8

Topics in Number Theory

Introduction to Iwasawa Theory

David Burns

Giving a one-lecture-introduction to Iwasawa theory is an unpossibly difficult task as this requires to give a survey of more than 150 years of development in mathematics. Moreover, Iwasawa theory is a comparatively technical subject. We abuse this as an excuse for missing out the one or other detail.

8.1 The analytic class number formula

We start our journey with 19th-century-mathematics. The reader might also want to consult his notes on last week's lecture for a more extensive treatment.

Let R be an integral domain and F its field of fractions. A ***fractional ideal*** I of R is a finitely generated R-submodule of F such that there exists an $x \in F^\times$ satisfying $x \cdot I \subseteq R$. For such a fractional ideal I we define its ***dual ideal*** to be

$$I^* = \{x \in F \mid x \cdot I \subseteq R\}.$$

If I and J both are fractional ideals, its ***product ideal*** $I \cdot J$ is given by the ideal generated by all products $i \cdot j$ for $i \in I$ and $j \in J$. That is,

$$I \cdot J = \{ \sum_{a \in A} i_a \cdot j_a \mid i_a \in I, j_a \in J, A \text{ finite } \}.$$

For example we have $I \cdot I^* \subseteq R$. If $I \cdot I^* = R$ we say that I is ***invertible***.

We now specialise to R being a Dedekind domain. In this case, every non-zero fractional ideal is invertible. Hence the set of all nonzero fractional ideals of R forms an abelian group under multiplication which we denote by $\mathrm{Frac}(R)$. Contained in $\mathrm{Frac}(R)$ is a canonical subgroup, the group of ***principal ideals***:

$$\mathrm{Prin}(R) = \{I \in \mathrm{Frac}(R) \mid \exists x \in F^\times : I = x \cdot R\}.$$

The ***ideal class group*** of R is now given by the quotient

$$\mathrm{Cl}(R) = \mathrm{Frac}(R) / \mathrm{Prin}(R).$$

[0]Edited by Dominik Bullach. Last time modified: 22:38 on Tuesday 29th October, 2019.

(8.1) Theorem. If R is either

- the integral closure $\mathcal{O}_F$ of $\mathbb{Z}$ in a finite field extension F of $\mathbb{Q}$, i. e. an ***algebraic number field*** F,
- or the integral closure of the polynomial ring $\mathbb{F}_p[T]$ in a finite field extension F of $\mathbb{F}_p(T)$ for a prime p, i. e. F is a ***global function field***,

then $\mathrm{Cl}(R)$ is finite.

(8.2) Remark. (1) Global function fields are exactly the coordinate rings of non-singular integral affine curves over $\mathbb{F}_p$. The notion "global" refers to the fact that the stalks are finite, i. e. the quotient $R/\mathfrak{p}$ for every prime ideal $\mathfrak{p} \subseteq R$ is finite.

(2) The class group $\mathrm{Cl}(R)$ measure the failure of R to be a principle ideal domain. Since every ideal of R becomes principal after localising at a prime $\mathfrak{p}$, i. e. passing to the completion $F_\mathfrak{p}$ of F at $\mathfrak{p}$, the ideal class group can also be interpreted as a measurement for the failure of a local-global-principle.

(3) The finiteness of $|\mathrm{Cl}(R)|$ is a phenomenon special for the two stated situation. There are examples of Dedekind domains that have infinite ideal class group.[1]

(4) Although being a finite abelian group, the class group is still hard to compute. Even its size (the ***class number***) is only computable for extensions $F|\mathbb{Q}$ respectively $F|\mathbb{F}_p(T)$ of small degree.

Recall that the ***Dedekind ζ-function*** of an algebraic number field F is defined as

$$\zeta_F(s) = \sum_{\mathfrak{a}} \left|\mathcal{O}_F/\mathfrak{a}\right|^{-s}, \quad \mathrm{Re}(s) > 1,$$

where the sum ranges over all non-zero integral ideals $\mathfrak{a} \subseteq \mathcal{O}_F$. Using unique decomposition of ideals in Dedekind domains into prime ideals one can show that

$$\zeta_F(s) = \prod_{\mathfrak{p}} (1 - \left|\mathcal{O}_F/\mathfrak{p}\right|^{-s})^{-1}$$

where the product now ranges over all prime ideals $\mathfrak{p}$ of $\mathcal{O}_F$.

(8.3) Theorem (*analytic class number formula*[2])**.** $\zeta_F(s)$ has a meromorphic continuation to $\mathbb{C}$ and the leading term in the Taylor expansion of $\zeta_F(s)$ at $s = 0$ is

$$\zeta_F^* = \text{transcendental factor } \times |\mathrm{Cl}(\mathcal{O}_F)|.$$

[1] Reference specifically for Federico Bo: `https://math.stackexchange.com/questions/594507/examples-of-dedekind-rings-with-infinite-class-number`)

[2] Usually, the analytic class number formula is attributed to Dedekind. However, the full story is a bit more complicated: `https://mathoverflow.net/questions/180400/history-of-the-analytic-class-number-formula`

(8.4) Remark. (1) The analytic class number formula is a striking theorem since it connects the local, analytic object ζ_F^* to the algebraic, global object $\mathrm{Cl}(\mathcal{O}_F)$.

(2) Using the functional equation of $\zeta_F(s)$, the analytic class number formula can also equivalently be stated as a formula for the residue of $\zeta_F(s)$ at $s = 1$.

8.2 The Weil conjectures

We now have a look at a seemingly unrelated situation with the question in mind: What is to learn from global function fields?

Let p a prime. Recall that for every $n \in \mathbb{N}$ there is a finite field $\mathbb{F}_{p^n}$ of size p^n. The respective Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}|\mathbb{F}_p)$ is cyclic of order n and admits a canonical generator, namely the ***Frobenius homomorphism*** σ. This homomorphism is characterised by $\sigma(x) = x^p$ for all $x \in \mathbb{F}_{p^n}$.
The algebraic closure of $\mathbb{F}_p$ can be described as $\mathbb{F}_p^c = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n}$ and the absolute Galois group in this situation is

$$\mathrm{Gal}(\mathbb{F}_p^c|\mathbb{F}_p) \cong \varprojlim_n \mathrm{Gal}(\mathbb{F}_{p^n}|\mathbb{F}_p) = \varprojlim_n \mathbb{Z}/n\mathbb{Z} =: \widehat{\mathbb{Z}},$$

where $\widehat{\mathbb{Z}}$ denotes the profinite completion of $\mathbb{Z}$. Here the projective limit is formed with respect to the natural projection maps $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ for $m \mid n$.

Let X be a non-singular projective algebraic variety defined over $\mathbb{F}_p$ and of dimension n. For every $m \in \mathbb{N}$ we denore by $N_m(X)$ the number $|X(\mathbb{F}_{p^m}|$ of $\mathbb{F}_{p^m}$-rational points. In general, $N_m(X)$ is very difficult to compute in isolation. We therefore approach this problem through the respective generating function

$$Z(X,t) = \exp\left(\sum_{m\in\mathbb{N}} \frac{N_m(X)}{m} t^m\right).$$

The zeta function of X can be obtained from $Z(X,t)$ via the substitution $t \mapsto p^{-s}$, i. e. $\zeta(X,s) = Z(X, p^{-s})$.

(8.5) Theorem (*Weil conjectures*). (1) $Z(X,t)$ is a rational function of t. That is, there are polynomials $P_i(t) \in \mathbb{Z}[t]$ such that

$$Z(X,t) = \prod_{i=0}^{2n} P_i(t)^{(-1)^{i+1}}.$$

(2) For $i \notin \{0, 2n\}$, these polynomials $P_i(t)$ are of the form $P_i(t) = \prod_j (1 - \alpha_{ij} t)$, where the $\alpha_{ij} \in \mathbb{C}$ are complex numbers of absolute value $|\alpha_{ij}| = p^{i/2}$.

(3) If X is the reduction mod p of a curve Y defined over an algebraic number field, the degree $P_i(t)$ equals the i-th Betti number of Y.

(8.6) Examples. (1) For $X = \mathbb{P}^1$ we have $N_m(X) = p^m + 1$ for every $m \in \mathbb{N}$. Hence

$$Z(X,t) = \frac{1}{(1-t)(1-pt)}$$

in this case.

(2) Let X be an elliptic curve defined over $\mathbb{F}_p$. Then $N_m(X) = 1 - \alpha^m - \beta^m + p^m$ for suitable $\alpha, \beta \in \mathbb{C}$ satisfying $\alpha = \bar{\beta}$ and $|\alpha| = p^{1/2}$. Moreover,

$$Z(X,t) = \frac{(1-\alpha t)(1-\beta t)}{(1-t)(1-\beta t)}.$$

(3) Let X be a curve of genus g. Then

$$Z(X,t) = \frac{\prod_{i=1}^{2g}(1-\alpha_i t)}{(1-t)(1-pt)},$$

where the α_i are the eigenvalues of the Frobenius homomorphism σ acting on $\mathrm{Jac}(X)(\mathbb{F}_p^c)$. Here $\mathrm{Jac}(X)$ denotes the Jacobian of X, i. e. the abelian variety characterised by

$$\mathrm{Jac}(X)(k') = \mathrm{Pic}^0(X_{k'}) = \mathrm{Div}^0(X_{k'}) / \mathrm{Prin}(X_{k'}),$$

where $k'|\mathbb{F}_p$ is a field extension. Note that $|\alpha_i| = p^{1/2}$, so $\zeta(X,s) = Z(X, p^{-s})$ has zeroes solely on the "critical line" of $\mathrm{Re}(s) = \frac{1}{2}$. This is commonly known as the ***Riemann hypothesis*** for X.

(8.7) Remark. (1) Observe that $Z(X,t)$ being a rational function in t implies the existence of a recursive formula for the sequence $\{N_m(X)\}_{n\in\mathbb{N}}$. The rationality of $Z(X,t)$ was proven by Dwork (1960) using p-adic analysis.

(2) The Riemann hypothesis for varieties was proven by Deligne (1974). The underlying of this prove is the use of l-adic cohomology, which was constructed precisely to prove the Weil conjectures.
For a prime $l \neq p$, the l-adic cohomology gives a finite-dimensional $\mathbb{Q}_l$-vector spaces $H^i(X \times_{\mathbb{F}_p} \mathbb{F}_p^c)$ upon which the Frobenius homomorphism σ_p acts. Grothendieck proved that

$$Z(X,t) = \prod_{i=0}^{2n} \det(1 - \sigma_p t \mid H^i(X \times_{\mathbb{F}_p} \mathbb{F}_p^c))^{(-1)^{i+1}},$$

where the as factors appearing polynomials a priori lie in $\mathbb{Q}_l[t]$ but are really elements of $\mathbb{Z}[t]$. Moreover, they do not depend on the choice of auxiliary prime l.

(8.8) Lessons. (L1) Extending the field of constants gives amenable families. This extension process is really adjoining roots of unity.

(L2) The action of the Frobenius σ_p produces explicit formulas for zeta functions.

8.3 Iwasawa theory

Henceforth we consider algebraic number fields and develop Iwasawa theory as means of learning lessons (L1) and (L2).

Setup

Let p be an odd prime and form for all $n \in \mathbb{N}$ the primitive p^n-th root of unity $\zeta_n = \exp(\frac{2\pi i}{n})$. By adjoining this root of unity we get a field $\mathbb{Q}(n) = \mathbb{Q}(\zeta)$, the Galois group of which can be parametrised by

$$G(n) := \mathrm{Gal}(\mathbb{Q}(n)|\mathbb{Q}) \xrightarrow{\simeq} \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times, \quad \{\zeta_n \mapsto \zeta_n^a\} \mapsto [a]_{p^n}.$$

Now form $\mathbb{Q}(\infty) = \bigcup_{n\in\mathbb{N}} \mathbb{Q}(n)$. Then

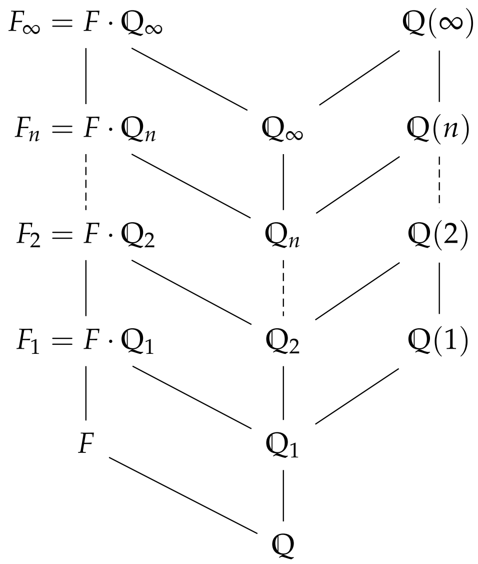
$$\begin{aligned} G(\infty) :&= \mathrm{Gal}(\mathbb{Q}(\infty)|\mathbb{Q}) = \varprojlim_n \mathrm{Gal}(\mathbb{Q}(n)|\mathbb{Q}) \\ &\cong \varprojlim_n \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times = \mathbb{Z}_p^\times \cong \left(\mathbb{Z}/p\mathbb{Z}\right)^\times \times \mathbb{Z}_p, \end{aligned}$$

where the last isomorphism uses the fact that for every $a \in \mathbb{Z}_p$ there is a unique $(p-1)$-th root of unity $\omega(a) \in \mathbb{Z}_p^\times$ such that $a \cdot \omega(a)^{-1} \in 1 + p\mathbb{Z}_p$. The isomorphism used above can then be described as

$$\mathbb{Z}_p^\times \xrightarrow{\simeq} \left(\mathbb{Z}/p\mathbb{Z}\right)^\times \times \mathbb{Z}_p, \quad a = \omega(a) \cdot (1+p)^{y(a)} \leftarrow\!\shortmid (\omega(a), y(a)).$$

Let $\Delta = \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ be the torsion subgroup of $G(\infty)$ and denote by $\mathbb{Q}_\infty = \mathbb{Q}(\infty)^\Delta$ the fixed field of Δ. Then by construction $\mathrm{Gal}(\mathbb{Q}_\infty|\mathbb{Q}) \cong \mathbb{Z}_p$ and $\mathbb{Q}_\infty$ is called the ***cyclotomic*** $\mathbb{Z}_p$***-extensio***n of $\mathbb{Q}$. In particular, for every $n \in \mathbb{N}$ there is a unique subfield $\mathbb{Q}_n$ of $\mathbb{Q}_\infty$ such that $\mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$, namely the fixed field of the subgroup $p^n\mathbb{Z}_p \subseteq \mathbb{Z}_p \cong \mathrm{Gal}(\mathbb{Q}_\infty|\mathbb{Q})$.

If F is an arbitrary number field, for the sake of simplicity such that $F \cap \mathbb{Q}(\infty) = \mathbb{Q}$, we can similarly form a $\mathbb{Z}_p$-extension of F by setting $F_n = F \cdot \mathbb{Q}_n$. In summary, we have a diagram of the following sort:



Choose a topological generator γ of $\Gamma = \mathrm{Gal}(F_\infty|F)$ and write $\Gamma_n = \mathrm{Gal}(F_n|F) \cong \mathbb{Z}/p^n\mathbb{Z}$. Then the restriction $\Gamma_n \to \Gamma_{n-1}$ induces a map $\pi_n \colon \mathbb{Z}_p[\Gamma_n] \to \mathbb{Z}_p[\Gamma_{n-1}]$. We can therefore give the following

(8.9) Definition. The ***Iwasawa algebra*** Λ is defined as $\Lambda = \varprojlim_{\pi_n} \mathbb{Z}_p[\Gamma_n]$.

It is a theorem by Serre that

$$\mathbb{Z}_p[\![T]\!] \to \Lambda, \quad 1 + T \mapsto (\gamma_{|F_n})_{n \in \mathbb{N}}$$

is an isomorphism. From this we can deduce that Λ is a regular ring of Krull dimension 2 and the prime ideals of Λ uniquely correspond to $(0), (p), (p, T), (f(T))$, where $f(T) \in \mathbb{Z}_p[T]$ is irreducible and ***distinguished***, i. e. $f(T) \equiv T^{\deg f} \mod p$.

Λ-modules

Let $(X_n)_{n \in \mathbb{N}}$ denote a compatible family of $\mathbb{Z}_p[\Gamma_n]$-modules, that is for every $n \in \mathbb{N}$ there is a commutative diagram

$$\begin{array}{ccc} X_n & \xrightarrow{\pi_n} & X_{n-1} \\ \big\downarrow{\scriptstyle \cdot\gamma_{|F_n}} & & \big\downarrow{\scriptstyle \cdot\gamma_{|F_n}} \\ X_n & \xrightarrow{\pi_n} & X_{n-1} \end{array}$$

In this case we can obtain a Λ-module by forming $X = \varprojlim_n X_n$.

The advantage of studying the Λ-module X instead of the $\mathbb{Z}_p[\Gamma_n]$-modules X_n on its own is that Λ-modules admit a very nice representation theory whereas the representation theory of $\mathbb{Z}_p[\Gamma_n]$-modules is quite ugly.

(8.10) Theorem (*structure theorem for finitely generated Λ-modules*)**.** Let M be a finitely generated Λ-module. Then there exist unique integers r, s, t, l_j, m_i and irreducible distinguished polynomials f_j such that there is an exact sequence

$$0 \longrightarrow (\text{ finite }) \longrightarrow M \longrightarrow \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/(p^{m_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(f_j^{l_j}) \longrightarrow (\text{ finite }) \longrightarrow 0$$

The uniqueness statement in the theorem allows us to define the following invariants of M:

- $\mathrm{rk}(M) = r$, notice that M is a torsion module if and only if $r = 0.$,
- $\mu(M) = \sum_{i=1}^{s} m_i$,
- $\lambda(M) = \sum_{j=1}^{t} l_j \deg(f_j)$, observe that $\lambda(M) = \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}} M)$ if M is torsion,
- $\mathrm{char}_\gamma(M) = p^{\mu(M)} \prod_j f_j^{l_j}$, where $\mathrm{char}_\gamma(M) = p^{\mu(M)} \cdot \det(tI - X \mid M \otimes \mathbb{Q}_p)$ if $r = 0$, i. e. in this case the characteristic polynomial of the indeterminate X on $M \otimes \mathbb{Q}_p$ appears.

Also, we have the following:

(FG) M is a finitely generated Λ-module if and only if $M/(p, T) \cdot M$ is finite,

(Tor) If M is finitely generated, then M is torsion if and only if $M/\nu_{n,e}M$ is finite for all n, where

$$\nu_{n,e} = \sum_{i=0}^{p^{n-e}-1} (\gamma^{p^e})^i \quad \in \Lambda.$$

(Rec) If M is a finitely generated torsion Λ-module, there exists $\nu \in \mathbb{N}_0$ such that

$$\left| M/\nu_{n,e}M \right| = p^{\mu(M)p^n + \lambda(M) + \nu} \quad \text{for } n >> 0.$$

We now apply this algebraic theory to a concrete module. For every field F_n as above let A_{F_n} denote the p-Sylow group of $\mathrm{Cl}(\mathcal{O}_{F_n})$. The Norm maps

$$N_{F_n|F_{n-1}} \colon F_n \to F_{n-1}, \quad x \mapsto \prod_{\sigma \in \mathrm{Gal}(F_n|F_{n-1})} \sigma(x)$$

also induces maps $A_{F_n} \to A_{F_{n-1}}$ which we can use to form $M = \varprojlim A_{F_n}$.

As a consequence of the above representation theory we get

(8.11) Theorem (Iwasawa, 50s)**.** For n large enough we have that

$$|A_{F_n}| = p^{\mu p^n + \lambda n + \nu}.$$

Furthermore, it is conjectured that $\mu = 0$. This means that class groups do not "grow too fast".

Iwasawa Main Conjecture

To consider lesson (L2), we now restrict to $F = \mathbb{Q}$. Let $f \in \mathbb{N}$ and let $\chi\colon \left(\mathbb{Z}/f\mathbb{Z}\right)^\times \to \mathbb{C}^\times$ be a Dirichlet character of conductor f. Then the L-series associated to χ is given by

$$L(\chi, s) = \sum_{n \in \mathbb{N}} \frac{\chi(n)}{n^s}, \quad \mathrm{Re}(s) > 1,$$

where $\chi(n) = 0$ if $(n, f) \neq 1$. One can show that $L(\chi, s)$ has a holomorphic continuation to $\mathbb{C}$ and satisfies

$$L(\chi, 1-n) = -\frac{B_{n,\chi}}{n} \quad \in \mathbb{Q}^c \quad \text{for } n \in \mathbb{N},$$

where $B_{n,\chi}$ denote the ***generalised Bernoulli-numbers***. These are characterised by

$$\sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n} = \sum_{a=1}^{f} \frac{\chi(a) t e^{a^t}}{e^{ft} - 1}.$$

(8.12) Example. For $f = 1 = \chi$ the L-function coincides with the Riemann ζ-function: $L(\chi, s) = \zeta_{\mathbb{Q}}(s)$. In this case $B_{n,\chi} = B_n$ are the classical Bernoulli numbers.

We also have the so-called "Kummer congruences": For $m, n \in \mathbb{N}$ and $m \equiv n \not\equiv 0 \mod (p-1)$ the congruence

$$\frac{B_m}{m} \equiv \frac{B_n}{n} \mod p$$

holds. This may be interpreted as "L-values behave in some sense p-adically continuously" and one might ask whether these arise as values of a p-adic function.

(8.13) Theorem (Kubota-Leopoldt)**.** There is a p-adic meromorphic function $L_p(s, \chi)$ on $\{s \in \mathbb{Z}_p \mid |s|_p \leq p^{1-\frac{1}{p-1}}\}$ such that for all $n \in \mathbb{N}$ the function $L_p(s, \chi)$ interpolates $L(1-n, \chi)$ up to some fudge factors.

It is a fact that there exists $f_{\gamma,\chi} \in \Lambda$ such that roughly $L_p(s, \chi) = f_{\gamma,\chi}(\kappa^s - 1)$ for $\kappa \in 1 + p\mathbb{Z}_p$ and $\gamma(\zeta_n) = \zeta_n^\kappa$.

Similar to the analytic class number formula, the Kubota-Leopold L-function is going to be the analytic side of a formula connecting it to an algebraic object. To construct the latter, let L_n be the maximal unramified abelian extension of $\mathbb{Q}_n$ of p-power degree. Define $L_\infty = \bigcup_{n\in\mathbb{N}} L_n$ and consider $X_\infty = \mathrm{Gal}(L_\infty|\mathbb{Q}_\infty)$.

Now X_∞ admits a Γ-action in the following way: Choose an extension $\tilde{\gamma}$ of $\gamma \in \Gamma$ to L_∞, i. e. a lift in $\mathrm{Gal}(L_\infty|\mathbb{Q})$. Then

$$\gamma \cdot x = \tilde{\gamma} x (\tilde{\gamma})^{-1}$$

defines a well-defined action of Γ on X_∞. This can be linearly (and continuously) extended to an action of Λ.

Observe that $X_n = \mathrm{Gal}(L_n|\mathbb{Q}_\infty) \cong A_{F_n}$ by class field theory. Iwasawa showed that X_∞ is a finitely generated torsion Λ-module.

(8.14) Theorem (*Iwasawa Main Conjecture*)**.**

$$\mathrm{char}(\chi \text{ component of } X_\infty) = \text{ unit } \times f_{\gamma,\chi}.$$

The Iwasawa Main conjecture was proven for $\mathbb{Q}$ by Mazur-Wiles (1984) and for totally real fields by Wiles (1990).

An analogous Main Conjectures exists also for elliptic curves. This conjecture is however only proven for a small number of very special cases and a proof would imply the p-part of the Birch-Swinnerton-Dyer Conjecture.