Galois representations and automorphic forms modulo p

Gergely Zábrádi
Eötvös Loránd University Budapest
Institute of Mathematics
Department of Algebra and Number Theory
zger@cs.elte.hu

Motivation

$f(x) \in \mathbb{Z}[x]$ irreducible. How does f decompose modulo p? ($2 \nmid p$ prime)

Motivation

$f(x) \in \mathbb{Z}[x]$ irreducible. How does f decompose modulo p? ($2 \nmid p$ prime) Easiest example: $f(x) = x^2 - d$ for some $d \in \mathbb{Z}$

$$
\begin{aligned}
x^2 - d \equiv x^2 \pmod{p} &\iff p \mid d \\
x^2 - d \equiv (x-b)(x+b) \pmod{p} \quad (b \neq 0) &\iff \left(\frac{d}{p}\right) = 1 \\
x^2 - d \text{ irreducible} \pmod{p} &\iff \left(\frac{d}{p}\right) = -1 \,.
\end{aligned}
$$

Motivation

$f(x) \in \mathbb{Z}[x]$ irreducible. How does f decompose modulo p? ($2 \nmid p$ prime) Easiest example: $f(x) = x^2 - d$ for some $d \in \mathbb{Z}$

$$x^2 - d \equiv x^2 \pmod p \iff p \mid d$$

$$x^2 - d \equiv (x-b)(x+b) \pmod p \quad (b \neq 0) \iff \left(\frac{d}{p}\right) = 1$$

$$x^2 - d \text{ irreducible} \pmod p \iff \left(\frac{d}{p}\right) = -1 .$$

Recall the quadratic reciprocity law: ($p \neq q$ odd primes)

$$\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right) , \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} .$$

Reformulate the problem!

If $d = 2^\epsilon q_1 \ldots q_r$ then—using the multiplicativity of $\left(\frac{\cdot}{p}\right)$—

$$\left(\frac{d}{p}\right) = \left(\frac{2}{p}\right)^\epsilon \prod_{i=1}^{r} \left(\frac{q_i}{p}\right) = (-1)^{\epsilon(p^2-1)/8} \prod_{i=1}^{r} (-1)^{(p-1)(q_i-1)/4} \left(\frac{p}{q_i}\right) .$$

Reformulate the problem!

If $d = 2^\epsilon q_1 \dots q_r$ then—using the multiplicativity of $\left(\frac{\cdot}{p}\right)$—

$$\left(\frac{d}{p}\right) = \left(\frac{2}{p}\right)^\epsilon \prod_{i=1}^{r} \left(\frac{q_i}{p}\right) = (-1)^{\epsilon(p^2-1)/8} \prod_{i=1}^{r} (-1)^{(p-1)(q_i-1)/4} \left(\frac{p}{q_i}\right) .$$

Key observation: the decomposition of $x^2 - d$ over $\mathbb{F}_p$ depends only on $p \mod (4d)$. The function$p \mapsto \left(\frac{d}{p}\right)$ is a homomorphism

$$\chi := \left(\frac{d}{\cdot}\right) : (\mathbb{Z}/4d\mathbb{Z})^\times \to \{\pm 1\} .$$

Reformulate the problem!

If $d = 2^\epsilon q_1 \dots q_r$ then—using the multiplicativity of $\left(\frac{\cdot}{p}\right)$—

$$\left(\frac{d}{p}\right) = \left(\frac{2}{p}\right)^\epsilon \prod_{i=1}^{r} \left(\frac{q_i}{p}\right) = (-1)^{\epsilon(p^2-1)/8} \prod_{i=1}^{r} (-1)^{(p-1)(q_i-1)/4} \left(\frac{p}{q_i}\right) .$$

Key observation: the decomposition of $x^2 - d$ over $\mathbb{F}_p$ depends only on $p \mod (4d)$. The function $p \mapsto \left(\frac{d}{p}\right)$ is a homomorphism

$$\chi := \left(\frac{d}{\cdot}\right) : (\mathbb{Z}/4d\mathbb{Z})^\times \to \{\pm 1\} .$$

What did we attach this Dirichlet character to?

Reformulate the problem!

If $d = 2^\epsilon q_1 \ldots q_r$ then—using the multiplicativity of $\left(\frac{\cdot}{p}\right)$—

$$\left(\frac{d}{p}\right) = \left(\frac{2}{p}\right)^\epsilon \prod_{i=1}^{r} \left(\frac{q_i}{p}\right) = (-1)^{\epsilon(p^2-1)/8} \prod_{i=1}^{r} (-1)^{(p-1)(q_i-1)/4} \left(\frac{p}{q_i}\right) .$$

Key observation: the decomposition of $x^2 - d$ over $\mathbb{F}_p$ depends only on $p \mod (4d)$. The function $p \mapsto \left(\frac{d}{p}\right)$ is a homomorphism

$$\chi := \left(\frac{d}{\cdot}\right) : (\mathbb{Z}/4d\mathbb{Z})^\times \to \{\pm 1\} .$$

What did we attach this Dirichlet character to?

To a character of the Galois group!

- Put $F = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$. Galois extension of $\mathbb{Q}$ with Galois group $G := \mathrm{Gal}(F/\mathbb{Q}) \cong C_2$.
- Nontrivial element in G maps $a + b\sqrt{d}$ to $a - b\sqrt{d}$. Unique nontrivial character: $\rho\colon G \to \{\pm 1\}$.

- Put $F = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$. Galois extension of $\mathbb{Q}$ with Galois group $G := \mathrm{Gal}(F/\mathbb{Q}) \cong C_2$.
- Nontrivial element in G maps $a + b\sqrt{d}$ to $a - b\sqrt{d}$. Unique nontrivial character: $\rho\colon G \to \{\pm 1\}$.

How do we read the decomposition of f mod p from $\mathrm{Gal}(F/\mathbb{Q})$?

- Put $F = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$. Galois extension of $\mathbb{Q}$ with Galois group $G := \mathrm{Gal}(F/\mathbb{Q}) \cong C_2$.
- Nontrivial element in G maps $a + b\sqrt{d}$ to $a - b\sqrt{d}$. Unique nontrivial character: $\rho \colon G \to \{\pm 1\}$.

How do we read the decomposition of f mod p from $\mathrm{Gal}(F/\mathbb{Q})$?

- To reduce mod p we need integral structure: Let $\mathcal{O}_F = \{\beta \in F \colon m_\beta(x) \in \mathbb{Z}[x]\}$ be the ring of integers in F.

$$\mathcal{O}_F = \begin{cases} \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} & \text{if } d \equiv 2, 3 \pmod 4 \\ \{a + b\frac{1+\sqrt{d}}{2} \mid a, b \in \mathbb{Z}\} & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

- Put $F = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$. Galois extension of $\mathbb{Q}$ with Galois group $G := \mathrm{Gal}(F/\mathbb{Q}) \cong C_2$.
- Nontrivial element in G maps $a + b\sqrt{d}$ to $a - b\sqrt{d}$. Unique nontrivial character: $\rho\colon G \to \{\pm 1\}$.

How do we read the decomposition of f mod p from $\mathrm{Gal}(F/\mathbb{Q})$?

- To reduce mod p we need integral structure: Let $\mathcal{O}_F = \{\beta \in F\colon m_\beta(x) \in \mathbb{Z}[x]\}$ be the ring of integers in F.

$$\mathcal{O}_F = \begin{cases} \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} & \text{if } d \equiv 2, 3 \pmod 4 \\ \{a + b\frac{1+\sqrt{d}}{2} \mid a, b \in \mathbb{Z}\} & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

$\mathcal{O}_F$ is a *Dedekind domain*: even though we may not have unique factorization for elements, but we do have unique factorization of ideals (into products of prime ideals)!

- Put $F = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$. Galois extension of $\mathbb{Q}$ with Galois group $G := \mathrm{Gal}(F/\mathbb{Q}) \cong C_2$.
- Nontrivial element in G maps $a + b\sqrt{d}$ to $a - b\sqrt{d}$. Unique nontrivial character: $\rho\colon G \to \{\pm 1\}$.

How do we read the decomposition of f mod p from $\mathrm{Gal}(F/\mathbb{Q})$?

- To reduce mod p we need integral structure: Let $\mathcal{O}_F = \{\beta \in F\colon m_\beta(x) \in \mathbb{Z}[x]\}$ be the ring of integers in F.

$$\mathcal{O}_F = \begin{cases} \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} & \text{if } d \equiv 2, 3 \pmod 4 \\ \{a + b\frac{1+\sqrt{d}}{2} \mid a, b \in \mathbb{Z}\} & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

$\mathcal{O}_F$ is a *Dedekind domain*: even though we may not have unique factorization for elements, but we do have unique factorization of ideals (into products of prime ideals)! Factorization of $p\mathcal{O}_F$ is related to that of $x^2 - d \pmod p$:

Key: Decomposing $p\mathcal{O}_F$ is equivalent to finding the prime ideals in $\mathcal{O}_F/p\mathcal{O}_F \cong \mathbb{F}_p[x]/(x^2 - d)$. 3 possiblities ($p$ is still odd)

Key: Decomposing $p\mathcal{O}_F$ is equivalent to finding the prime ideals in $\mathcal{O}_F/p\mathcal{O}_F \cong \mathbb{F}_p[x]/(x^2-d)$. 3 possiblities ($p$ is still odd)

- p ramifies: $p\mathcal{O}_F = \mathfrak{p}_1^2 \iff p \mid d \iff x^2 - d \equiv x^2 \pmod{p}$;
- p splits: $p = \mathfrak{p}_1\mathfrak{p}_2 \iff \left(\frac{d}{p}\right) = 1 \iff$
  $\iff x^2 - d \equiv (x-b)(x-c) \pmod{p}$;
- $p\mathcal{O}_F = p\mathcal{O}_F$ remains prime $\iff \left(\frac{d}{p}\right) = -1 \iff x^2 - d$ irred. mod p.

Key: Decomposing $p\mathcal{O}_F$ is equivalent to finding the prime ideals in $\mathcal{O}_F/p\mathcal{O}_F \cong \mathbb{F}_p[x]/(x^2-d)$. 3 possiblities ($p$ is still odd)

- p ramifies: $p\mathcal{O}_F = \mathfrak{p}_1^2 \iff p \mid d \iff x^2 - d \equiv x^2 \pmod{p}$;
- p splits: $p = \mathfrak{p}_1\mathfrak{p}_2 \iff \left(\frac{d}{p}\right) = 1 \iff$ $\iff x^2 - d \equiv (x-b)(x-c) \pmod{p}$;
- $p\mathcal{O}_F = p\mathcal{O}_F$ remains prime $\iff \left(\frac{d}{p}\right) = -1 \iff x^2 - d$ irred. mod p.

Fact: G acts transitively on the primes of $\mathcal{O}_F$ dividing p. $\mathcal{O}_F/\mathfrak{p}_1 \cong \mathbb{F}_p(\sqrt{d})$, so the stabilizer $G_{\mathfrak{p}_1} \leq G$ of $\mathfrak{p}_1$ maps onto $\mathrm{Gal}(\mathbb{F}_p(\sqrt{d})/\mathbb{F}_p) = \langle \mathrm{Frob}_p \rangle$.

Key: Decomposing $p\mathcal{O}_F$ is equivalent to finding the prime ideals in $\mathcal{O}_F/p\mathcal{O}_F \cong \mathbb{F}_p[x]/(x^2-d)$. 3 possiblities ($p$ is still odd)

- p ramifies: $p\mathcal{O}_F = \mathfrak{p}_1^2 \iff p \mid d \iff x^2-d \equiv x^2 \pmod{p}$;
- p splits: $p = \mathfrak{p}_1\mathfrak{p}_2 \iff \left(\frac{d}{p}\right) = 1 \iff$ $\iff x^2-d \equiv (x-b)(x-c) \pmod{p}$;
- $p\mathcal{O}_F = p\mathcal{O}_F$ remains prime $\iff \left(\frac{d}{p}\right) = -1 \iff x^2-d$ irred. mod p.

Fact: G acts transitively on the primes of $\mathcal{O}_F$ dividing p. $\mathcal{O}_F/\mathfrak{p}_1 \cong \mathbb{F}_p(\sqrt{d})$, so the stabilizer $G_{\mathfrak{p}_1} \leq G$ of $\mathfrak{p}_1$ maps onto $\mathrm{Gal}(\mathbb{F}_p(\sqrt{d})/\mathbb{F}_p) = \langle \mathrm{Frob}_p \rangle$.

Assuming $p \nmid 4d$ we may choose a lift $\widetilde{\mathrm{Frob}_p} \in G$ which is trivial iff $\rho(\widetilde{\mathrm{Frob}_p}) = 1$ iff p splits.

Key: Decomposing $p\mathcal{O}_F$ is equivalent to finding the prime ideals in $\mathcal{O}_F/p\mathcal{O}_F \cong \mathbb{F}_p[x]/(x^2-d)$. 3 possiblities ($p$ is still odd)

- p ramifies: $p\mathcal{O}_F = \mathfrak{p}_1^2 \iff p \mid d \iff x^2-d \equiv x^2 \pmod{p}$;
- p splits: $p = \mathfrak{p}_1\mathfrak{p}_2 \iff \left(\frac{d}{p}\right) = 1 \iff$
  $\iff x^2 - d \equiv (x-b)(x-c) \pmod{p}$;
- $p\mathcal{O}_F = p\mathcal{O}_F$ remains prime $\iff \left(\frac{d}{p}\right) = -1 \iff x^2-d$ irred. mod p.

Fact: G acts transitively on the primes of $\mathcal{O}_F$ dividing p.
$\mathcal{O}_F/\mathfrak{p}_1 \cong \mathbb{F}_p(\sqrt{d})$, so the stabilizer $G_{\mathfrak{p}_1} \leq G$ of $\mathfrak{p}_1$ maps onto $\mathrm{Gal}(\mathbb{F}_p(\sqrt{d})/\mathbb{F}_p) = \langle \mathrm{Frob}_p \rangle$.

Assuming $p \nmid 4d$ we may choose a lift $\widetilde{\mathrm{Frob}_p} \in G$ which is trivial iff $\rho(\widetilde{\mathrm{Frob}_p}) = 1$ iff p splits.

How does ρ correspond to $\chi = \left(\frac{d}{\cdot}\right) : (\mathbb{Z}/4d\mathbb{Z})^\times \to \{\pm 1\}$?

G is naturally a quotient group of $(\mathbb{Z}/4d\mathbb{Z})^\times$!

G is naturally a quotient group of $(\mathbb{Z}/4d\mathbb{Z})^\times$!

- We may write $\sqrt{d}$ as a sum of $4d$th roots of unity: For $q \neq 2$ and ζ_n primitive nth root of 1 prime $(n \geq 1)$ we have

$$\sqrt{(-1)^{\frac{q-1}{2}} q} = \sum_{j=0}^{q-1} \zeta_q^{j^2} , \quad \sqrt{2} = \zeta_8 + \zeta_8^7 .$$

G is naturally a quotient group of $(\mathbb{Z}/4d\mathbb{Z})^\times$!

- We may write $\sqrt{d}$ as a sum of $4d$th roots of unity: For $q \neq 2$ and ζ_n primitive nth root of 1 prime ($n \geq 1$) we have

$$\sqrt{(-1)^{\frac{q-1}{2}} q} = \sum_{j=0}^{q-1} \zeta_q^{j^2} , \quad \sqrt{2} = \zeta_8 + \zeta_8^7 .$$

- This shows $\mathbb{Q}(\sqrt{d}) \leq \mathbb{Q}(\zeta_{4d})$ whence $G = \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ is a quotient of $\mathrm{Gal}(\mathbb{Q}(\zeta_{4d})/\mathbb{Q}) \cong (\mathbb{Z}/4d\mathbb{Z})^\times$:

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{4d})/\mathbb{Q}) \ni g \mapsto k \pmod{4d} \text{ if } g(\zeta_{4d}) = \zeta_{4d}^k .$$

G is naturally a quotient group of $(\mathbb{Z}/4d\mathbb{Z})^\times$!

- We may write $\sqrt{d}$ as a sum of $4d$th roots of unity: For $q \neq 2$ and ζ_n primitive nth root of 1 prime ($n \geq 1$) we have

$$\sqrt{(-1)^{\frac{q-1}{2}} q} = \sum_{j=0}^{q-1} \zeta_q^{j^2} , \quad \sqrt{2} = \zeta_8 + \zeta_8^7 .$$

- This shows $\mathbb{Q}(\sqrt{d}) \leq \mathbb{Q}(\zeta_{4d})$ whence $G = \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ is a quotient of $\mathrm{Gal}(\mathbb{Q}(\zeta_{4d})/\mathbb{Q}) \cong (\mathbb{Z}/4d\mathbb{Z})^\times$:

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{4d})/\mathbb{Q}) \ni g \mapsto k \pmod{4d} \text{ if } g(\zeta_{4d}) = \zeta_{4d}^k .$$

Theorem (Kronecker–Weber, 19th century)

If $F/\mathbb{Q}$ Galois with abelian Galois group then there exists an integer $n \geq 1$ such that $F \leq \mathbb{Q}(\zeta_n)$.

Theorem

The maximal abelian extension of $\mathbb{Q}$ is $\mathbb{Q}(\mu_\infty) := \bigcup_n \mathbb{Q}(\zeta_n)$.

Theorem

The maximal abelian extension of $\mathbb{Q}$ is $\mathbb{Q}(\mu_\infty) := \bigcup_n \mathbb{Q}(\zeta_n)$.

The absolute Galois group of $\mathbb{Q}$ is the group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of all automorphisms of the field $\overline{\mathbb{Q}}$ of algebraic numbers.

Theorem

The maximal abelian extension of $\mathbb{Q}$ is $\mathbb{Q}(\mu_\infty) := \bigcup_n \mathbb{Q}(\zeta_n)$.

The absolute Galois group of $\mathbb{Q}$ is the group $G_\mathbb{Q} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of all automorphisms of the field $\overline{\mathbb{Q}}$ of algebraic numbers.
Theorem implies $G_\mathbb{Q}^{ab} = G_\mathbb{Q}/[G_\mathbb{Q}, G_\mathbb{Q}] = \mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q})$.

Theorem

The maximal abelian extension of $\mathbb{Q}$ is $\mathbb{Q}(\mu_\infty) := \bigcup_n \mathbb{Q}(\zeta_n)$.

The absolute Galois group of $\mathbb{Q}$ is the group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of all automorphisms of the field $\overline{\mathbb{Q}}$ of algebraic numbers.
Theorem implies $G_{\mathbb{Q}}^{ab} = G_{\mathbb{Q}}/[G_{\mathbb{Q}}, G_{\mathbb{Q}}] = \mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q})$.

Can we describe this abelian group?

Theorem

The maximal abelian extension of $\mathbb{Q}$ is $\mathbb{Q}(\mu_\infty) := \bigcup_n \mathbb{Q}(\zeta_n)$.

The absolute Galois group of $\mathbb{Q}$ is the group $G_\mathbb{Q} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of all automorphisms of the field $\overline{\mathbb{Q}}$ of algebraic numbers.
Theorem implies $G_\mathbb{Q}^{ab} = G_\mathbb{Q}/[G_\mathbb{Q}, G_\mathbb{Q}] = \mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q})$.

Can we describe this abelian group?

If $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ then the Chinese Remainder Theorem yields

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$$

Theorem

The maximal abelian extension of $\mathbb{Q}$ is $\mathbb{Q}(\mu_\infty) := \bigcup_n \mathbb{Q}(\zeta_n)$.

The absolute Galois group of $\mathbb{Q}$ is the group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of all automorphisms of the field $\overline{\mathbb{Q}}$ of algebraic numbers.
Theorem implies $G_{\mathbb{Q}}^{ab} = G_{\mathbb{Q}}/[G_{\mathbb{Q}}, G_{\mathbb{Q}}] = \mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q})$.

Can we describe this abelian group?

If $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ then the Chinese Remainder Theorem yields

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$$

What does $n \to \infty$ mean in this context?

The elements of $\mathbb{Z}/p^\alpha\mathbb{Z}$ have the form

$$a = a_0 + a_1 p + \cdots + a_{\alpha-1} p^{\alpha-1}$$

with $a_i \in \{0, 1, \ldots, p-1\}$ for all $0 \leq i \leq \alpha - 1$. Moreover, a lies in $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, ie. $(a, p) = 1$ iff $a_0 \neq 0$.

The elements of $\mathbb{Z}/p^\alpha\mathbb{Z}$ have the form

$$a = a_0 + a_1 p + \cdots + a_{\alpha-1} p^{\alpha-1}$$

with $a_i \in \{0, 1, \ldots, p-1\}$ for all $0 \leq i \leq \alpha - 1$. Moreover, a lies in $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, ie. $(a, p) = 1$ iff $a_0 \neq 0$.
Here $\alpha \to \infty$ means we should consider infinite (formal) sums

$$a = a_0 + a_1 p + \cdots + a_{\alpha-1} p^{\alpha-1} + \cdots = \sum_{i=0}^{\infty} a_i p^i \ .$$

These form a ring under usual addition and multiplication—the ring $\mathbb{Z}_p$ of p-adic integers. Note that we need to "carry over" when, say, we add 1 and $p-1$: it will be $0 + 1 \cdot p + 0 \cdot p^2 + \cdots$.

The elements of $\mathbb{Z}/p^\alpha\mathbb{Z}$ have the form

$$a = a_0 + a_1 p + \cdots + a_{\alpha-1} p^{\alpha-1}$$

with $a_i \in \{0, 1, \ldots, p-1\}$ for all $0 \leq i \leq \alpha - 1$. Moreover, a lies in $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, ie. $(a, p) = 1$ iff $a_0 \neq 0$.
Here $\alpha \to \infty$ means we should consider infinite (formal) sums

$$a = a_0 + a_1 p + \cdots + a_{\alpha-1} p^{\alpha-1} + \cdots = \sum_{i=0}^{\infty} a_i p^i \ .$$

These form a ring under usual addition and multiplication—the ring $\mathbb{Z}_p$ of p-adic integers. Note that we need to "carry over" when, say, we add 1 and $p-1$: it will be $0 + 1 \cdot p + 0 \cdot p^2 + \cdots$.
We can embed $\mathbb{Z}$ into $\mathbb{Z}_p$, eg. we have

$$-1 = (p-1) + (p-1)p + \cdots + (p-1)p^i + \cdots \ .$$

$\mathbb{Z}_p$ is not a field, the invertible elements are those with $a_0 \neq 0$.

The field $\mathbb{Q}_p$ of p-adic numbers is defined as the field of fractions of $\mathbb{Z}_p$—it suffices to invert p. The nonzero elements of $\mathbb{Q}_p$ can be written as

$$a = \sum_{i=-N}^{\infty} a_i p^i$$

with $N \in \mathbb{Z}$ which expansion is unique once we assume $a_{-N} \neq 0$.

The field $\mathbb{Q}_p$ of p-adic numbers is defined as the field of fractions of $\mathbb{Z}_p$—it suffices to invert p. The nonzero elements of $\mathbb{Q}_p$ can be written as

$$a = \sum_{i=-N}^{\infty} a_i p^i$$

with $N \in \mathbb{Z}$ which expansion is unique once we assume $a_{-N} \neq 0$. The maximal abelian Galois group of $\mathbb{Q}$ can be described as

$$G_{\mathbb{Q}}^{ab} \cong \prod_{p \text{ prime}} \mathbb{Z}_p^\times .$$

The field $\mathbb{Q}_p$ of p-adic numbers is defined as the field of fractions of $\mathbb{Z}_p$—it suffices to invert p. The nonzero elements of $\mathbb{Q}_p$ can be written as

$$a = \sum_{i=-N}^{\infty} a_i p^i$$

with $N \in \mathbb{Z}$ which expansion is unique once we assume $a_{-N} \neq 0$. The maximal abelian Galois group of $\mathbb{Q}$ can be described as

$$G_{\mathbb{Q}}^{ab} \cong \prod_{p \text{ prime}} \mathbb{Z}_p^\times .$$

Note that any character $\rho \colon G_{\mathbb{Q}} \to \mathbb{C}^\times$ factors through $G_{\mathbb{Q}}^{ab}$, so we have a correspondence

$$\{\text{characters of } G_{\mathbb{Q}}\} \leftrightarrow \{\text{characters of } \prod_{p \text{ prime}} \mathbb{Z}_p^\times\} .$$

Problem: What can we say about polynomials $f(x) \in \mathbb{Z}[x]$ of higher degree? The above picture only sees those with abelian Galois group which is not the case in general!

Problem: What can we say about polynomials $f(x) \in \mathbb{Z}[x]$ of higher degree? The above picture only sees those with abelian Galois group which is not the case in general!

We need to consider higher dimensional representations!

The Galois side

- $\mathbb{C}^\times = \mathrm{GL}_1(\mathbb{C})$, so we consider group homomorphisms

$$\rho \colon G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$$

into the group of invertible $n \times n$ matrices over a field K.

The Galois side

- $\mathbb{C}^\times = \mathrm{GL}_1(\mathbb{C})$, so we consider group homomorphisms
$$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$$
into the group of invertible $n \times n$ matrices over a field K.
- $G_{\mathbb{Q}}$ is a *very* misterious group: Inverse Galois problem (believed to be true) asks whether all the finite groups arise as a (continuous) quotient of $G_{\mathbb{Q}}$. Known (Shafarevich 1970s) to be true for soluble groups.

The Galois side

- $\mathbb{C}^\times = \mathrm{GL}_1(\mathbb{C})$, so we consider group homomorphisms
$$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$$
into the group of invertible $n \times n$ matrices over a field K.
- $G_{\mathbb{Q}}$ is a *very* misterious group: Inverse Galois problem (believed to be true) asks whether all the finite groups arise as a (continuous) quotient of $G_{\mathbb{Q}}$. Known (Shafarevich 1970s) to be true for soluble groups.
- $\mathbb{Q}$ is a subfield in $\mathbb{Q}_p$, so we may embed $\overline{\mathbb{Q}}$ (non-uniquely) into the algebraic closure $\overline{\mathbb{Q}_p}$.

The Galois side

- $\mathbb{C}^\times = \mathrm{GL}_1(\mathbb{C})$, so we consider group homomorphisms
$$\rho \colon G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$$
into the group of invertible $n \times n$ matrices over a field K.
- $G_{\mathbb{Q}}$ is a *very* misterious group: Inverse Galois problem (believed to be true) asks whether all the finite groups arise as a (continuous) quotient of $G_{\mathbb{Q}}$. Known (Shafarevich 1970s) to be true for soluble groups.
- $\mathbb{Q}$ is a subfield in $\mathbb{Q}_p$, so we may embed $\overline{\mathbb{Q}}$ (non-uniquely) into the algebraic closure $\overline{\mathbb{Q}_p}$.
- This yields an embedding $G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$ of absolute Galois groups. The "local" Galois groups $G_{\mathbb{Q}_p}$ are much easier to understand: for instance, they are soluble!

The Galois side

- $\mathbb{C}^\times = \mathrm{GL}_1(\mathbb{C})$, so we consider group homomorphisms
$$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$$
into the group of invertible $n \times n$ matrices over a field K.
- $G_{\mathbb{Q}}$ is a *very* misterious group: Inverse Galois problem (believed to be true) asks whether all the finite groups arise as a (continuous) quotient of $G_{\mathbb{Q}}$. Known (Shafarevich 1970s) to be true for soluble groups.
- $\mathbb{Q}$ is a subfield in $\mathbb{Q}_p$, so we may embed $\overline{\mathbb{Q}}$ (non-uniquely) into the algebraic closure $\overline{\mathbb{Q}_p}$.
- This yields an embedding $G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$ of absolute Galois groups. The "local" Galois groups $G_{\mathbb{Q}_p}$ are much easier to understand: for instance, they are soluble!
- We may think of ρ as a bunch of local Galois representations $\rho_p\colon G_{\mathbb{Q}_p} \to \mathrm{GL}_n(K)$ together with some compatibility conditions.

Automorphic side

- Attached to a prime p we have the subgroup $\mathbb{Z}_p^\times \leq \prod_{\ell \text{ prime}} \mathbb{Z}_\ell^\times$. Note that we also have the class of p in $(\mathbb{Z}/\ell^r\mathbb{Z})$ for all primes $\ell \neq p$. For a character χ of $\prod_{\ell \text{ prime}} \mathbb{Z}_\ell^\times$ we may glue these two together to obtain a character of $\mathbb{Q}_p^\times = \mathbb{Z}_p^\times \times p^{\mathbb{Z}}$.

Automorphic side

- Attached to a prime p we have the subgroup $\mathbb{Z}_p^\times \leq \prod_{\ell \text{ prime}} \mathbb{Z}_\ell^\times$. Note that we also have the class of p in $(\mathbb{Z}/\ell^r\mathbb{Z})$ for all primes $\ell \neq p$. For a character χ of $\prod_{\ell \text{ prime}} \mathbb{Z}_\ell^\times$ we may glue these two together to obtain a character of $\mathbb{Q}_p^\times = \mathbb{Z}_p^\times \times p^{\mathbb{Z}}$.
- So the natural n-dimensional generalizations of this are representations of $\mathrm{GL}_n(\mathbb{Q}_p)$ on arbitrary vectorspaces.

Automorphic side

- Attached to a prime p we have the subgroup $\mathbb{Z}_p^\times \leq \prod_{\ell \text{ prime}} \mathbb{Z}_\ell^\times$. Note that we also have the class of p in $(\mathbb{Z}/\ell^r\mathbb{Z})$ for all primes $\ell \neq p$. For a character χ of $\prod_{\ell \text{ prime}} \mathbb{Z}_\ell^\times$ we may glue these two together to obtain a character of $\mathbb{Q}_p^\times = \mathbb{Z}_p^\times \times p^{\mathbb{Z}}$.
- So the natural n-dimensional generalizations of this are representations of $\mathrm{GL}_n(\mathbb{Q}_p)$ on arbitrary vectorspaces.
- Compatibility conditions for varying primes p: "automorphic forms"

Automorphic side

- Attached to a prime p we have the subgroup $\mathbb{Z}_p^\times \leq \prod_{\ell \text{ prime}} \mathbb{Z}_\ell^\times$. Note that we also have the class of p in $(\mathbb{Z}/\ell^r\mathbb{Z})$ for all primes $\ell \neq p$. For a character χ of $\prod_{\ell \text{ prime}} \mathbb{Z}_\ell^\times$ we may glue these two together to obtain a character of $\mathbb{Q}_p^\times = \mathbb{Z}_p^\times \times p^{\mathbb{Z}}$.
- So the natural n-dimensional generalizations of this are representations of $\mathrm{GL}_n(\mathbb{Q}_p)$ on arbitrary vectorspaces.
- Compatibility conditions for varying primes p: "automorphic forms"

Langlands programme: Match these two sides!

What is known

What is known

- $n = 1$

What is known

- $n = 1$
- Classical local Langlands (Harris–Taylor, Henniart): matching n-dimensional $G_{\mathbb{Q}_p}$-representations over $\mathbb{Q}_\ell$ with representations of $\mathrm{GL}_n(\mathbb{Q}_p)$ over $\mathbb{Q}_\ell$ ($\ell \neq p$)

What is known

- $n = 1$
- Classical local Langlands (Harris–Taylor, Henniart): matching n-dimensional $G_{\mathbb{Q}_p}$-representations over $\mathbb{Q}_\ell$ with representations of $\mathrm{GL}_n(\mathbb{Q}_p)$ over $\mathbb{Q}_\ell$ ($\ell \neq p$)
- Elliptic curves: $E\colon y^2 = x^3 + ax + b \rightsquigarrow$ Galois representation: $E[\ell^r] \cong \mathbb{Z}/\ell^r\mathbb{Z} \oplus \mathbb{Z}/\ell^r\mathbb{Z}$. $G_{\mathbb{Q}}$ acts on this, so we obtain a representation ρ_{E,ℓ^r} into $\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})$.

Theorem (Wiles, Taylor–Wiles, 1994)

Elliptic curves are modular.

This lead to a proof of Fermat's Last Theorem!

What is known

- $n = 1$
- Classical local Langlands (Harris–Taylor, Henniart): matching n-dimensional $G_{\mathbb{Q}_p}$-representations over $\mathbb{Q}_\ell$ with representations of $\mathrm{GL}_n(\mathbb{Q}_p)$ over $\mathbb{Q}_\ell$ ($\ell \neq p$)
- Elliptic curves: $E : y^2 = x^3 + ax + b \rightsquigarrow$ Galois representation: $E[\ell^r] \cong \mathbb{Z}/\ell^r\mathbb{Z} \oplus \mathbb{Z}/\ell^r\mathbb{Z}$. $G_{\mathbb{Q}}$ acts on this, so we obtain a representation ρ_{E,ℓ^r} into $\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})$.

Theorem (Wiles, Taylor–Wiles, 1994)

Elliptic curves are modular.

This lead to a proof of Fermat's Last Theorem!

- $n = 2$ is almost settled (Berger, Breuil, Colmez, Emerton, Kisin, Paškunas) globally—this needed a stronger local Langlands allowing $\ell = p$ proven for $n = 2$ by Colmez

Easier to explain the mod p situation (representations over $\mathbb{F}_p$ on both sides)—closely related to p-adic representations.

Easier to explain the mod p situation (representations over $\mathbb{F}_p$ on both sides)—closely related to p-adic representations.

- $n = 2$: Settled by Colmez+others (as above): Colmez constructed a functor

  $$\mathbb{V}\colon \{\mathrm{GL}_2(\mathbb{Q}_p)\text{−representations } /\mathbb{F}_p\} \to \{G_{\mathbb{Q}_p}\text{−representations } /\mathbb{F}_p\}$$

  that is "compatible" with the global picture

Easier to explain the mod p situation (representations over $\mathbb{F}_p$ on both sides)—closely related to p-adic representations.

- $n = 2$: Settled by Colmez+others (as above): Colmez constructed a functor

$$\mathbb{V}\colon \{\mathrm{GL}_2(\mathbb{Q}_p)\text{−representations } /\mathbb{F}_p\} \to \{G_{\mathbb{Q}_p}\text{−representations } /\mathbb{F}_p\}$$

  that is "compatible" with the global picture
- Various attempts to generalize this to $n > 2$ (Breuil, Große-Klönne, Schneider–Vigneras, Z)—constructions of functors

Easier to explain the mod p situation (representations over $\mathbb{F}_p$ on both sides)—closely related to p-adic representations.

- $n = 2$: Settled by Colmez+others (as above): Colmez constructed a functor

  $$\mathbb{V}\colon \{\mathrm{GL}_2(\mathbb{Q}_p)\text{−representations } /\mathbb{F}_p\} \to \{G_{\mathbb{Q}_p}\text{−representations } /\mathbb{F}_p\}$$

  that is "compatible" with the global picture
- Various attempts to generalize this to $n > 2$ (Breuil, Große-Klönne, Schneider–Vigneras, Z)—constructions of functors
- Z: functor $\mathbb{V}_\Delta$ to representations of $\underbrace{G_{\mathbb{Q}_p} \times \cdots \times G_{\mathbb{Q}_p}}_{n} \times \mathbb{Q}_p^\times$

  with many nice properties

Conjecture (Z, building on Breuil–Herzig–Schraen)

To an automorphic representation Π_p the functor $\mathbb{V}_\Delta$ attaches $\bigotimes_{i=1}^{n} \wedge^i \rho_p$ where $\rho_p \leftrightarrow \Pi_p$.

Thanks for your attention!