particular, if G has no such characters, then O_N is a free $\mathbb{Z}[G]$-module.

Relative tame Galois Module Structure:

What can we say about O_N as an $O_K[G]$-module (instead of $\mathbb{Z}[G]$-module)?

Relative tame Galois Module Structure:

What can we say about O_N as an $O_K[G]$-module (instead of $\mathbb{Z}[G]$-module)?

It is locally free of rank 1, and determines a class in the locally free classgroup $\mathrm{Cl}(O_K[G])$.

Relative tame Galois Module Structure:

What can we say about O_N as an $O_K[G]$-module (instead of $\mathbb{Z}[G]$-module)?

It is locally free of rank 1, and determines a class in the locally free classgroup $\mathrm{Cl}(O_K[G])$.

In general, this class is not determined by analytic invariants. Instead, we can ask which classes in $\mathrm{Cl}(O_K[G])$ are obtained as N varies over all tame G-extensions of K. This gives the set of **realisable classes** $\mathcal{R}(O_K[G])$.

Relative tame Galois Module Structure:

What can we say about O_N as an $O_K[G]$-module (instead of $\mathbb{Z}[G]$-module)?

It is locally free of rank 1, and determines a class in the locally free classgroup $\mathrm{Cl}(O_K[G])$.

In general, this class is not determined by analytic invariants. Instead, we can ask which classes in $\mathrm{Cl}(O_K[G])$ are obtained as N varies over all tame G-extensions of K. This gives the set of **realisable classes** $\mathcal{R}(O_K[G])$.

McCulloh (1987) determined $\mathcal{R}(O_K[G])$ when G is abelian.

Relative tame Galois Module Structure:

What can we say about O_N as an $O_K[G]$-module (instead of $\mathbb{Z}[G]$-module)?

It is locally free of rank 1, and determines a class in the locally free classgroup $\mathrm{Cl}(O_K[G])$.

In general, this class is not determined by analytic invariants. Instead, we can ask which classes in $\mathrm{Cl}(O_K[G])$ are obtained as N varies over all tame G-extensions of K. This gives the set of **realisable classes** $\mathcal{R}(O_K[G])$.

McCulloh (1987) determined $\mathcal{R}(O_K[G])$ when G is abelian.

There are similar results for some non-abelian groups G, e.g. for certain metabelian groups $G = (C_p^r) \rtimes C_m$ (with $\zeta_p \in K$); cf. Byott and Sodaïgui (2013).

Relative tame Galois Module Structure:

What can we say about O_N as an $O_K[G]$-module (instead of $\mathbb{Z}[G]$-module)?

It is locally free of rank 1, and determines a class in the locally free classgroup $\mathrm{Cl}(O_K[G])$.

In general, this class is not determined by analytic invariants. Instead, we can ask which classes in $\mathrm{Cl}(O_K[G])$ are obtained as N varies over all tame G-extensions of K. This gives the set of **realisable classes** $\mathcal{R}(O_K[G])$.

McCulloh (1987) determined $\mathcal{R}(O_K[G])$ when G is abelian.

There are similar results for some non-abelian groups G, e.g. for certain metabelian groups $G = (C_p^r) \rtimes C_m$ (with $\zeta_p \in K$); cf. Byott and Sodaïgui (2013).

It is expected that $\mathcal{R}(O_K[G])$ is always a subgroup of $O_K[G]$.

Relative tame Galois Module Structure:

What can we say about O_N as an $O_K[G]$-module (instead of $\mathbb{Z}[G]$-module)?

It is locally free of rank 1, and determines a class in the locally free classgroup $\mathrm{Cl}(O_K[G])$.

In general, this class is not determined by analytic invariants. Instead, we can ask which classes in $\mathrm{Cl}(O_K[G])$ are obtained as N varies over all tame G-extensions of K. This gives the set of **realisable classes** $\mathcal{R}(O_K[G])$.

McCulloh (1987) determined $\mathcal{R}(O_K[G])$ when G is abelian.

There are similar results for some non-abelian groups G, e.g. for certain metabelian groups $G = (C_p^r) \rtimes C_m$ (with $\zeta_p \in K$); cf. Byott and Sodaïgui (2013).

It is expected that $\mathcal{R}(O_K[G])$ is always a subgroup of $O_K[G]$.

In general, we do not even know it is non-empty.

Wild extensions

If N/K is a wild Galois extension and $G = \mathrm{Gal}(N/K)$, then O_N cannot be even locally free over $O_K[G]$.

Wild extensions

If N/K is a wild Galois extension and $G = \mathrm{Gal}(N/K)$, then O_N cannot be even locally free over $O_K[G]$.

We can ask if O_N is locally free over its associated order

$$\mathcal{A}_{N/K} = \{\lambda \in K[G] : \lambda \cdot O_N \subseteq O_N\}.$$

Wild extensions

If N/K is a wild Galois extension and $G = \mathrm{Gal}(N/K)$, then O_N cannot be even locally free over $O_K[G]$.

We can ask if O_N is locally free over its associated order

$$\mathcal{A}_{N/K} = \{\lambda \in K[G] : \lambda \cdot O_N \subseteq O_N\}.$$

This is a "local" question (i.e. it depends on one prime p at a time), so we can localise (and complete) at p and work in a p-adic setting.

Wild extensions

If N/K is a wild Galois extension and $G = \mathrm{Gal}(N/K)$, then O_N cannot be even locally free over $O_K[G]$.

We can ask if O_N is locally free over its associated order

$$\mathcal{A}_{N/K} = \{\lambda \in K[G] : \lambda \cdot O_N \subseteq O_N\}.$$

This is a "local" question (i.e. it depends on one prime p at a time), so we can localise (and complete) at p and work in a p-adic setting.

Changing notation, let K be a finite extension of $\mathbb{Q}_p$, with ring of integers O_K, and let N/K be a Galois extension with Galois group G.

Wild extensions

If N/K is a wild Galois extension and $G = \mathrm{Gal}(N/K)$, then O_N cannot be even locally free over $O_K[G]$.

We can ask if O_N is locally free over its associated order

$$\mathcal{A}_{N/K} = \{\lambda \in K[G] : \lambda \cdot O_N \subseteq O_N\}.$$

This is a "local" question (i.e. it depends on one prime p at a time), so we can localise (and complete) at p and work in a p-adic setting.

Changing notation, let K be a finite extension of $\mathbb{Q}_p$, with ring of integers O_K, and let N/K be a Galois extension with Galois group G.

We just consider the simplest interesting case: $G \cong C_p$.

O_K is a Principal Ideal Domain with a unique maximal ideal.

O_K is a Principal Ideal Domain with a unique maximal ideal.

Let π_K be a generator for this ideal. (If $K = \mathbb{Q}_p$ we can choose $\pi_K = p$).

O_K is a Principal Ideal Domain with a unique maximal ideal.

Let π_K be a generator for this ideal. (If $K = \mathbb{Q}_p$ we can choose $\pi_K = p$).

If $x \in K\backslash\{0\}$, we can write $x = u\pi_K^m$ for some unit $u \in O_K^\times$ and some $m \in \mathbb{Z}$.

O_K is a Principal Ideal Domain with a unique maximal ideal.

Let π_K be a generator for this ideal. (If $K = \mathbb{Q}_p$ we can choose $\pi_K = p$).

If $x \in K \backslash \{0\}$, we can write $x = u\pi_K^m$ for some unit $u \in O_K^\times$ and some $m \in \mathbb{Z}$.

We have $x \in O_K \Leftrightarrow m \geq 0$.

O_K is a Principal Ideal Domain with a unique maximal ideal.

Let π_K be a generator for this ideal. (If $K = \mathbb{Q}_p$ we can choose $\pi_K = p$).

If $x \in K\backslash\{0\}$, we can write $x = u\pi_K^m$ for some unit $u \in O_K^\times$ and some $m \in \mathbb{Z}$.

We have $x \in O_K \Leftrightarrow m \geq 0$.

We define the valuation $v_K : K \to \mathbb{Z} \cup \{\infty\}$ by

$$v_K(x) = \begin{cases} m & \text{if } x \neq 0; \\ \infty & \text{if } x = 0. \end{cases}$$

O_K is a Principal Ideal Domain with a unique maximal ideal.

Let π_K be a generator for this ideal. (If $K = \mathbb{Q}_p$ we can choose $\pi_K = p$).

If $x \in K \backslash \{0\}$, we can write $x = u\pi_K^m$ for some unit $u \in O_K^\times$ and some $m \in \mathbb{Z}$.

We have $x \in O_K \Leftrightarrow m \geq 0$.

We define the valuation $v_K : K \to \mathbb{Z} \cup \{\infty\}$ by

$$v_K(x) = \begin{cases} m & \text{if } x \neq 0; \\ \infty & \text{if } x = 0. \end{cases}$$

Similarly, O_N has a unique maximal ideal $\pi_N O_N$, and we have a valuation $v_N : N \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$.

There are two possibilities for our degree p extension N/K: either $v_N(\pi_K) = 1$ or $v_N(\pi_K) = p$.

There are two possibilities for our degree p extension N/K: either $v_N(\pi_K) = 1$ or $v_N(\pi_K) = p$.

If $v_N(\pi_K) = 1$ then N/K is **unramified**. Then it is tame and O_N is free over $\mathcal{A}(N/K) = O_K[G]$.

There are two possibilities for our degree p extension N/K: either $v_N(\pi_K) = 1$ or $v_N(\pi_K) = p$.

If $v_N(\pi_K) = 1$ then N/K is **unramified**. Then it is tame and O_N is free over $\mathcal{A}(N/K) = O_K[G]$.

If $v_N(\pi_K) = p$ then N/K is **totally ramified** and $\mathcal{A}(N/K) \supsetneq O_K[G]$.

There are two possibilities for our degree p extension N/K: either $v_N(\pi_K) = 1$ or $v_N(\pi_K) = p$.

If $v_N(\pi_K) = 1$ then N/K is **unramified**. Then it is tame and O_N is free over $\mathcal{A}(N/K) = O_K[G]$.

If $v_N(\pi_K) = p$ then N/K is **totally ramified** and $\mathcal{A}(N/K) \supsetneq O_K[G]$.

Let $G = \langle \sigma \rangle \cong C_p$, and let

$$b = v_N((\sigma - 1) \cdot \pi_N) - 1 \in \mathbb{Z}_{>0}.$$

There are two possibilities for our degree p extension N/K: either $v_N(\pi_K) = 1$ or $v_N(\pi_K) = p$.

If $v_N(\pi_K) = 1$ then N/K is **unramified**. Then it is tame and O_N is free over $\mathcal{A}(N/K) = O_K[G]$.

If $v_N(\pi_K) = p$ then N/K is **totally ramified** and $\mathcal{A}(N/K) \supsetneq O_K[G]$.

Let $G = \langle \sigma \rangle \cong C_p$, and let

$$b = v_N((\sigma - 1) \cdot \pi_N) - 1 \in \mathbb{Z}_{>0}.$$

Then, for all $x \in N \backslash \{0\}$,

$$v_N((\sigma - 1) \cdot x) \quad \begin{cases} = v_N(x) + b & \text{if } p \nmid v_N(x), \\ > v_N(x) + b & \text{if } p \mid v_N(x). \end{cases}$$

There are two possibilities for our degree p extension N/K: either $v_N(\pi_K) = 1$ or $v_N(\pi_K) = p$.

If $v_N(\pi_K) = 1$ then N/K is **unramified**. Then it is tame and O_N is free over $\mathcal{A}(N/K) = O_K[G]$.

If $v_N(\pi_K) = p$ then N/K is **totally ramified** and $\mathcal{A}(N/K) \supsetneq O_K[G]$.

Let $G = \langle \sigma \rangle \cong C_p$, and let

$$b = v_N((\sigma - 1) \cdot \pi_N) - 1 \in \mathbb{Z}_{>0}.$$

Then, for all $x \in N \backslash \{0\}$,

$$v_N((\sigma - 1) \cdot x) \quad \begin{cases} = v_N(x) + b & \text{if } p \nmid v_N(x), \\ > v_N(x) + b & \text{if } p \mid v_N(x). \end{cases}$$

b is called the **ramification break** of N/K.

There are two possibilities for our degree p extension N/K: either $v_N(\pi_K) = 1$ or $v_N(\pi_K) = p$.

If $v_N(\pi_K) = 1$ then N/K is **unramified**. Then it is tame and O_N is free over $\mathcal{A}(N/K) = O_K[G]$.

If $v_N(\pi_K) = p$ then N/K is **totally ramified** and $\mathcal{A}(N/K) \supsetneq O_K[G]$.

Let $G = \langle \sigma \rangle \cong C_p$, and let

$$b = v_N((\sigma - 1) \cdot \pi_N) - 1 \in \mathbb{Z}_{>0}.$$

Then, for all $x \in N \backslash \{0\}$,

$$v_N((\sigma - 1) \cdot x) \quad \begin{cases} = v_N(x) + b & \text{if } p \nmid v_N(x), \\ > v_N(x) + b & \text{if } p \mid v_N(x). \end{cases}$$

b is called the **ramification break** of N/K.

It turns out that the possible values for b are:

$$1 \leq b \leq \frac{ep}{p-1} \text{ where } e = v_{\mathbb{Q}_p}(\pi_K),$$

$$p \nmid b \text{ unless } b = ep/(p-1).$$

To avoid special cases, assume that b is not too close to its upper bound

To avoid special cases, assume that b is not too close to its upper bound

$$b < \frac{ep}{p-1} - 1.$$

To avoid special cases, assume that b is not too close to its upper bound

$$b < \frac{ep}{p-1} - 1.$$

Then O_N has O_K-basis 1, π_N, π_N^2, $\ldots$, π_N^{p-1}.

To avoid special cases, assume that b is not too close to its upper bound

$$b < \frac{ep}{p-1} - 1.$$

Then O_N has O_K-basis $1, \pi_N, \pi_N^2, \ldots, \pi_N^{p-1}$.

Also, $K[G]$ has a K-basis $1, \sigma - 1, (\sigma - 1)^2, \ldots, (\sigma - 1)^{p-1}$.

To avoid special cases, assume that b is not too close to its upper bound

$$b < \frac{ep}{p-1} - 1.$$

Then O_N has O_K-basis $1, \pi_N, \pi_N^2, \ldots, \pi_N^{p-1}$.

Also, $K[G]$ has a K-basis $1, \sigma - 1, (\sigma-1)^2, \ldots, (\sigma-1)^{p-1}$.

For $0 \le j \le p-1$, let $r(j) \in \mathbb{Z}$ be as large as possible with

$$\pi_K^{-r(j)}(\sigma - 1)^j \in \mathcal{A}(N/K).$$

To avoid special cases, assume that b is not too close to its upper bound

$$b < \frac{ep}{p-1} - 1.$$

Then O_N has O_K-basis 1, π_N, π_N^2, ..., π_N^{p-1}.

Also, $K[G]$ has a K-basis 1, $\sigma - 1$, $(\sigma-1)^2$, ..., $(\sigma-1)^{p-1}$.

For $0 \le j \le p-1$, let $r(j) \in \mathbb{Z}$ be as large as possible with

$$\pi_K^{-r(j)}(\sigma-1)^j \in \mathcal{A}(N/K).$$

This means

$$\frac{(\sigma-1)^j}{\pi_K^{r(j)}} \cdot \pi_N^i \in O_N \text{ for } 0 \le i \le p-1,$$

To avoid special cases, assume that b is not too close to its upper bound

$$b < \frac{ep}{p-1} - 1.$$

Then O_N has O_K-basis $1, \pi_N, \pi_N^2, \ldots, \pi_N^{p-1}$.

Also, $K[G]$ has a K-basis $1, \sigma - 1, (\sigma-1)^2, \ldots, (\sigma-1)^{p-1}$.

For $0 \le j \le p-1$, let $r(j) \in \mathbb{Z}$ be as large as possible with

$$\pi_K^{-r(j)}(\sigma-1)^j \in \mathcal{A}(N/K).$$

This means

$$\frac{(\sigma-1)^j}{\pi_K^{r(j)}} \cdot \pi_N^i \in O_N \text{ for } 0 \le i \le p-1,$$

so that

$$-pr + bj + i \ge 0 \text{ if } i \equiv 0, b, 2b, \ldots, (p-1-j)b \pmod{p}.$$

Using this we can show that $\mathcal{A}(N/K)$ has a basis of the form

$$\pi_K^{-r(j)}(\sigma - 1)^j \in \mathcal{A}(N/K) \text{ for } 0 \leq j \leq p-1,$$

where the $r(j)$ can be calculated, and we can check when O_N is free over $\mathcal{A}(N/K)$.

Theorem (Bertrandias and Ferton, 1972)

Let $b = pb_1 + b_0$ with $1 \leq b_0 \leq p-1$. Then

$$O_N \text{ is free over } \mathcal{A}(N/K) \Leftrightarrow b_0 \text{ divides } p-1.$$

What happens for degree p^2 (or higher)?

Now suppose $\mathrm{Gal}(N/K) = \langle \sigma, \tau \rangle \cong C_P \times C_p$ with N/K totally ramified.

What happens for degree p^2 (or higher)?

Now suppose $\mathrm{Gal}(N/K) = \langle \sigma, \tau \rangle \cong C_P \times C_p$ with N/K totally ramified.

We then have two ramification breaks $b_2 \geq b_1$ with

$$\begin{aligned} v_N((\sigma - 1) \cdot x) &= v_N(x) + b_1 \text{ if } p \nmid v_N(x), \\ v_N((\tau - 1) \cdot x) &= v_N(x) + b_2 \text{ if } p \nmid v_N(x), \end{aligned}$$

(and with "$=$" replaced by "$>$" when $p \mid v_N(x)$).

What happens for degree p^2 (or higher)?

Now suppose $\mathrm{Gal}(N/K) = \langle \sigma, \tau \rangle \cong C_P \times C_p$ with N/K totally ramified.

We then have two ramification breaks $b_2 \geq b_1$ with

$$\begin{aligned} v_N((\sigma - 1) \cdot x) &= v_N(x) + b_1 \text{ if } p \nmid v_N(x), \\ v_N((\tau - 1) \cdot x) &= v_N(x) + b_2 \text{ if } p \nmid v_N(x), \end{aligned}$$

(and with "$=$" replaced by "$>$" when $p \mid v_N(x)$).

This does not give us enough information to find $\mathcal{A}(N/K)$.

What happens for degree p^2 (or higher)?

Now suppose $\mathrm{Gal}(N/K) = \langle \sigma, \tau \rangle \cong C_P \times C_p$ with N/K totally ramified.

We then have two ramification breaks $b_2 \geq b_1$ with

$$\begin{aligned} v_N((\sigma - 1) \cdot x) &= v_N(x) + b_1 \text{ if } p \nmid v_N(x), \\ v_N((\tau - 1) \cdot x) &= v_N(x) + b_2 \text{ if } p \nmid v_N(x), \end{aligned}$$

(and with "$=$" replaced by "$>$" when $p \mid v_N(x)$).

This does not give us enough information to find $\mathcal{A}(N/K)$.

What we really need in order to generalise the calculations for the degree p case is two elements Ψ_1, $\Psi_2 \in K[G]$ with the following property:

What happens for degree p^2 (or higher)?

Now suppose $\mathrm{Gal}(N/K) = \langle \sigma, \tau \rangle \cong C_P \times C_p$ with N/K totally ramified.

We then have two ramification breaks $b_2 \geq b_1$ with

$$\begin{aligned} v_N((\sigma - 1)\cdot x) &= v_N(x) + b_1 \text{ if } p \nmid v_N(x), \\ v_N((\tau - 1)\cdot x) &= v_N(x) + b_2 \text{ if } p \nmid v_N(x), \end{aligned}$$

(and with "$=$" replaced by "$>$" when $p \mid v_N(x)$).

This does not give us enough information to find $\mathcal{A}(N/K)$.

What we really need in order to generalise the calculations for the degree p case is two elements Ψ_1, $\Psi_2 \in K[G]$ with the following property:

If $v_N(x) \equiv -a_0 b_2 - p a_1 b_1 \pmod{p^2}$, with $0 \leq a_0, a_1 \leq p-1$, then

$$\begin{aligned} v_N(\Psi_1 \cdot x) &= v_N(x) + b_2 \text{ if } a_0 \neq 0, \\ v_N(\Psi_2 \cdot x) &= v_N(x) + pb_1 \text{ if } a_1 \neq 0. \end{aligned}$$

Sometimes (but not always), it is possible to construct suitable Ψ_1, Ψ_2.

What happens for degree p^2 (or higher)?

Now suppose $\mathrm{Gal}(N/K) = \langle \sigma, \tau \rangle \cong C_P \times C_p$ with N/K totally ramified.

We then have two ramification breaks $b_2 \geq b_1$ with

$$\begin{aligned} v_N((\sigma - 1) \cdot x) &= v_N(x) + b_1 \text{ if } p \nmid v_N(x), \\ v_N((\tau - 1) \cdot x) &= v_N(x) + b_2 \text{ if } p \nmid v_N(x), \end{aligned}$$

(and with "$=$" replaced by "$>$" when $p \mid v_N(x)$).

This does not give us enough information to find $\mathcal{A}(N/K)$.

What we really need in order to generalise the calculations for the degree p case is two elements Ψ_1, $\Psi_2 \in K[G]$ with the following property:

If $v_N(x) \equiv -a_0 b_2 - p a_1 b_1 \pmod{p^2}$, with $0 \leq a_0, a_1 \leq p - 1$, then

$$\begin{aligned} v_N(\Psi_1 \cdot x) &= v_N(x) + b_2 \text{ if } a_0 \neq 0, \\ v_N(\Psi_2 \cdot x) &= v_N(x) + p b_1 \text{ if } a_1 \neq 0. \end{aligned}$$

Sometimes (but not always), it is possible to construct suitable Ψ_1, Ψ_2.

This is the starting point for the theory of **Galois Scaffolds**.