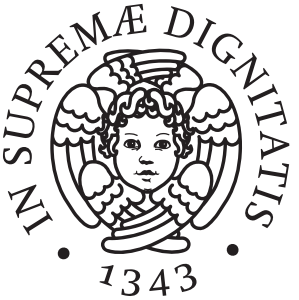
Università di Pisa



Facoltà di Matematica

Teoria del campo di classe locale

Tesi di Laurea Triennale
in Matematica

Candidato
Andrea Gallese

Relatore
Davide Lombardo
Università di Pisa

Anno Accademico 2018 - 2019

Indice

Indice **1**

Introduzione **3**

1 Coomologia di Gruppi **5**
1.1 Costruzione 6
1.2 Funtorialità 8
1.3 Successione Spettrale di Hochschild-Serre 10
1.4 Corestrizione 10
1.5 Gruppi di Tate 13
1.6 Moduli Indotti 15

2 Esplorazione **17**
2.1 Gruppi Ciclici 17
2.2 Banalità Coomologica 19
2.3 Dimensione Coomologica 22

3 Campi Locali **27**
3.1 Teoria di Galois 27
3.2 Teoria di Kummer 29
3.3 Struttura di un Campo Locale 31
3.4 Calcolo del gruppo di Brauer 33
3.5 Tutto il resto 36

4 Risultati di Dualità **39**
4.1 Tazza Prodotto 39
4.2 Dualità di Tate-Nakayama 41
4.3 Reciprocità Locale 44
4.4 Dualità di Tate 45

Bibliografia **51**

Introduzione

La teoria del campo di classe è lo studio delle estensioni abeliane di un campo K globale o, come nel nostro caso, locale. L'obiettivo principale di questa teoria è la descrizione del gruppo di Galois relativo alla massima estensione abeliana di K in termini di struttura aritmetica e topologica del campo stesso. In particolare, dimostreremo che questo gruppo è, nel caso p-adico, il completamento profinito del gruppo moltiplicativo del campo.

Affronteremo lo studio di questa teoria secondo gli approcci più moderni: introdurremo la coomologia di gruppi come il derivato del funtore che "prende gli invarianti" e dedicheremo i primi due capitoli a raffinare questo linguaggio, così da essere sicuri di avere tutti i vocaboli necessari per discutere della teoria di Galois. Mostreremo che la riformulazione di alcuni risultati classici in teoria dei campi, attraverso il nostro strumento, risulta piacevole, elegante e sintetica: procederemo dunque ad una minuziosa opera di traduzione delle proprietà aritmetiche dei campi locali in termini coomologici.

I campi locali presentano una struttura aritmetica relativamente semplice, della quale ci serviremo per calcolare la coomologia del gruppo di Galois assoluto. In particolare, uno studio dettagliato dell'estensione non ramificata massimale ci permetterà di dedurre numerose proprietà coomologiche del gruppo di Galois assoluto di K. Questi risultati ci permetteranno di produrre gli isomorfismi necessari a calcolare il gruppo di Brauer e la dimensione coomologica di questo tipo di campi.

Conclusi i preparativi, presenteremo il prodotto naturale della teoria coomologica in esame. Questo permette di costruire degli interessanti isomorfismi tra gruppi di coomologia con coefficienti diversi, che possiamo raggruppare sotto due celebri teoremi di dualità, dovuti rispettivamente a Tate-Nakayama e a Tate. Interpretando opportunamente la prima di queste dualità, riusciremo a costruire un isomorfismo esplicito tra i gruppi di Galois delle estensioni abeliane e alcuni quozienti del gruppo moltiplicativo del campo, l'applicazione di reciprocità locale; sfrutteremo invece la dualità di Tate per calcolare l'abelianizzato del gruppo di Galois assoluto di un campo p-adico, concludendo in bellezza lo studio della teoria del campo di classe locale.

La trattazione dell'argomento segue quasi interamente gli appunti di un corso tenuto dal prof. D. Harari, dal titolo "Théorie du corps de classes" [Har13].

CAPITOLO 1

Coomologia di Gruppi

L'obiettivo di questo primo capitolo è introdurre la coomologia di gruppi, mostrarne le principali proprietà e presentare alcune generalizzazioni.

Poniamoci nella dovuta generalità. Sia G un gruppo, consideriamo la categoria Mod_G costituita dai gruppi abeliani muniti di un'azione di G, i cui morfismi siano le mappe che ne rispettano la struttura: gli omomorfismi di gruppo G-equivarianti. Equivalentemente, possiamo pensare a Mod_G come la categoria dei moduli sull'anello di gruppo $\mathbb{Z}[G]$. In quest'ottica, è naturale riferirsi agli oggetti della nostra categoria come "G-moduli". Per fissare le idee si pensi, per esempio, al gruppo di Galois di un'estensione finita L/K; questo agisce naturalmente su L e di conseguenza su tutti i campi intermedi normali, rendendo sia il loro gruppo additivo che il loro gruppo moltiplicativo dei $\mathcal{G}al\,(L/K)$-moduli.

Siamo interessati al funtore $\mathcal{F}$ che, preso un modulo, restituisce il sottomodulo costituito dagli elementi invarianti rispetto all'azione del gruppo

$$\begin{aligned}\mathcal{F}\colon \mathsf{Mod}_G &\to \mathcal{A}b\\ A &\mapsto A^G = \{a \in A \mid ga = a\ \forall\, g \in G\},\end{aligned}$$

di evidente importanza in Teoria di Galois. Questo funtore è esatto a sinistra ma, in generale, non a destra. Partendo questo da una categoria con abbastanza iniettivi, ci è concesso prenderne il derivato destro $R^i\mathcal{F}$, da cui la nostra prima definizione.

□ **Definizione 1.0.1.** Dato un gruppo finito G e un intero i non negativo, chiamiamo i-esimo gruppo di coomologia di G il derivato destro

$$\mathrm{H}^i(G, \bullet) := R^i\mathcal{F}(\bullet).$$

Con questa definizione, grazie alla magia occulta dei funtori derivati, assegniamo a uno G-modulo A un'intera famiglia di invarianti $\mathrm{H}^i(G, A)$, il cui studio ci permetterà di descrivere meglio sia il modulo che il gruppo in questione. Dall'altro lato la definizione appena data sembra, al momento, un cambio di notazione completamente arbitrario: perché non continuare a chiamare i nostri oggetti funtori derivati per il resto della tesi? Limitiamoci ad

osservare che la presentazione scelta mette in evidenza la proprietà fondamentale di questi oggetti.

■ **Teorema 1.0.2.** *Data una successione esatta corta di G moduli*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

si ha una successione esatta lunga di gruppi abeliani

$$\begin{aligned} 0 &\longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \\ &\hookrightarrow \mathrm{H}^1(G, A) \longrightarrow \mathrm{H}^1(G, B) \longrightarrow \mathrm{H}^1(G, C) \\ &\hookrightarrow \mathrm{H}^2(G, A) \longrightarrow \dots \end{aligned}$$

Questa proposizione, come molte altre proprietà dei funtori derivati, non verrà dimostrata: ci limiteremo a ricordare alcuni risultati e lasceremo a un buon libro di algebra [Wei94] il compito di indagare i misteri dell'algebra omologica. Per evidenziare però che non stiamo usando della teoria particolarmente esotica aggiungerei la seguente rassicurazione:

Osservazione 1.0.3. Indichiamo con $\mathbb{Z}$, da qui in avanti, il G-modulo costituito dal gruppo additivo degli interi munito dell'azione banale. Il funtore $\mathcal{F}$ che abbiamo deciso di studiare non è altro che $\mathrm{Hom}_G(\mathbb{Z}, \bullet)$: infatti, affinché un omomorfismo di gruppi da $\mathbb{Z}$ in un modulo qualunque sia G equivariante, è necessario e sufficiente che l'immagine di 1 sia un punto fisso dell'azione. Il derivato destro è dunque il familiare $\mathrm{Ext}^i_G(\mathbb{Z}, \bullet)$.

Ricorderemo comunque velocemente la costruzione astratta del funtore derivato, cogliendo l'occasione per dare una qualche intuizione dietro alcuni dei risultati che enunceremo.

1.1 Costruzione

Ci sono due strade equivalenti per ottenere i gruppi $\mathrm{H}^i(G, A)$: possiamo partire da una risoluzione proiettiva di $\mathbb{Z}$ come G-modulo

$$\dots \to P_2 \to P_1 \to P_0 \to \mathbb{Z} \to 0,$$

applicare il funtore controvariante $\mathrm{Hom}_G(\bullet, A)$ per ottenere il complesso coomologico

$$0 \to \mathrm{Hom}(P_0, A) \to \mathrm{Hom}(P_1, A) \to \mathrm{Hom}(P_2, A) \to \dots$$

e infine prenderne la coomologia; oppure partire da una risoluzione iniettiva di A

$$0 \to A \to I^0 \to I^1 \to I^2 \to \dots,$$

applicare il funtore covariante $\mathcal{F} = \mathrm{Hom}_G(\mathbb{Z}, \bullet)$ per ottenere il complesso coomologico

$$0 \to \mathcal{F}\left(I^0\right) \to \mathcal{F}\left(I^1\right) \to \mathcal{F}\left(I^2\right) \to \dots,$$

e, ancora una volta, prenderne la coomologia.

Non è banale mostrare né che le due definizioni non dipendono dalla risoluzione scelta né che sono equivalenti, ma per fortuna non ce ne occuperemo. Dalla costruzione è comunque evidente che tutti i moduli iniettivi hanno coomologia banale

$$\mathrm{H}^i(G,\, I) = 0 \quad \forall\, i > 0. \tag{1.1}$$

Equivalentemente, possiamo ottenere i gruppi $\mathrm{H}^i(G,\, A)$ come coomologia dal complesso

$$0 \to K^0(A) \to K^1(A) \to K^2(A) \to \dots,$$

dove $K^i(A) = \{f\colon G^i \to A\}$ è il gruppo (abeliano) delle applicazioni in i-variabili dal gruppo G in A e i differenziali $\delta^i\colon K^i \to K^{i+1}$ sono definiti da un'inintelligibile somma a segni alterni, nel classico stile della coomologia singolare:

$$\begin{aligned}\delta f(g_1,\, \dots,\, g_{i+1}) = {} & g_1 f(g_2,\, \dots,\, g_{i+1}) \\ & + \sum_{j=1}^{i} (-1)^j f(g_1,\, \dots,\, g_j g_{j+1},\, \dots,\, g_{i+1}) \\ & + (-1)^{i+1} f(g_1, \dots, g_i).\end{aligned}$$

Questa definizione ha il vantaggio di fornirci una descrizione esplicita degli elementi del gruppo $\mathrm{H}^i(G,\, A)$, detti "cocatene"; descrizione che, pur avendo una qualche utilità in grado basso ($i = 0,\, 1$), risulta troppo macchinosa per poterci effettivamente lavorare. Dunque, ricaviamone quanto possibile e dimentichiamocene in fretta. Avendo una presentazione esplicita degli elementi, ci è concesso cominciare qualche ragionamento di cardinalità: se A è finito, allora ogni gruppo $K^i(A)$ è finito e di conseguenza lo è anche ogni suo quoziente.

Lemma 1.1.1. *Se sia G che A sono finiti, allora tutti i gruppi di coomologia $\mathrm{H}^i(G,\, A)$ sono finiti.*

Una volta trovato il coraggio di scrivere per esteso nuclei e immagini dei differenziali di grado basso, è possibile calcolare esplicitamente il gruppo in grado zero, $\mathrm{H}^0(G,\, A) = A^G$, e il gruppi in grado uno quando G agisce banalmente su A, nel qual caso si presenta nella docile forma di $\mathrm{H}^1(G,\, A) = \mathrm{Hom}_{\mathbb{Z}}(G,\, A)$.

Verso il profinito. La teoria per gruppi arbitrariamente complessi procede, ma a noi è concesso il lusso di qualche ipotesi di comodità. In Teoria di Galois compaiono solo gruppi finiti o, mal che vada, profiniti; potremo quindi assumere quasi sempre che G sia finito, a patto però di estendere il nostro linguaggio in modo da comprendere anche i gruppi profiniti. Ricordiamo che un gruppo profinito G è, per definizione, limite inverso di gruppi finiti G_n muniti della topologia discreta:

$$G = \varprojlim_n G_n$$

La difficoltà principale che si pone è l'entrata in scena della topologia: la categoria dei G-moduli non è adatta ai nostri scopi, perché non tiene conto della geometria del gruppo. Chiediamo quindi il minimo indispensabile, ovvero che i G-moduli siano muniti di una topologia per cui l'azione di G sia continua; oppure, equivalentemente, che lo stabilizzatore di ogni punto sia aperto. In questa nuova categoria si riesce a definire la coomologia per gruppi profiniti, esattamente come fatto sopra per i gruppi, perché questa ha abbastanza iniettivi [Wei94, Lemma 6.11.10]; per nostra fortuna la coomologia dei gruppi profiniti si riconduce al calcolo sui quozienti finiti, pertanto svilupperemo la teoria per i soli gruppi finiti e cercheremo, solo alla fine, di capire se e come è possibile estenderla ai gruppi profiniti.

1.2 Funtorialità

I gruppi di coomologia sono funtoriali nei coefficienti A per costruzione, ma cosa succede quando cambiamo il gruppo G? Un problema che si pone immediatamente, seppur puramente formale, è che cambiando gruppo usciamo dalla categoria ambiente: abbiamo quindi bisogno del cugino del funtore dimenticante.

□ **Definizione 1.2.1.** Dati due gruppi G e H, un omomorfismo $f\colon H \to G$ e uno G-modulo A, chiamiamo $f^\times A$ il gruppo abeliano A munito dell'azione

$$h \cdot_H A := f(h) \cdot_G A \qquad \forall\, h \in H.$$

È bene ribadire che $f^\times$ è un'operazione puramente formale che ci aiuta a sottolineare quando stiamo pensando a un dato gruppo abeliano con un'azione diversa da quella con la quale è stato introdotto; inizieremo presto a omettere $f^\times$ per semplificare la notazione, lasciando che sia il contesto a suggerire la giusta azione. Osserviamo inoltre che l'operazione è parzialmente invertibile, in almeno due modi diversi: possiamo considerare il G-modulo

$$\mathrm{Ind}_H^G = \mathbb{Z}[G] \otimes_H A$$

oppure munire il gruppo abeliano

$$\mathrm{coInd}_H^G(A) := \{f\colon G \to A \mid f(hg) = h \cdot f(g) \ \ \forall\, h \in H\} = \mathrm{Hom}_H(\mathbb{Z}[G],\, A)$$

di un'azione di G molto naturale: $g \cdot f(x) = f(xg)$ per ogni $g \in G$. Questi recuperano quanto dimenticato nel seguente senso:

■ **Proposizione 1.2.2.** *Entrambi i funtori*

$$\mathrm{coInd}\colon \mathsf{Mod_H} \to \mathsf{Mod_G} \qquad e \qquad \mathrm{Ind}_H^G\colon \mathsf{Mod_H} \to \mathsf{Mod_G}$$

sono aggiunti ad $f^\times$. Ovvero, per ogni $A \in \mathsf{Mod_G}$ e $B \in \mathsf{Mod_H}$, soddisfano

$$\mathrm{Hom}_H(f^\times A,\, B) = \mathrm{Hom}_G(A,\, \mathrm{coInd}_H^G(B)) \quad e \quad \mathrm{Hom}_H(A,\, f^\times B) = \mathrm{Hom}_G(\mathrm{Ind}_H^G(A),\, B)$$

Siamo finalmente pronti per affrontare il risultato principale del capitolo, che ci permetterà di costruire tutte le mappe di cui avremo bisogno in seguito.

■ **Proposizione 1.2.3.** *Siano A uno G-modulo e A' un H-modulo. Dati $f\colon H \to G$ un omomorfismo di gruppi e $u\colon f^\times A \to A'$ un omomorfismo H-equivariante, otteniamo una mappa in coomologia*

$$\mathrm{H}^i(G,\, A) \to \mathrm{H}^i(H,\, A') \qquad \forall i \geq 0.$$

Dimostrazione. Poiché i funtori derivati $\mathrm{H}^i(G, \bullet)$ sono universali per costruzione [Wei94, Th. 2.4.7], esiste un (unico) sollevamento della trasformazione naturale

$$\mathrm{H}^0(G,\, A) = A^G \hookrightarrow (f^\times A)^H = \mathrm{H}^0(H,\, f^\times A)$$

a un morfismo tra gruppi di coomologia in ogni grado. Dalla funtorialità di $\mathrm{H}^i(H, \bullet)$ nel secondo argomento, otteniamo la tesi componendo la mappa appena trovata con quella indotta da u. □

Affrontato il problema nella dovuta generalità, decliniamo la soluzione nei casi a cui siamo interessati: fissiamo un sottogruppo H di G. Concederemo un nome alle mappe più naturali e, al contempo, più rilevanti nello studio dei gruppi di coomologia.

□ **Definizione 1.2.4** (Restrizione)**.** Chiamiamo mappa di restrizione l'omomorfismo

$$\texttt{res}\colon \mathrm{H}^i(G,\, A) \to \mathrm{H}^i(H,\, \iota^\times A)$$

indotto dall'inclusione naturale $\iota\colon H \to G$.

□ **Definizione 1.2.5** (Inflazione)**.** Chiamiamo mappa d'inflazione l'omomorfismo

$$\texttt{inf}\colon \mathrm{H}^i(G/H,\, A^H) \to \mathrm{H}^i(G,\, A)$$

indotto dalla proiezione naturale $\pi\colon G \to G/H$ e dall'inclusione $u\colon A^H \to A$.

Un'altra mappa che si incontra spontaneamente in natura è quella indotta dal coniugio: lasciamo agire G su se stesso per coniugio e, fissato un elemento $t \in G$, consideriamo il relativo automorfismo interno $\sigma_t\colon G \to G$. Questo induce un automorfismo di $\mathrm{H}^i(G,\, A)$ che riusciamo a descrivere esplicitamente.

■ **Proposizione 1.2.6.** *L'isomorfismo indotto dal coniugio per t*

$$\sigma_t\colon \mathrm{H}^i(G,\, A) \to \mathrm{H}^i(G,\, A)$$

è l'identità.

Dimostrazione. Dimostriamo il risultato per décalage: per $i = 0$ non c'è nulla da dimostrare. Supponiamo ora la tesi fino al grado i. Preso un modulo A, consideriamo un'immersione in un modulo iniettivo I:

$$0 \to A \to I \to Q \to 0.$$

La successione esatta lunga associata (per 1.0.2) è costellata di zeri ovunque si prenda la coomologia di I (per 1.1), rimangono quindi solo il segmento iniziale

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A^G & \longrightarrow & I^G & \longrightarrow & Q^G & \longrightarrow & \mathrm{H}^1(G,\, A) \longrightarrow 0 \\
 & & \downarrow{\scriptstyle \sigma_t=\mathrm{id}} & & \downarrow{\scriptstyle \sigma_t=\mathrm{id}} & & \downarrow{\scriptstyle \sigma_t=\mathrm{id}} & & \downarrow{\scriptstyle \sigma_t} \\
0 & \longrightarrow & A^G & \longrightarrow & I^G & \longrightarrow & Q^G & \longrightarrow & \mathrm{H}^1(G,\, A) \longrightarrow 0
\end{array}$$

e alcuni frammenti per $i > 0$

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{H}^i(G,\, Q) & \longrightarrow & \mathrm{H}^{i+1}(G,\, A) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \sigma_t=\mathrm{id}} & & \downarrow{\scriptstyle \sigma_t} & & \\
0 & \longrightarrow & \mathrm{H}^i(G,\, Q) & \longrightarrow & \mathrm{H}^{i+1}(G,\, A) & \longrightarrow & 0,
\end{array}$$

da cui deduciamo la tesi in grado $i + 1$. □

Verso il profinito. Possiamo ora enunciare il risultato che ci ha permesso di confinare i gruppi profiniti in queste piccole parentesi: la coomologia dei gruppi profiniti si riconduce a quella dei gruppi finiti.

■ *Proposizione* 1.2.7. *Sia G un gruppo profinito che agisce su un modulo A, allora*

$$\mathrm{H}^n(G, A) = \varinjlim_{U<G} \mathrm{H}^n(G/U, A^U),$$

dove U varia tra i sottogruppi normali aperti *di G.*

1.3 Successione Spettrale di Hochschild-Serre

Sia H un sottogruppo normale di G. Ha senso considerare i funtori $\mathcal{F}\colon A \to A^H$, che manda G-moduli in G/H-moduli, e $\mathcal{G}\colon B \to B^{G/H}$, che manda G/H-moduli in gruppi abeliani. La loro composizione è il funtore che prende gli invarianti per l'azione di G. Una volta verificato che i moduli iniettivi vengono mandati in moduli aciclici, possiamo prendere la successione spettrale di Grothendieck associata, che nel caso in questione è detta successione spettrale di Hochschild-Serre.

■ **Teorema 1.3.1** (Hochschild-Serre)**.** *Esiste una successione spettrale di primo quadrante, convergente*

$$E_2^{pq} = \mathrm{H}^p(G/H, \mathrm{H}^q(H, A)) \;\Rightarrow\; \mathrm{H}^{p+q}(G, A).$$

Siamo fondamentalmente interessati a sfruttare la filtrazione in grado basso per produrre una successione esatta.

▼ **Corollario 1.3.2** (Successione Restrizione-Inflazione)**.** *Si trova la successione esatta:*

$$0 \longrightarrow \mathrm{H}^1(G/H, A^H) \xrightarrow{\texttt{inf}} \mathrm{H}^1(G, A) \xrightarrow{\texttt{res}} \mathrm{H}^1(H, A)^{G/H} \xrightarrow{\texttt{trs}} \mathrm{H}^2(G/H, A^H) \xrightarrow{\texttt{inf}} \mathrm{H}^2(G, A).$$

Variando lievemente l'argomentazione, troviamo anche la successione seguente.

▼ **Corollario 1.3.3** (Successione Restrizione-Inflazione)**.** *Se $\mathrm{H}^i(H, A) = 0$ per ogni $1 \leq i < q$, si trova allora la successione esatta:*

$$0 \longrightarrow \mathrm{H}^q(G/H, A^H) \xrightarrow{\texttt{inf}} \mathrm{H}^q(G, A) \xrightarrow{\texttt{res}} \mathrm{H}^q(H, A).$$

Verso il profinito. La successione spettrale di Hochschild-Serre è ben definita anche per G profinito, una volta assunto che H sia un sottogruppo normale *chiuso* (in modo da preservare la delicata topologia profinita) di G. Ne ricaviamo analoghi corollari.

1.4 Corestrizione

Costruiamo ora una mappa che va nella direzione opposta rispetto alla restrizione, ovvero che in qualche modo risale dalla coomologia di H a quella di G. Per costruire questa mappa è fondamentale che l'indice $[G : H]$ sia finito, cosa che accade sicuramente supponendo G finito.

□ **Definizione 1.4.1** (Corestrizione)**.** Fissiamo uno G-modulo A e un sottogruppo $H < G$. In grado $i = 0$ definiamo la corestrizione tra $A^H \to A^G$ come la *norma*

$$N_{G/H}\colon a \mapsto \sum_{x \in G/H} x \cdot a,$$

che coincide con la moltiplicazione per l'elemento $N = \sum_{g\in R} g$ di $\mathbb{Z}[G]$, somma di rappresentanti delle classi laterali di H. Vale la pena di osservare subito che, proprio perché si identifica con la moltiplicazione per N, tutti i diagrammi che induce commutano: preso un morfismo $f\colon A \to B$ il diagramma

$$\begin{array}{ccc} A^H & \xrightarrow{f} & B^H \\ \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} \\ A^G & \xrightarrow{f} & B^G \end{array}$$

commuta, perché, per definizione, la mappa f è $\mathbb{Z}[G]$-lineare.

Quando H è un sottogruppo di G, le definizioni di indotto e coindotto coincidono

$$\mathrm{Hom}_H(\mathbb{Z}[G],\, A) \simeq \mathbb{Z}[G] \otimes_H A,$$

smetteremo dunque di distinguerli. Ne segue che $\mathrm{Ind}_H^G(\,\bullet\,)$ è un funtore esatto, dunque che $f^\times$, essendone l'aggiunto da ambo i lati (per 1.2.2), preserva sia iniettivi che proiettivi. Per estendere la mappa a tutti i gradi possiamo quindi partire da una risoluzione iniettiva di A, prenderne gli invarianti sia rispetto ad H che a G e, prima di prenderne l'omologia, applicare la norma per ottenere un morfismo di complessi

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \left(I^0\right)^H & \longrightarrow & \left(I^1\right)^H & \longrightarrow & \left(I^2\right)^H & \longrightarrow & \dots \\ & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} & & \\ 0 & \longrightarrow & \left(I^0\right)^G & \longrightarrow & \left(I^1\right)^G & \longrightarrow & \left(I^2\right)^G & \longrightarrow & \dots \end{array}$$

e quindi una mappa in coomologia che chiamiamo *corestrizione*:

$$\texttt{cor}\colon \mathrm{H}^i(H,\, A) \to \mathrm{H}^i(G,\, A).$$

La nostra prima preoccupazione è controllare come la corestrizione si comporta rispetto alla restrizione: osserviamo che componendo le due mappe otteniamo un endomorfismo di $\mathrm{H}^i(G,\, A)$. Riusciamo a descrivere questo omomorfismo esplicitamente.

■ **Teorema 1.4.2.** *Sia $m = [G : H]$ l'indice di H in G. La composizione*

$$\mathrm{H}^i(G,\, A) \xrightarrow{\texttt{res}} \mathrm{H}^i(H,\, A) \xrightarrow{\texttt{cor}} \mathrm{H}^i(G,\, A)$$

coincide con la moltiplicazione per m.

Dimostrazione. La dimostrazione è per décalage: in $i = 0$ ritroviamo l'azione della norma su elementi fissati dall'azione di G

$$A^G \xhookrightarrow{\iota} A^H \xrightarrow{N} A^G$$

che è proprio $\sum_{x\in G/H} x \cdot a = ma$, trovando su A^G l'azione banale di G/H. Supponiamo ora la tesi vera fino al grado i, per ogni G-modulo. Immergiamo A in un iniettivo I, così da ottenere la successione esatta corta

$$0 \to A \to I \to Q \to 0,$$

la cui successione esatta lunga associata (per 1.0.2) è costellata di zeri ovunque si prenda la coomologia dell'iniettivo (per 1.1), rimangono quindi solo il segmento iniziale

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^G & \longrightarrow & I^G & \longrightarrow & Q^G & \longrightarrow & \mathrm{H}^1(G,\, A) \longrightarrow 0 \\ & & \downarrow{\scriptstyle \cdot m} & & \downarrow{\scriptstyle \cdot m} & & \downarrow{\scriptstyle \cdot m} & & \downarrow{\scriptstyle \mathtt{cor}\cdot\mathtt{res}} \\ 0 & \longrightarrow & A^G & \longrightarrow & I^G & \longrightarrow & Q^G & \longrightarrow & \mathrm{H}^1(G,\, A) \longrightarrow 0 \end{array}$$

e alcuni frammenti per $i > 0$

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{H}^i(G,\, Q) & \longrightarrow & \mathrm{H}^{i+1}(G,\, A) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \cdot m} & & \downarrow{\scriptstyle \mathtt{cor}\cdot\mathtt{res}} & & \\ 0 & \longrightarrow & \mathrm{H}^i(G,\, Q) & \longrightarrow & \mathrm{H}^{i+1}(G,\, A) & \longrightarrow & 0, \end{array}$$

da cui deduciamo la tesi in grado $i + 1$. □

Abbiamo ottenuto un risultato molto piacevole: componendo due mappe particolarmente misteriose, definite in modo bizzarro e algebricamente macchinoso, agiamo sugli elementi in modo elementare. Questo trucco edifica un ponte tra l'algebra omologica e l'aritmetica, che possiamo attraversare per tornare indietro con un paio di comodi risultati; per esempio, prendendo il sottogruppo banale $H = \{1\}$ la composizione di restrizione e corestrizione

$$\mathrm{H}^i(G,\, A) \xrightarrow{\mathtt{res}} \mathrm{H}^i(H,\, A) = 0 \xrightarrow{\mathtt{cor}} \mathrm{H}^i(G,\, A)$$

è necessariamente nulla, dunque:

▼ **Corollario 1.4.3.** *Sia $n = [G : 1]$ l'ordine di G. I gruppi di coomologia $\mathrm{H}^i(G,\, A)$ sono di n-torsione, per ogni $i > 0$.*

Iniziamo ad avere qualche informazione importante su come sono fatti questi gruppi! Se per esempio sapessimo che A è finitamente generato e di conseguenza $\mathrm{H}^i(G,\, A)$ è finitamente generato (per la descrizione esplicita in cocatene, per dire), scopriremmo dunque che dev'essere finito, in quanto finitamente generato e di torsione.

Tra le meraviglie dell'aritmetica, troviamo il seguente risultato, tanto più raffinato del precedente quanto della meno chiara utilità. Si tratta di un primo passo verso la decomposizione dello studio dei gruppi di coomologia nello studio delle singole componenti primarie e si rivelerà fondamentale quando affronteremo il discorso più dettagliatamente.

Lemma 1.4.4. *Preso un primo p per cui $[G : H]$ è coprimo con p, la restrizione è iniettiva sulla componente p-primaria di $\mathrm{H}^i(G,\, A)$:*

$$0 \longrightarrow T_p\, \mathrm{H}^i(G,\, A) \xrightarrow{\mathtt{res}} \mathrm{H}^i(H,\, A).$$

Sotto queste ipotesi, infatti, la composizione $\mathtt{cor}\cdot\mathtt{res}$ si restringe ad una mappa iniettiva, dunque la mappa più interna, la restrizione, dev'essere iniettiva a sua volta. Per di più, osserviamo che è stato introdotto surrettiziamente un nuovo pezzettino di notazione: T_pM sarà da qui in poi la componente p-primaria del gruppo abeliano M.

Verso il profinito. La norma, e di conseguenza la corestrizione, è ben definita per ogni sottogruppo U d'indice finito e chiuso di G. Poiché i sottogruppi chiusi d'indice finito coincidono con quelli aperti, il corollario sulla torsione 1.4.3 si estende ai gruppi profiniti: il limite diretto non può che mandare gruppi di torsione in gruppi di torsione.

1.5 Gruppi di Tate

La coomologia di gruppi introdotta fino a questo momento è accompagnata, poco sorprendentemente, da una duale teoria omologica. I due strumenti si riescono a mettere in comunicazione fra loro e, modificati opportunamente, a riunire in un unico grande macchinario: i gruppi di coomologia di Tate, $\widehat{\mathrm{H}}^i(G,\, A)$.

Consideriamo il funtore $\mathcal{G}$ che, preso un modulo, restituisce il più grande quoziente su cui G agisce banalmente, detto modulo dei co-invarianti:

$$\begin{aligned} \mathcal{G}\colon \mathsf{Mod}_{\mathsf{G}} &\to \mathcal{A}b \\ A &\mapsto A_G. \end{aligned}$$

Riusciamo a descrivere $\mathcal{G}$ esplicitamente osservando che il nucleo della proiezione $A \to A_G$ dev'essere il sottomodulo generato dagli elementi della forma $(a - ga)$, infatti quozientare per quest'ultimo corrisponde esattamente a imporre che l'azione sia banale. Nel caso dell'anello di gruppo otteniamo il cosiddetto *ideale di augmentazione*:

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0,$$

che ci fornisce una descrizione semplice del funtore in analisi

$$\mathcal{G}\colon A \to A_G = A/I_G A = A \otimes_G \mathbb{Z}.$$

Essendo un prodotto tensore, $\mathcal{G}$ è esatto a destra ma, in generale, non a sinistra. Possiamo quindi prenderne il derivato sinistro:

□ **Definizione 1.5.1** (Omologia di Gruppi)**.** Dato un gruppo finito G e un intero $i \geq 0$, chiamiamo i-esimo gruppo di omologia di G il funtore

$$\mathrm{H}_i(G,\, \bullet\,) := L^i\mathcal{G}(\,\bullet\,) = \mathrm{Tor}_G(\mathbb{Z},\, \bullet\,).$$

Otteniamo così un funtore omologico, per cui vale il duale di praticamente ogni teorema enunciato fin'ora per il corrispondente funtore coomologico: ad una successione esatta corta sarà associata una lunga in omologia, potremo definire delle opportune mappe di restrizione, corestrizione e coinflazione... Le dimostrazioni di questi teoremi si ottengono dualizzando quelle presentate: non saremo così diligenti da riscriverle, ci limitiamo ad incoraggiare il lettore interessato a rileggerle, sostituendo "iniettivo" con "proiettivo" e guardando i diagrammi attraverso uno specchio.

Occupiamoci piuttosto del collegamento tra i due strumenti. L'obiettivo principale è raccordare le due successioni esatte lunghe in una successione lunghissima, illimitata in entrambe le direzioni. L'unico problema che si presenta è che, al momento, entrambe le

successioni terminano: dovremo quindi modificare i gruppi terminali di ciascuna. Per fare questo prendiamo la norma associata al sottogruppo banale

$$\begin{aligned} N\colon A &\to A^G \\ a &\mapsto \sum_{g\in G} g\cdot a \end{aligned}$$

e osserviamo che passa al quoziente $N\colon A/I_G \to A^G$.

□ **Definizione 1.5.2** (Gruppi di Tate)**.** Questa definizione è quasi esclusivamente un cambio di notazione: i gruppi di grado positivo saranno i coomologici, mentre quelli di grado negativo saranno gli omologici

$$\widehat{\mathrm{H}}^i(G,\,A) = \mathrm{H}_i(G,\,A) \quad \forall\, i>0, \qquad\qquad \widehat{\mathrm{H}}^{-i}(G,\,A) = \mathrm{H}_{i-1}(G,\,A) \quad \forall\, i>1;$$

definiamo invece i gruppi di Tate di grado $i=-1,\,0$ come ker e coker della norma:

$$0 \longrightarrow \widehat{\mathrm{H}}^{-1}(G,\,A) \longrightarrow A_G \xrightarrow{N} A^G \longrightarrow \widehat{\mathrm{H}}^{0}(G,\,A) \longrightarrow 0. \tag{1.2}$$

Sistemati i dettagli ad arte, enunciamo il risultato che ricompensa i nostri sforzi.

■ **Teorema 1.5.3.** *Data una successione esatta corta di G moduli*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

si ha una successione esatta lunghissima di gruppi abeliani

$$\begin{aligned} \ldots \longrightarrow \widehat{\mathrm{H}}^{-2}(G,\,C) \longrightarrow \widehat{\mathrm{H}}^{-1}(G,\,A) \longrightarrow \widehat{\mathrm{H}}^{-1}(G,\,B) \longrightarrow \widehat{\mathrm{H}}^{-1}(G,\,C) \longrightarrow \\ \longrightarrow \widehat{\mathrm{H}}^{0}(G,\,A) \longrightarrow \widehat{\mathrm{H}}^{0}(G,\,B) \longrightarrow \widehat{\mathrm{H}}^{0}(G,\,C) \longrightarrow \widehat{\mathrm{H}}^{1}(G,\,A) \longrightarrow \ldots \end{aligned}$$

Dimostrazione. La dimostrazione è una delicata operazione di incollamento: avviciniamo le due estremità che desideriamo saldare e colleghiamole provvisoriamente tramite la norma, che già sappiamo produrre dei quadrati commutativi. Una volta invocato il Lemma dei Cinque, la tesi segue dalla contemplazione del seguente diagramma

$$\begin{array}{ccccccccccc} & & & & \widehat{\mathrm{H}}^{-1}(G,\,A) & \dashrightarrow & \widehat{\mathrm{H}}^{-1}(G,\,B) & \dashrightarrow & \widehat{\mathrm{H}}^{-1}(G,\,C) & \dashrightarrow & \\ & & & & \downarrow & & \downarrow & & \downarrow & & \\ \ldots & \longrightarrow & \widehat{\mathrm{H}}^{-2}(G,\,C) & \xrightarrow{\delta_0} & A_G & \longrightarrow & B_G & \longrightarrow & C_G & \longrightarrow & 0 \\ & & & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A^G & \longrightarrow & B^G & \longrightarrow & C^G & \xrightarrow{\delta^0} & \widehat{\mathrm{H}}^{1}(G,\,A) & \longrightarrow & \ldots \\ & & \downarrow & & \downarrow & & \downarrow & & & & \\ & & \widehat{\mathrm{H}}^{0}(G,\,A) & \dashrightarrow & \widehat{\mathrm{H}}^{0}(G,\,B) & \dashrightarrow & \widehat{\mathrm{H}}^{0}(G,\,C). & \dashrightarrow & & & \end{array}$$

□

Tutti i risultati che abbiamo dimostrato per i gruppi di coomologia e vi abbiamo convinto valere anche per i gruppi di omologia, si estenderanno ai gruppi di Tate: le mappe di restrizione, inflazione e corestrizione diventano morfismi di successioni esatte lunghissime non appena ci si accorge che le loro definizioni classiche in grado $i = 0, -1$ fattorizzano tramite la norma.

Verso il profinito. Nonostante sia possibile estendere i gruppi di Tate anche a gruppi profiniti, non faremo questo sforzo, limitandoci a non usarli.

1.6 Moduli Indotti

Introduciamo un'importante famiglia di moduli, il cui calcolo della coomologia rientra di diritto nei prerequisiti teorici. L'inclusione naturale $\iota\colon H \to G$, assieme alla proiezione $u\colon \mathrm{Ind}_H^G(A) \to A$ data dalla valutazione nell'elemento neutro, induce (per 1.2.3) un omomorfismo

$$\mathrm{H}^i(G,\, \mathrm{Ind}_H^G(A)) \to \mathrm{H}^i(H,\, A),$$

particolarmente semplice in coomologia.

Lemma 1.6.1 (di Shapiro)**.** *L'omomorfismo sopra definito*

$$\mathrm{H}^i(G,\, \mathrm{Ind}_H^G(A)) \to \mathrm{H}^i(H,\, A)$$

è un isomorfismo.

Dimostrazione. Per l'aggiunzione del funtore Ind_H^G con il funtore dimenticante $f^\times$ (1.2.2), troviamo un isomorfismo

$$\mathrm{Hom}_G(\mathbb{Z},\, \mathrm{Ind}_H^G(\,\bullet\,)) \to \mathrm{Hom}_H(f^\times\mathbb{Z},\, \bullet\,).$$

Ne segue che i rispettivi derivati saranno isomorfi, i quali, essendo Ind_H^G esatto e $f^\times\mathbb{Z} = \mathbb{Z}$ perché già munito dell'azione banale, sono i gruppi di coomologia della tesi. □

Di particolare interesse sono i moduli indotti direttamente da gruppi abeliani senza struttura, perché è particolarmente semplice calcolarne la coomologia.

□ **Definizione 1.6.2.** Chiamiamo *modulo indotto* uno G-modulo M che si possa scrivere nella forma $M = \mathrm{Ind}_1^G(A)$, per un opportuno gruppo abeliano A.

Per esempio, i moduli liberi sono indotti: un modulo libero $F = \bigoplus_n \mathbb{Z}[G]$ si scrive infatti come $F = (\bigoplus_n \mathbb{Z}\,) \otimes_{\mathbb{Z}} \mathbb{Z}[G]$, indotto per definizione. Segue immediatamente dal Lemma di Shapiro che

▼ **Corollario 1.6.3.** *Se A è un modulo indotto, allora $\mathrm{H}^i(G,\, A) = 0$ per ogni $i > 0$.*

Se la proposizione di aggiunzione (1.2.2) ammettesse una versione duale, troveremmo una variante del Lemma di Shapiro per gruppi di omologia e ne seguirebbe altrettanto immediatamente la banalità dei gruppi di omologia per i moduli indotti, da lì la banalità di tutti i gruppi di Tate: in effetti è così [Wei94, lemma 6.3.2].

▼ **Corollario 1.6.4.** *Se A è un modulo indotto, allora $\widehat{\mathrm{H}}^i(G,\, A) = 0$ per ogni i.*

Proprio per questo risultato i moduli indotti sono uno strumento comodissimo per il calcolo della coomologia di moduli qualunque; preso un modulo A, possiamo immergerlo nel suo indotto

$$\begin{aligned} A &\hookrightarrow \mathrm{Ind}_1^G(A) \\ a &\mapsto f_a \colon g \mapsto g \cdot a, \end{aligned}$$

oppure proiettarci sopra l'indotto

$$\begin{aligned} \mathrm{Ind}_1^G(A) &\twoheadrightarrow A \\ f &\mapsto \sum g \cdot f(g^{-1}x), \end{aligned}$$

in modo da avere sempre delle successioni esatte corte pronte per soddisfare un improvviso bisogno dimostrazioni per décalage. Possiamo infatti sfruttare la banalità degli indotti per costruire dei moduli con coomologia "traslata": scriviamo esplicitamente la successione indotta dall'inclusione

$$0 \to A \to \mathrm{Ind}_1^G \to A_1 \to 0;$$

questa produce una successione esatta lunghissima che contiene degli isomorfismi $\widehat{\mathrm{H}}^i(G,\, A_1) = \widehat{\mathrm{H}}^{i+1}(G,\, A)$. Analogamente possiamo fare esplicitando la successione associata alla proiezione:

$$0 \to A_{-1} \to \mathrm{Ind}_1^G(A) \to A \to 0.$$

La costruzione ammette un'ovvia generalizzazione

□ **Definizione 1.6.5.** Sia A uno G-modulo. Chiamiamo *moduli con coomologia traslata* $A_0 = A$, A_1 e A_{-1} definiti come sopra. Definiamo ricorsivamente

$$\begin{aligned} A_r &= (A_{r-1})_1 && \text{per } r > 1, \\ A_r &= (A_{r+1})_{-1} && \text{per } r < -1. \end{aligned}$$

In questi moduli ritroviamo la quintessenza di tutte le dimostrazione per décalage, vale infatti:

$$\widehat{\mathrm{H}}^i(G,\, A_r) = \widehat{\mathrm{H}}^{i+r}(G,\, A). \tag{1.3}$$

CAPITOLO 2

Esplorazione

In questo capitolo giocheremo con il nostro nuovo strumento, esplorandone le potenzialità e gettando delle solide basi sui cui poggeranno i calcoli successivi. Il primo obbiettivo sarà studiare la coomologia dei gruppi ciclici, che si rivelerà piuttosto semplice e di evidente importanza in tutto il seguito. Segue immediatamente un tentativo di studiare i gruppi per approssimazione: partendo da quelli ciclici, passando per i p-gruppi, per poi affrontare gruppi finiti qualsivoglia. Sarà dunque importante capire come ricondurre il calcolo operativo della coomologia di un gruppo a quello dei suoi Sylow. Nel farlo, produrremo un criterio per stabilire quando i gruppi di Tate di un modulo sono tutti banali.

Sistemati i giocattoli, sarà il momento di concentrarci sul vero obbiettivo del nostro lavoro: i gruppi di Galois. Per affrontare la Teoria di Galois avremo bisogno di abbandonare l'ipotesi di finitezza, producendo qualche risultato anche per gruppi profiniti. Introdurremo dunque la nozione di dimensione coomologica, come indice di complessità di un gruppo, di particolare interesse nella caratterizzazione dei gruppi infiniti.

2.1 Gruppi Ciclici

Sia nel seguito G un gruppo ciclico di ordine n di cui fissiamo un generatore σ. La coomologia di G è particolarmente semplice da descrivere: è sufficiente calcolare i gruppi di Tate in grado $i = 0, -1$.

■ **Teorema 2.1.1.** *Siano G un gruppo ciclico finito e A uno G-modulo. I gruppi di Tate sono 2-periodici nel grado:*

$$\widehat{\mathrm{H}}^{i+2}(G, A) = \widehat{\mathrm{H}}^{i}(G, A).$$

Dimostrazione. Siano $N = 1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1}$ e $D = 1 - \sigma$ due elementi di $\mathbb{Z}[G]$. Il teorema si basa interamente sullo scrivere la risoluzione proiettiva

$$\ldots \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{D} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{D} \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0,$$

da cui segue la 2-periodicità sia in coomologia che in omologia. Un elegante metodo per estendere la periodicità ai gradi $i = 0, -1$ si ottiene considerando i moduli con coomologia traslata: possiamo così spostare i gruppi problematici, per dire, in grado positivo. □

Per i moduli i cui gruppi di Tate sono finiti abbiamo scoperto due importanti invarianti: la cardinalità dei gruppi in grado pari e dei gruppi in grado dispari, che chiamiamo $h_0(A)$ e $h_1(A)$.

□ **Definizione 2.1.2.** (Quoziente di Herbrand) Se A ha gruppi di Tate finiti chiamiamo *quoziente di Herbrand* il numero naturale

$$h(A) := \frac{h_0(A)}{h_1(A)} = \frac{|\,\widehat{\mathrm{H}}^0(G,\,A)|}{|\,\widehat{\mathrm{H}}^1(G,\,A)|}.$$

Enunciamo ora alcune piacevoli proprietà.

Lemma 2.1.3. *Data una successione esatta corta*

$$0 \to A \to B \to C \to 0,$$

se il quoziente h è definito per due moduli su tre, è definito anche per il terzo. In questo caso vale $h(A)h(C) = h(B)$.

Dimostrazione. La successione esatta lunghissima associata può essere riassunta in una successione "esagonalmente esatta"

$$\begin{array}{ccccc} \widehat{\mathrm{H}}^0(G,\,A) & \to & \widehat{\mathrm{H}}^0(G,\,B) & & \\ \uparrow & \nearrow & & \searrow & \\ \widehat{\mathrm{H}}^1(G,\,C) & & & & \widehat{\mathrm{H}}^0(G,\,C) \\ \nwarrow & & & & \downarrow \\ & \widehat{\mathrm{H}}^1(G,\,B) & \leftarrow & \widehat{\mathrm{H}}^1(G,\,A), & \end{array}$$

che possiamo slacciare in un punto a piacere

$$0 \to Q \to \widehat{\mathrm{H}}^0(G,\,A) \to \widehat{\mathrm{H}}^0(G,\,B) \to \cdots \to \widehat{\mathrm{H}}^1(G,\,C) \to Q \to 0,$$

aggiungendo un opportuno modulo

$$Q = \ker\left[\widehat{\mathrm{H}}^0(G,\,A) \to \widehat{\mathrm{H}}^0(G,\,B)\right] = \mathrm{coker}\left[\widehat{\mathrm{H}}^1(G,\,B) \to \widehat{\mathrm{H}}^1(G,\,C)\right].$$

Dobbiamo pertanto avere, per esattezza, che

$$h_0(B)h_1(A)h_1(C) \cdot |\,Q\,| = h_0(A)h_0(C)h_1(B) \cdot |\,Q\,|,$$

da cui la tesi. □

Lemma 2.1.4. *Se A è finito, $h(A) = 1$.*

Dimostrazione. Nella definizione di gruppi di Tate compariva la successione esatta

$$0 \longrightarrow \widehat{\mathrm{H}}^{i^{-1}}(G,\, A) \longrightarrow A_G \xrightarrow{N} A^G \longrightarrow \widehat{\mathrm{H}}^{i^{0}}(G,\, A) \longrightarrow 0,$$

da cui deduciamo che $h_1(A) \cdot |\, A^G \,| = h_0(A) \cdot |\, A_G \,|$; siccome il gruppo è ciclico, abbiamo anche la desiderata relazione fra invarianti e co-invarianti:

$$0 \longrightarrow A_G \longrightarrow A \xrightarrow{D} A \longrightarrow A^G \longrightarrow 0.$$

Grazie alle cui relazioni sugli ordini dei gruppi concludiamo. □

2.2 Banalità Coomologica

Lo studio della coomologia di un generico gruppo si fa troppo complessa per poter sperare di enunciare teoremi di portata analoga a quelli validi per i gruppi ciclici. Si riesce però a dire qualcosa sui moduli che hanno tutti i gruppi di coomologia banali.

□ **Definizione 2.2.1.** Diciamo che uno G modulo A è *coomologicamente banale* se

$$\mathrm{H}^i(H,\, A) = 0 \qquad \forall\, i > 0, \quad \forall\, H < G.$$

Il lettore più accorto potrebbe trovarsi perplesso da questa scelta: perché, dopo i generosi risultati dei capitoli precedenti, abbiamo abbandonato i gruppi di Tate? Scopriremo nel seguito che le due definizioni sono equivalenti.

Abbiamo già mostrato che i moduli indotti sono coomologicamente banali (Lemma 1.6.4). In particolare i moduli liberi sono coomologicamente banali e, di conseguenza, i moduli proiettivi (ragionando per décalage). Anche i moduli iniettivi sono coomologicamente banali, per come abbiamo costruito i gruppi di coomologia (1.1).

In generale non è facile risalire dalla coomologia dei Sylow a quella del gruppo originario, una delle ragioni per cui siamo interessati ai moduli coomologicamente banali è che si riesce a spezzarne lo studio in parti più semplici. Per ogni primo p fissiamo un p-Sylow G_p di G e studiamone la coomologia; la scelta del p-Sylow non intacca la generalità dello studio, infatti il gruppo $\widehat{\mathrm{H}}^i(G_p,\, A)$ non dipende dalla scelta del Sylow: ogni automorfismo interno σ_t di G induce infatti un isomorfismo in coomologia.

Lemma 2.2.2. *Uno G-modulo A è coomologicamente banale se e solo se è coomologicamente banale come G_p-modulo per ogni p primo.*

Dimostrazione. Supponiamo che A sia G_p-coomologicamente banale per ogni p (l'altra implicazione è ovvia). Fissiamo un sottogruppo $H < G$. Vogliamo mostrare che $\mathrm{H}^i(H,\, A) = 0$ per ogni $i > 0$. Scelto un primo p, prendiamo un Sylow $H_p < H$ che possiamo supporre, senza perdita di generalità, incluso in G_p: per ipotesi $\mathrm{H}^i(H_p,\, A)$ è nullo. Sapendo ora che l'omomorfismo di restrizione è iniettivo sulla componente p-primaria (lemma 1.4.4),

$$0 \longrightarrow T_p\, \mathrm{H}^i(H,\, A) \xrightarrow{\texttt{res}} \mathrm{H}^i(H_p, A) = 0,$$

scopriamo che questa è nulla. Ricordando che i gruppi di coomologia sono di torsione (1.4.3), la tesi segue dall'arbitrarietà di p. □

Convinti ora che studiare la coomologia dei p-gruppi sia una strada promettente, cominciamo con un lemma tecnico.

Lemma 2.2.3. *Sia G un p-gruppo finito, ogni modulo A di torsione p-primario ha sottomodulo degli invarianti non banale. Detto altrimenti: se $A^G = 0$, allora $A = 0$.*

Dimostrazione. Per ogni elemento $a \in A$ consideriamo il sottomodulo finito M generato da a, questo viene partizionato dall'azione di G in orbite, che possiamo separare in banali e non per scrivere l'equazione delle classi:

$$| M | = | M^G | + \sum_{x \in R} \frac{| G |}{|Stab(x)|},$$

dove R è un opportuno sistema di rappresentanti. Concludiamo che, dividendo tutti gli altri addendi, p deve dividere anche $| M^G |$. □

Questo lemma ci tornerà particolarmente utile nella dimostrazione del risultato seguente: un criterio per stabilire la banalità dei moduli di p-torsione.

■ **Proposizione 2.2.4.** *Sia A uno G_p-modulo di p-torsione. Se esiste un indice q per cui $\widehat{\mathrm{H}}^q(G, A) = 0$, allora A è indotto.*

Dimostrazione. Dimostreremo che A è uno $\mathbb{F}_p[G]$-modulo libero; il che è equivalente alla tesi perché $\mathbb{F}_p[G] = \mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{F}_p$ è indotto.

Cominciamo osservando che A^G è un $\mathbb{F}_p$-modulo libero per ipotesi. Scelta una base di A^G, sia F il $\mathbb{F}_p[G]$-modulo libero generato sulla stessa base, per cui abbiamo un isomorfismo

$$j \colon A^G \to F^G.$$

Mostreremo che esiste un sollevamento di j a un isomorfismo tra F ed A. Consideriamo la successione esatta

$$0 \to A^G \to A \to A/A^G \to 0$$

e prendiamone gli $\mathrm{Hom}_{\mathbb{Z}}(\bullet, F)$

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(A/A^G, F) \to \mathrm{Hom}_{\mathbb{Z}}(A, F) \to \mathrm{Hom}_{\mathbb{Z}}(A^G, F). \tag{2.1}$$

Poiché F è indotto, anche $\mathrm{Hom}_{\mathbb{Z}}(A/A^G, F)$ è indotto! Nella successione esatta lunga associata troviamo dunque la suriezione

$$\mathrm{Hom}_G(A, F) \longrightarrow \mathrm{Hom}_G(A^G, F) \longrightarrow 0,$$

da cui segue l'esistenza di un sollevamento $J \colon A \to F$ di $j \colon A^G \to F^G$.

Non ci resta che mostrare che J è biettivo. L'iniettività è immediata: $\ker J$ è uno G-modulo di p-torsione senza invarianti, infatti

$$(\ker J)^G = \ker j = 0,$$

dunque è banale per l'appena dimostrato Lemma 2.2.3. Rimaniamo pertanto con la successione esatta

$$0 \longrightarrow A \xrightarrow{J} F \longrightarrow Q \longrightarrow 0,$$

la cui successione esatta lunga associata comincia con

$$0 \longrightarrow A^G \xrightarrow{j} F^G \longrightarrow Q^G \longrightarrow \mathrm{H}^1(G,\, A).$$

Se $q = 1$ ne deduciamo che, essendo j un isomorfismo, $Q^G \to 0$ è iniettiva, dunque $Q^G = 0$ e la tesi segue applicando nuovamente il Lemma 2.2.3. Se $q \neq 1$ abbiamo bisogno di ingegnarci altrimenti: dobbiamo traslare l'ipotesi. Il modulo con coomologia traslata A_{q-1} ricade nelle ipotesi del caso precedente ed è pertanto coomologicamente banale: ci forza così l'ipotesi

$$\widehat{\mathrm{H}}^1(G,\, A) = \widehat{\mathrm{H}}^{2\text{-}q}(G,\, A_{q-1}) = 0$$

di cui avevamo bisogno per concludere. □

Con un ulteriore piccolo sforzo è possibile rimuovere l'ipotesi di p-torsione, ottenendo un magnifico criterio per la banalità di un modulo. Per quanto osservato a inizio capitolo (2.2.2), continuiamo a enunciare i teoremi per p-gruppi, sottolineando però che per estenderli al caso generale è sufficiente richiedere le stesse ipotesi, ma su ogni primo.

■ **Teorema 2.2.5.** *Sia A uno G_p-modulo. Se esiste un indice q per cui*

$$\widehat{\mathrm{H}}^q(G_p,\, A) = \widehat{\mathrm{H}}^{q+1}(G_p,\, A) = 0,$$

allora A è coomologicamente banale.

Dimostrazione. Vogliamo mostrare che A è proiettivo. Esiste un modulo libero F per cui possiamo scrivere

$$0 \to R \to F \to A \to 0,$$

non ci resta che trovare una sezione. Passando alla successione esatta lunghissima, poiché F è coomologicamente banale, riusciamo a spostare l'ipotesi su R:

$$\widehat{\mathrm{H}}^{q+1}(G_p,\, R) = \widehat{\mathrm{H}}^{q+2}(G_p,\, R) = 0.$$

Possiamo pertanto supporre senza perdita di generalità che A sia libero come gruppo abeliano: il nucleo R lo è comunque e se fosse coomologicamente banale lascerebbe A da solo ad affogare in un mare di zeri. In questo caso $\mathrm{Hom}_{\mathbb{Z}}(A,\, \bullet)$ è esatto e ci restituisce quindi una successione esatta corta

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(A,\, R) \to \mathrm{Hom}_{\mathbb{Z}}(A,\, F) \to \mathrm{Hom}_{\mathbb{Z}}(A,\, A) \to 0. \tag{2.2}$$

Mostriamo che sotto queste ipotesi, il primo termine ha primo gruppo di coomologia banale.

Lemma 2.2.6. *Detto $M = \mathrm{Hom}_{\mathbb{Z}}(A, R)$, troviamo $\mathrm{H}^1(G,\, M) = 0$.*

Dimostrazione. Consideriamo la successione esatta

$$0 \longrightarrow R \xrightarrow{\cdot p} R \longrightarrow R/pR \longrightarrow 0,$$

e la successione esatta lunghissima associata; il conucleo R/pR è uno G_p-modulo di p-torsione per cui $\widehat{\mathrm{H}}^{q+1}(G_p, R/pR) = 0$ e pertanto, rileggendo la proposizione precedente (2.2.4), scopriamo che è indotto. Applicando $\mathrm{Hom}_{\mathbb{Z}}(A,\, \bullet)$ alla successione esatta otteniamo

$$0 \longrightarrow M \xrightarrow{\cdot p} M \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(A,\, R/pR) \longrightarrow 0,$$

nella cui successione esatta lunga, poiché $\mathrm{Hom}_{\mathbb{Z}}(A,\, R/pR)$ è a sua volta indotto, troviamo

$$\mathrm{H}^1(G_p,\, M) \xrightarrow{\cdot p} \mathrm{H}^1(G_p,\, M) \longrightarrow 0.$$

Se la moltiplicazione per p è suriettiva, il gruppo abeliano $\mathrm{H}^1(G_p,\, M)$ non può avere p-torsione, ne tanto meno componente p-primaria. Sapendo però che dev'essere un gruppo di $|G_p|$-torsione (per 1.4.3), siamo costretti a concludere che è nullo. □

Prendendo la successione esatta lunga associata alla (2.2) scopriamo che

$$\mathrm{Hom}_G(A,\, F) \longrightarrow \mathrm{Hom}_G(A,\, A) \longrightarrow 0,$$

ovvero che esiste una sezione dell'identità id_A. □

Segue immediatamente che:

▼ **Corollario 2.2.7.** *Se A è coomologicamente banale, tutti gli $\widehat{\mathrm{H}}^i(G,\, A)$ sono banali.*

Concludiamo il capitolo con un risultato la cui utilità sarà chiara solo fra qualche capitolo.

▼ **Corollario 2.2.8.** *Sia A un modulo coomologicamente banale e D un modulo piatto. L'estensione per scalari $A \otimes D$ è coomologicamente banale.*

Dimostrazione. La dimostrazione del teorema precedente mostra che se A è coomologicamente banale, allora esistono F libero e P proiettivo per cui la successione

$$0 \to P \to F \to A \to 0$$

è esatta. Per piattezza anche la successione

$$0 \to P \otimes D \to F \otimes D \to A \otimes D \to 0$$

è esatta. Poiché $F \otimes D$ rimane indotto e $P \otimes D$ rimane addendo diretto di un indotto, nella successione esatta lunghissima associata troviamo i gruppi di coomologia con coefficienti in $A \otimes D$ immersi in un mare di zeri; concludiamo che $A \otimes D$ dev'essere coomologicamente banale. □

2.3 Dimensione Coomologica

La dimensione coomologica di un gruppo è un indice di complessità: è il numero di gruppi di coomologia non nulli che ci aspettiamo di trovare, più o meno indipendentemente dal modulo dal quale peschiamo i coefficienti. Questo tipo di studio risulta interessante per lo più per gruppi infiniti; è giunto il momento di abbandonare l'ipotesi di finitezza.

□ **Definizione 2.3.1** (Dimensione coomologica)**.** Sia G un gruppo profinito e p un numero primo. La *p-dimensione coomologica* di G è il più piccolo intero n per cui: per ogni G-modulo A di torsione, la componente p-primaria di $\mathrm{H}^q(G,\, A)$ è nulla non appena $q > n$, volendo

$$\mathrm{cd}_p(G) := \inf\{n \in \mathbb{N} \mid T_p\, \mathrm{H}^q(G,\, A) = 0 \quad \forall\, q > n, \quad \forall A \text{ di torsione}\}.$$

La *dimensione coomologica* è definita di conseguenza come $\mathrm{cd}(G) := \sup_p \mathrm{cd}_p(G)$.

È necessaria una certa attenzione nel maneggiare la definizione di dimensione coomologica: abbiamo richiesto che A fosse un modulo *di torsione*, rimuovendo questa ipotesi si finisce a parlare di dimensione coomologica stretta, che è tutta un'altra storia (anzi, ancora peggio, una storia leggermente diversa).

Siamo in grado di formulare un criterio per il calcolo della dimensione coomologica, riducendo i moduli su cui dobbiamo calcolare la coomologia a solamente quelli semplici.

■ **Proposizione 2.3.2.** *Sia G_p un p-gruppo profinito. La dimensione $\mathrm{cd}_p(G_p) \leq n$ se e solo se $\mathrm{H}^{n+1}(G_p, \mathbb{Z}/p\mathbb{Z}) = 0$.*

Dimostrazione. Il risultato è vagamente intuitivo e la dimostrazione sarà modellata attorno a questa sensazione: la componente di p-torsione si può calcolare senza perdita di generalità sui moduli p-primari, che a loro volta potremo spezzare in sottomoduli semplici, riducendo il calcolo all'unico modulo semplice di p-torsione che esiste, $\mathbb{Z}/p\mathbb{Z}$. Procediamo con ordine.

Mostriamo che l'unico G-modulo semplice di p-torsione è $\mathbb{Z}/p\mathbb{Z}$ (con l'azione banale!). Un modulo di questo tipo dev'essere, ovviamente, finito; nell'intersezione degli stablizzatori dei vari elementi, che ricordiamo essere aperti, troviamo un sottogruppo $U < G$ aperto e normale per cui A è un G/U-modulo semplice, riportandoci a dimostrare il risultato per un gruppo finito, per cui la tesi è chiara (grazie al lemma 2.2.3).

Se $\mathrm{H}^{n+1}(G_p, \mathbb{Z}/p\mathbb{Z})$ è nullo, allora $\mathrm{H}^{n+1}(G_p, A)$ è nullo per ogni modulo A finito di p-torsione: In questo caso possiamo infatti scrivere una serie di composizione

$$0 = A^m \hookrightarrow A^{m-1} \hookrightarrow \cdots \hookrightarrow A^1 \hookrightarrow A^0 = A,$$

i cui quozienti sono tutti semplici, ovvero, per quanto appena mostrato, si trovano in successioni esatte corte della forma

$$0 \to A^{i+1} \to A^i \to \mathbb{Z}/p\mathbb{Z} \to 0.$$

La collezione di successioni esatte lunghe associate restituisce una catena di mappe suriettive in grado $n+1$ per ipotesi,

$$0 = \mathrm{H}^{n+1}(G,\, A^0) \twoheadrightarrow \mathrm{H}^{n+1}(G,\, A^1) \twoheadrightarrow \cdots \twoheadrightarrow \mathrm{H}^{n+1}(G,\, A),$$

da cui segue la banalità di tutti i gruppi coinvolti. Rimuoviamo facilmente l'ipotesi di finitezza, sfruttando il solito risultato di passaggio al limite 1.2.7, una volta scritto A come unione (o, per farla difficile, limite induttivo) dei suoi sottomoduli finiti.

Per concludere, dimostriamo per décalage che i gruppi di coomologia in grado maggiore di $n+1$ sono anch'essi nulli, per ogni modulo A di p-torsione. È sufficiente scrivere il modulo di coomologia traslata A_r e osservare che, nonostante G non sia finito, continua ad avere coomologia traslata per $r \geq 0$ perché l'indotto $\mathrm{Ind}_1^G(A)$ è anch'esso di p-torsione, essendo composto da mappe che, per essere continue, devono essere localmente costanti e pertanto con immagine finita. Concludiamo dunque che

$$\widehat{\mathrm{H}}^{n+1+r}(G,\, A) = \widehat{\mathrm{H}}^{n+1}(G,\, A_r) = 0 \qquad \forall\, r > 0. \qquad \square$$

Calcoliamo la dimensione coomologica del gruppo additivo degli interi p-adici $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$. Per il solito teorema di passaggio al limite (1.2.7), si ha che

$$\mathrm{H}^2(\mathbb{Z}_p, \mathbb{Z}/p\mathbb{Z}) = \varinjlim_n \mathrm{H}^2(\mathbb{Z}/p^n\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) = \varinjlim_n \widehat{\mathrm{H}}^0(\mathbb{Z}/p^n\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}).$$

I gruppi di Tate di grado zero li conosciamo esplicitamente: per definizione sono $\mathbb{Z}/p\mathbb{Z}$ quozientato per l'immagine della norma che, trovando l'azione banale, coincide con la moltiplicazione per l'ordine del gruppo p^n e quindi è la mappa nulla. Le mappe di collegamento sono indotte dalla proiezione naturale e coincidono quindi con l'inflazione, che in grado zero è per definizione la norma. Poiché tutte le mappe sono nulle

$$\mathrm{H}^2(\mathbb{Z}_p, \mathbb{Z}/p\mathbb{Z}) = \varinjlim \mathbb{Z}/p\mathbb{Z} = 0.$$

Per la proposizione appena dimostrata $\mathrm{cd}_p(\mathbb{Z}_p) \leq 1$; otteniamo l'altra uguaglianza calcolando esplicitamente

$$\mathrm{H}^1(\mathbb{Z}_p, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}(\mathbb{Z}_p, \mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z} \neq 0.$$

Dunque $\mathrm{cd}_p(\mathbb{Z}_p) = 1$. Riprendiamo lo studio della dimensione coomologica, mostrando in che modo la dimensione di un gruppo è legata a quella dei suoi sottogruppi.

■ **Proposizione 2.3.3.** *Sia G un gruppo profinito e H un suo sottogruppo chiuso. Per ogni primo p si ha*

$$\mathrm{cd}_p(H) \leq \mathrm{cd}_p(G).$$

Se per di più l'indice $[G : H]$ è coprimo con p, si ha uguaglianza.

Dimostrazione. Se A è un H-modulo p-primario, allora anche $\mathrm{Ind}_H^G(A)$ è p-primario. Per il Lemma di Shapiro si ha che per ogni indice i

$$\mathrm{H}^i(H, A) = \mathrm{H}^i(G, \mathrm{Ind}_H^G(A)),$$

da cui la tesi. Se l'indice $[G : H]$ è coprimo con p, per ogni modulo la restrizione fornisce una mappa nella direzione opposta

$$0 \longrightarrow T_p\,\mathrm{H}^i(G, A) \xrightarrow{\texttt{res}} \mathrm{H}^i(H, A),$$

iniettiva per il lemma 1.4.4. □

Quest'ultima proposizione ci permette di ricondurre il calcolo della dimensione di un gruppo a quella dei suoi Sylow. L'esempio per eccellenza è $\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$, dei cui Sylow $\mathbb{Z}_p$ conosciamo già la dimensione: per ogni primo p si ha

$$\mathrm{cd}_p(\hat{\mathbb{Z}}) = \mathrm{cd}_p(\mathbb{Z}_p) = 1,$$

da cui $\mathrm{cd}(\hat{\mathbb{Z}}) = 1$.

Non possiamo sperare in un risultato analogo al precedente per i quozienti: per esempio $\mathbb{Z}_p$ ha dimensione coomologica finita, mentre i suoi quozienti finiti essendo ciclici hanno gruppi non nulli di indice arbitrariamente grande. Troviamo comunque una disuguaglianza della direzione opposta.

■ **Proposizione 2.3.4.** *Sia H un sottogruppo chiuso e normale di G. Allora, per ogni numero primo p, si ha che*

$$\mathrm{cd}_p(G) \leq \mathrm{cd}_p(H) + \mathrm{cd}_p(G/H).$$

Dimostrazione. Segue dall'esistenza successione spettrale di Hochschild-Serre: per ogni modulo di A di torsione, la successione ci fornisce una filtrazione di $\mathrm{H}^n(G, A)$ i cui quozienti sono, partendo dalla descrizione della seconda pagina, sottoquozienti di $\mathrm{H}^i(G/H, \mathrm{H}^j(H, A))$ per $i + j = n$. Osserviamo che $\mathrm{H}^j(H, A)$ sarà nullo non appena $j > \mathrm{cd}_p(H)$ e che, essendo $\mathrm{H}^j(H, A)$ di torsione a sua volta (1.4.3), anche $\mathrm{H}^i(G/H, \mathrm{H}^j(H, A))$ sarà nullo non appena $i > \mathrm{cd}_p(G/H)$; da cui la disuguaglianza voluta. □

CAPITOLO 3

Campi Locali

In questo capitolo faremo fruttare quanto preparato in precedenza: cominceremo a parlare di estensioni di campi e a studiare la coomologia dei relativi gruppi di Galois. Inizieremo con qualche risultato di carattere generale riguardo le estensioni di Galois, dalle nozioni di base alla teoria di Kummer, per restringere poi la nostra attenzione ai campi locali.

Per campo locale intendiamo un campo completo rispetto a una valutazione discreta di rango 1. Si può pensare, senza perdita di generalità, a estensioni finite dei p-adici $\mathbb{Q}_p$ o delle serie Laurent su campi finiti $\mathbb{F}_p((t))$. Studiamo questi campi per almeno due buone ragioni; in primis, perché presentano una struttura relativamente semplice: i relativi anelli degli interi sono locali (da cui il nome) e le unità sono di facile descrizione; in secondo luogo, perché sono un ottimo punto di partenza per dedurre risultati analoghi anche nel caso globale, trattazione che però esula dagli scopi di questa tesi.

Il capitolo sarà dunque rivolto a calcolare la coomologia dei moduli intrinsecamente associati a un'estensione di Galois di un campo locale, come il gruppo additivo e moltiplicativo del campo soprastante: mostreremo che in grado uno è sempre nulla, la calcoleremo il grado due e mostreremo che dal grado tre in poi torna a essere nulla.

3.1 Teoria di Galois

Sia k un campo. Fissiamo una chiusura separabile $\bar{k}$. D'ora in avanti denoteremo, per brevità, con Γ_k il gruppo di Galois assoluto $\mathcal{G}al\left(\bar{k}/k\right)$, sostituendolo talvolta con k stesso: in questo senso parleremo impropriamente di coomologia di k, per esempio scrivendo

$$\mathrm{H}^i(k,\, A) := \mathrm{H}^i(\Gamma_k,\, A).$$

Osserviamo che, presa una diversa chiusura separabile $\bar{k}'$ e un sollevamento di id_k a un isomorfismo $f\colon \bar{k} \to \bar{k}'$, questo induce un isomorfismo in coomologia

$$f^*\colon \mathrm{H}^i(\mathcal{G}al\left(\bar{K}/K\right),\, A) \to \mathrm{H}^i(\mathcal{G}al\left(\bar{K}'/K\right),\, A)$$

che non dipende dalla scelta di f: possiamo cambiare l'immersione f solo agendo in partenza o in arrivo con un elemento del rispettivo gruppo di Galois, il che equivale a permutare il gruppo stesso per coniugio, isomorfismo che, per la proposizione 1.2.6, è l'identità in coomologia. Scelte comunque due chiusure separabili, i relativi gruppi di coomologia sono canonicamente isomorfi. Possiamo quindi parlare senza remore della "coomologia di k", della sua dimensione coomologica e dei suoi gruppi di coomologia.

Fissiamo un'estensione di Galois L/k e cominciamo ad analizzare la coomologia del modulo più naturale del relativo gruppo $\mathcal{G}al\,(L/k)$: il campo L. Il gruppo di Galois è composto dagli automorfismi del campo, per definizione, quindi è ben definita un'azione tanto sul gruppo additivo L, quanto sul gruppo moltiplicativo $L^\times$.

■ **Teorema 3.1.1.** *Sia L/k un'estensione di Galois. Il gruppo additivo di L è coomologicamente banale.*

Dimostrazione. Nel caso di estensioni finite, la tesi segue dal Teorema della Base Normale: questo afferma che L è un $k[G]$ modulo libero. Per estensioni infinite è sufficiente passare al limite sulle sottoestensioni finite (tramite la solita proposizione 1.2.7). □

Non potevamo chiedere niente di meglio. La coomologia del gruppo moltiplicativo non è altrettanto semplice: lo studio di quest'ultima è il cuore della Teoria. La banalità del primo di gruppo di coomologia è già parecchio interessante, si tratta infatti di una riscrittura del Teorema di Indipendenza dei Caratteri di Artin nel nostro linguaggio:

■ **Teorema 3.1.2** (Hilbert 90)**.** *Sia L/k un'estensione di Galois. Si ha*

$$\mathrm{H}^1(\mathcal{G}al\,(L/k)\,,\,L^\times) = 0.$$

Dimostrazione. Assumiamo, per il momento, che L/k sia finita. Mostreremo che tutti i cocicli sono cobordi: prendiamo un cociclo $a\colon G \to L^\times$. Gli elementi di G sono linearmente indipendenti su L, quindi troviamo $x \in L^\times$ per cui

$$y = \sum_{g\in G} a_g\, g(x) \neq 0.$$

Ma, traslando questo elemento di h e ricordando che $a_{hg} = a_h\, ha_g$ per definizione, otteniamo

$$hy = \sum_{g\in G} ha_g\, hg(x) = a_h^{-1} \sum_{hg\in G} a_{hg}\, hg(x) = a_h^{-1} y$$

per ogni $h \in G$, da cui la tesi $a_h = (h-1)y^{-1}$. Ancora una volta, passando al limite (con 1.2.7) otteniamo la tesi anche per le estensioni infinite. □

Il grado $i = 2$ si fa ancora più interessante, tanto da meritarsi un nome proprio.

□ **Definizione 3.1.3** (Gruppo di Brauer)**.** Il gruppo di Brauer di k è

$$\mathrm{Br}\, k = \mathrm{H}^2(k,\, \bar{k}^\times).$$

Il gruppo di Brauer compare in diverse aree della matematica ed è di particolare importanza in algebra non commutativa, dove si scopre classificare le algebra centrali semplici sul campo in oggetto. Non entreremo nel dettaglio di questa corrispondenza, invitando però il lettore esperto a interpretare i risultati dei capitoli seguenti anche in quest'ottica: se ne ricava una buona intuizione dei risultati.

Nel seguito sarà comodo avere della notazione per indicare $\mathrm{H}^2(\mathcal{G}al\,(L/k)\,,\,L^\times)$, che possiamo pensare come il gruppo di Brauer "relativo" all'estensione L/k: lo chiameremo $\mathrm{Br}(L/k)$.

Lemma 3.1.4. *Per ogni estensione L/k finita di Galois, troviamo una successione esatta*

$$0 \to \mathrm{Br}(L/k) \to \mathrm{Br}\,k \to \mathrm{Br}\,L.$$

Dimostrazione. Possiamo riscrivere la tesi come

$$0 \to \mathrm{H}^2(\mathcal{G}al\,(L/k)\,,\,L^\times) \to \mathrm{H}^2(\mathcal{G}al\,\left(\bar{k},\,k\right),\,\bar{k}^\times) \to \mathrm{H}^2(\mathcal{G}al\,\left(\bar{k},\,L\right),\,\bar{k}^\times),$$

che è proprio una delle successioni di termini di grado basso della successione spettrale di Hochschild-Serre(corollario 1.3.3). □

Grazie a questo risultato, ci è concesso pensare al gruppo di Brauer di un campo come l'unione dei gruppi $\mathrm{H}^2(G,\,L^\times)$, che siamo interessati a calcolare, su tutte le estensioni di Galois finite. Enunciamo ora un'osservazione molto comoda per maneggiare il gruppo di Brauer di un campo, che quindi useremo spesso in futuro.

■ **Proposizione 3.1.5.** *Il sottogruppo di n-torsione* $(\mathrm{Br}\,k)[\,n\,]$ *coincide con* $\mathrm{H}^2(k,\mu_n)$.

Dimostrazione. La successione esatta lunga associata a

$$0 \longrightarrow \mu_n \longrightarrow \bar{k}^\times \xrightarrow{\cdot n} \bar{k}^\times \longrightarrow 0,$$

grazie a Hilbert 90, contiene il segmento

$$0 \longrightarrow \mathrm{H}^2(G,\,\mu_n) \longrightarrow \mathrm{H}^2(G,\,\bar{K}^\times) \xrightarrow{\cdot n} \mathrm{H}^2(G,\,\bar{K}^\times). \qquad \square$$

Verso il profinito e oltre. È incredibilmente rassicurante osservare che, nonostante sia indispensabile aver definito la coomologia per gruppi profiniti, tutto si riconduca senza problemi alla coomologia di gruppi finiti. Tiriamo un sospiro di sollievo e procediamo con serenità.

3.2 Teoria di Kummer

Questa sezione è dedicata a mostrare l'efficacia del linguaggio coomologico sviluppato fin'ora nel trattare alcuni problemi classici in teoria dei campi. Sia $\Gamma_k = \mathcal{G}al\,\left(\bar{k}/k\right)$ il gruppo di Galois assoluto di k. Fissiamo un gruppo abeliano A, finito e munito della topologia discreta; scegliendo un omomorfismo continuo

$$\varphi\colon \Gamma_k \to A,$$

produciamo come nucleo un sottogruppo chiuso e normale. Per il teorema di corrispondenza di Galois, vi è associata un'estensione L di gruppo

$$\mathcal{G}al\,(L/k) = \frac{\mathcal{G}al\,(\bar{k}/k)}{\ker\varphi} \hookrightarrow A.$$

Al fine di classificare le estensioni di gruppo di Galois A abeliano è pertanto sufficiente trovare tutti gli omomorfismi $\mathrm{Hom}_{\mathsf{Gr}}(\Gamma_k,\, A)$, in realtà a meno della relazione che identifica due omomorfismi con lo stesso nucleo. Poiché G non agisce su A, siamo in grado di trasportare il problema nel linguaggio della coomologia: siamo interessati a calcolare $\mathrm{H}^1(\Gamma_k,\, A) = \mathrm{Hom}_{\mathsf{Gr}}(\Gamma_k,\, A)$. Possiamo quindi sfoggiare il nostro arsenale per produrre un piacevole risultato.

■ **Teorema 3.2.1** (di Kummer)**.** *Sia K un campo e p un numero primo. Supponiamo che K contenga le radici p-esime dell'unità μ_p. In questo caso, c'è una corrispondenza tra le estensioni cicliche di gruppo $\mathbb{Z}/p\mathbb{Z}$ (o banale) di K e $K^\times/K^{\times p}$.*

Dimostrazione. Calcoleremo $\mathrm{H}^1(\Gamma_k,\, \mathbb{Z}/p\mathbb{Z})$. Prendere la p-esima potenza $x \mapsto x^p$ è un'operazione suriettiva nella chiusura algebrica, da cui l'esattezza di

$$0 \longrightarrow \mu_p \longrightarrow \bar{K}^\times \xrightarrow{\cdot p} \bar{K}^\times \longrightarrow 0.$$

La successione esatta lunga associata comincia, applicando Hilbert 90, con

$$0 \longrightarrow \mu_p \longrightarrow K^\times \xrightarrow{\cdot p} K^\times \longrightarrow \mathrm{H}^1(\Gamma_k,\, \mu_p) \longrightarrow 0;$$

che è proprio quello che cercavamo: poiché le radici p-esime dell'unità vivono in k per ipotesi, Γ_k vi agisce banalmente e pertanto

$$\mathrm{H}^1(\Gamma_k,\, \mathbb{Z}/p\mathbb{Z}) = \mathrm{H}^1(\Gamma_k,\, \mu_p) = K^\times/K^{\times p}. \qquad \square$$

Il Teorema di Kummer si colloca appena all'inizio di una teoria più ampia, piuttosto che esserne il culmine. La dimostrazione mostra la potenza e la comodità del linguaggio coomologico per affrontate lo studio delle estensioni di campi: in poche righe siamo riusciti a smontare un teorema per nulla banale, avendo costruito in precedenza tutta la rete di mappe e isomorfismi che questa dimostrazione avrebbe altrimenti richiesto di esplicitare. A titolo informativo presentiamo il seguente risultato, che permette sia di chiarire quanto esplicita si possa rendere la corrispondenza di Kummer sia, al contempo, di mostrare il tipo di risultati che si può sperare di ottenere procedendo in questa direzione.

■ **Proposizione 3.2.2.** *Sia $K/\mathbb{Q}$ un'estensione ciclica di grado 3. Allora K è il campo di spezzamento di un polinomio della forma*

$$x^3 - 3x - \frac{(2(a^2 - 3b^2))}{(a^2 + 3b^2)}$$

per certi a, b razionali. Viceversa, ogni tale polinomio o è riducibile o ha gruppo di Galois ciclico.

È possibile utilizzare questo arsenale anche in modo più ricreativo.

■ **Teorema 3.2.3.** *Le terne pitagoriche primitive sono della forma* $(a^2 - b^2,\, 2ab,\, a^2 + b^2)$.

Dimostrazione. Le terne pitagoriche primitive sono in bigezione con i punti di $\mathbb{Q}(i)$ sulla circonferenza unitaria, ovvero di norma 1. Per la definizione del gruppo di Tate di grado $i = -1$, la ciclicità di $G = \mathcal{G}al\,(\mathbb{Q}(i)/\mathbb{Q})$ e Hilbert 90, abbiamo che

$$(\ker N)\,/I_G\mathbb{Q}(i)^\times = \widehat{\mathrm{H}}^{-1}(G,\, \mathbb{Q}(i)^\times) = \mathrm{H}^1(G,\, \mathbb{Q}(i)^\times) = 0,$$

ovvero $\ker N = I_G\mathbb{Q}(i)^\times$: ogni elemento di norma unitaria si scrive nella forma

$$(1-g)(a+ib) = \frac{a+ib}{a-ib} = \frac{a^2-b^2}{a^2+b^2} + i\,\frac{2ab}{a^2+b^2}. \qquad \square$$

3.3 Struttura di un Campo Locale

Ricordiamo brevemente tutto quello che è necessario sapere sui campi locali per poter procedere. Chiamato K il nostro campo locale, possiamo definire l'anello degli interi su K come gli elementi di valutazione non negativa

$$\mathcal{O}_K = \{x \in K \mid v(x) \geq 0\}.$$

Questo è naturalmente un anello a valutazione discreta, pertanto locale: chiamiamo π un generatore dell'ideale primo e $\kappa = \mathcal{O}_K/(\pi)$ il campo residuo. Le unità di quest'anello sono il nucleo dell'omomorfismo di valutazione

$$1 \longrightarrow \mathcal{O}_K^\times \longrightarrow K^\times \xrightarrow{v} \mathbb{Z} \longrightarrow 0. \tag{3.1}$$

La valutazione fornisce una piacevole filtrazione delle unità principali, ovvero quelle nella forma $x = u\pi^k + 1$, permettendoci per esempio di distinguerle in classi

$$U_K^i := \{x \in \mathcal{O}_K^\times \mid v(x-1) \geq i\}.$$

Si può mostrare che l'omomorfismo $U_K^i \to \kappa$ che manda $x \mapsto (x-1)/p^n$ è suriettivo e genera della successioni esatte corte

$$1 \longrightarrow U_K^{i+1} \longrightarrow U_K^i \longrightarrow \kappa \longrightarrow 0. \tag{3.2}$$

Abbiamo così ottenuto una filtrazione $\mathcal{O}_K^\times \supseteq U_K^1 \supseteq U_K^2 \supseteq \ldots$ i cui quozienti U_K^i/U_K^{i+1} sono tutti isomorfi a κ. Infine troviamo, a collegare la prima successione (3.1) con quelle sottostanti,

$$1 \longrightarrow U_K^1 \longrightarrow \mathcal{O}_K^\times \longrightarrow \kappa^\times \longrightarrow 1, \tag{3.3}$$

che, per il Lemma di Hensel, spezza.

Procediamo ora nell'enunciare qualche risultato che, sfruttando la relativa semplicità di questa struttura, ci fornisce qualche informazione aggiuntiva sulla coomologia delle estensioni di questi campi locali. Cominciamo dalle estensioni più facili da controllare: quelle non ramificate.

■ **Teorema 3.3.1.** *Sia L/K un'estensione di Galois, finita e non ramificata, di gruppo G. I gruppi $\mathcal{O}_K^\times$ e U_L^1 sono coomologicamente banali.*

Dimostrazione. Sia λ il campo residuo di L. Aver assunto l'estensione non ramificata ci concede la comodità di poter identificare $G = \mathcal{G}al\,(L/K) = \mathcal{G}al\,(\lambda/\kappa)$. Poiché il gruppo additivo di λ è coomologicamente banale (teorema 3.1.1), dalla successione esatta

$$1 \longrightarrow U_L^{i+1} \longrightarrow U_L^i \longrightarrow \lambda \longrightarrow 0$$

la stessa proprietà segue per tutti gli U_L^i/U_L^{i+1}. Poiché la coomologia di un gruppo finito commuta con il limite proiettivo nel secondo argomento se tutti i moduli in questione sono finiti [Har13, proposizione 1.12], segue per induzione che U_L^1/U_L^i, e passando al limite anche tutto $U_L^1 = \varprojlim U_L^1/U_L^i$, è coomologicamente banale.

Per estendere la proprietà a tutto $\mathcal{O}_L^\times$ riscriviamo la successione esatta (3.3)

$$1 \longrightarrow U_L^1 \longrightarrow \mathcal{O}_L^\times \longrightarrow \lambda^\times \longrightarrow 1$$

e osserviamo che non solo U_L^1 è coomologicamente banale, ma anche $\lambda^\times$: infatti il gruppo G è ciclico e in grado $i = 1$ è banale per Hilbert 90, in grado $i = 2$ è banale perché $\mathrm{Br}\,\lambda$ è nullo, perché $\hat{\mathbb{Z}}$ ha dimensione coomologica 1. La tesi segue prendendo la successione esatta lunga associata. □

Per estensioni ramificate la situazione non è così semplice, anche rimanendo interessati alle sole estensioni cicliche; tant'è che abbiamo bisogno di premettere un lemma tecnico alla generalizzazione del risultato appena ottenuto.

Lemma 3.3.2 (del sottomodulo banale)**.** *Sia L/K un'estensione finita di Galois di gruppo G. Esiste un sottomodulo $V \subseteq U_L^1$ d'indice finito e coomologicamente banale.*

Dimostrazione. Per il teorema della Base Normale esiste un elemento $\alpha \in L$ per cui $\{g\alpha \mid g \in G\}$ sia una base di L come spazio vettoriale su K. Poiché l'estensione è finita, troviamo un elemento $a \in K^\times$ di valutazione abbastanza grande da far cadere tutti i $a(g\alpha)$ negli interi $\mathcal{O}_L$: chiamiamo M l'$\mathcal{O}_K$-sottomodulo di $\mathcal{O}_L$ generato da questi elementi; M è isomorfo a $\mathcal{O}_K[G]$ per costruzione. Per di più, M è un sottogruppo aperto di $\mathcal{O}_L$ (che, equipaggiato con la topologia indotta da L, è un gruppo additivo profinito): dette p_i le proiezioni sulle coordinate, otteniamo infatti M come intersezione di aperti della forma $\{x \in \mathcal{O}_L \mid v_K p_i(x) \geq m_i\}$, per opportuni interi m_i. Ne segue che M è un sottogruppo di indice finito e dunque che esiste un intero m per cui

$$\pi^m \mathcal{O}_L \subseteq M \subseteq \mathcal{O}_L.$$

Traslando opportunamente M, costruiamo una serie di sottomoduli di U_L^1

$$V_i = 1 + \pi^{m+i} M,$$

con la piacevole proprietà di filtrare V_1, presentando quozienti coomologicamente banali: abbiamo infatti un isomorfismo $V_i/V_{i+1} \to M/\pi M$ dato da

$$v_i \mapsto \pi^{-m-i}(v_i - 1) \ + \pi M,$$

che possiamo riassumere in diverse successioni esatte corte

$$0 \to V_{i+1} \to V_i \to \kappa[G] \to 0;$$

da cui deduciamo, analogamente a quanto fatto nella proposizione precedente, che il sottomodulo $V = V_1$, di indice finito in U_L^1 per costruzione, è anch'esso coomologicamente banale ed è quindi il modulo desiderato. □

■ **Teorema 3.3.3** (Assioma del Campo di Classe)**.** *Sia L/K un'estensione di Galois, finita e di gruppo $G = \mathcal{G}al\,(L/K)$ ciclico. Allora $\mathrm{H}^1(G,\, L^\times) = 0$ e $\widehat{\mathrm{H}}^0(G,\, L^\times)$ ha cardinalità $[L : K]$.*

Dimostrazione. La prima asserzione segue da Hilbert 90. Applichiamo il lemma del sottomodulo banale e scriviamo la successione esatta

$$1 \to V \to \mathcal{O}_L^\times \to \mathcal{O}_L^\times/V \to 1;$$

il primo modulo è coomologicamente banale per costruzione, pertanto il suo quoziente di Herbrand è $h(V) = 1$, e anche l'ultimo modulo ha $h = 1$: infatti è finito, perché

$$[\mathcal{O}_L^\times : V] = [\mathcal{O}_L^\times : U_L^1] \cdot [U_L^1 : V],$$

dove il secondo indice è finito per costruzione e il primo perché il quoziente di quei due gruppi è $\lambda^\times$ (si guardi la successione esatta (3.3)). Segue dalle proprietà del quoziente di Herbrand (prima 2.1.4 e poi 2.1.3) che $h(\mathcal{O}_L^\times) = 1$. Passiamo ora alla successione esatta (3.1)

$$1 \longrightarrow \mathcal{O}_L^\times \longrightarrow L^\times \xrightarrow{v} \mathbb{Z} \longrightarrow 0,$$

della quale conosciamo il quoziente di Herbrand del primo e dell'ultimo gruppo: sappiamo infatti che

$$\mathrm{H}^1(G,\, \mathbb{Z}) = \mathrm{Hom}_{\mathsf{Gr}}(G,\, \mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}(G^{\mathsf{ab}},\, \mathbb{Z}) = 0$$

perché G è finito e agisce banalmente su $\mathbb{Z}$ e che

$$\widehat{\mathrm{H}}^0(G,\, \mathbb{Z}) = \frac{\mathbb{Z}^G}{N\mathbb{Z}} = \frac{\mathbb{Z}}{|G|\,\mathbb{Z}}$$

per definizione. Infine, per le proprietà del quoziente di Herbrand e Hilbert 90

$$h(L^\times) = h(\mathbb{Z}) \qquad \Longrightarrow \qquad |\,\widehat{\mathrm{H}}^0(K, L^\times)\,| = |G| = [L : K]. \qquad \square$$

Questi due risultati, fondamentalmente, traducono nel linguaggio coomologico le proprietà aritmetiche di un campo locale. Sembra superfluo aggiungere che non è possibile percorrere una strada simile per ottenere risultati analoghi nel caso di campi globali. Nel prossimo paragrafo sfrutteremo quanto appena scoperto per calcolare la coomologia in grado 2.

3.4 Calcolo del gruppo di Brauer

Ogni campo locale ha esattamente un'estensione non ramificata per ogni grado $K_n^{\mathtt{nr}}$, il cui gruppo di Galois coincide con la corrispondente estensione del campo residuo dello stesso grado: $\mathcal{G}al\,(K_n^{\mathtt{nr}}/K) = \mathcal{G}al\,(\kappa^n/\kappa) = \mathbb{Z}/n\mathbb{Z}$. Ne segue che la massima estensione non ramificata $K_{\mathtt{nr}} = \varinjlim K_n^{\mathtt{nr}}$ ha gruppo di Galois

$$G = \mathcal{G}al\,(K_{\mathtt{nr}}/K) = \mathcal{G}al\,(\bar\kappa/\kappa) = \hat{\mathbb{Z}}.$$

Siamo interessati a calcolare $\mathrm{H}^2(\Gamma,\, K_{\mathtt{nr}}^\times)$. Dalla successione esatta corta

$$1 \longrightarrow \mathcal{O}_{K_{\mathtt{nr}}}^\times \longrightarrow K_{\mathtt{nr}}^\times \xrightarrow{v} \mathbb{Z} \longrightarrow 0,$$

ricordando che $\mathcal{O}_{K_{\mathrm{nr}}}^{\times}$ è coomologicamente banale (o meglio, osservando che tutti gli oggetti del sistema induttivo di cui dobbiamo prendere il limite per calcolarlo lo sono), otteniamo un isomorfismo

$$v^*\colon \mathrm{H}^2(G,\, K_{\mathtt{nr}}^{\times}) \to \mathrm{H}^2(G,\, \mathbb{Z}).$$

Un po' a sorpresa, ripetiamo il ragionamento sulla successione esatta

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0,$$

in cui troviamo $\mathbb{Q}$ iniettivo, per ottenere un secondo isomorfismo

$$\delta\colon \mathrm{H}^2(G,\, \mathbb{Z}) \to \mathrm{H}^1(G,\, \mathbb{Q}/\mathbb{Z}).$$

Poiché $\mathbb{Q}/\mathbb{Z}$ è munito dell'azione banale, siamo in realtà interessati a calcolare $\mathrm{Hom}(G,\, \mathbb{Q}/\mathbb{Z})$, morfismi che ovviamente coincidono con le possibili immagini del generatore topologico 1 di $G = \hat{\mathbb{Z}}$: abbiamo un'identificazione formale $\gamma\colon \mathrm{H}^1(G,\, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$.

□ **Definizione 3.4.1.** Chiamiamo inv_K l'isomorfismo che otteniamo componendo le tre mappe di sopra

$$\mathrm{inv}_K\colon \mathrm{H}^2(G,\, K_{\mathtt{nr}}^{\times}) \xrightarrow{v^*} \mathrm{H}^2(G,\, \mathbb{Z}) \xrightarrow{\delta} \mathrm{H}^1(G,\, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\gamma} \mathbb{Q}/\mathbb{Z}.$$

Avendo calcolato questo gruppo, abbiamo svolto in scioltezza metà del lavoro. Le buone proprietà di questo isomorfismo saranno fondamentali per affrontare il conto rimanente.

■ **Proposizione 3.4.2.** *Sia L/K un'estensione finita di grado $n = [L : K]$. Il seguente diagramma commuta*

$$\begin{array}{ccc} \mathrm{H}^2(G_K,\, K_{\mathtt{nr}}^{\times}) & \xrightarrow{\mathrm{inv}_K} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathtt{res}} & & \downarrow{\scriptstyle \cdot n} \\ \mathrm{H}^2(G_L,\, K_{\mathtt{nr}}^{\times}) & \xrightarrow{\mathrm{inv}_L} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Dimostrazione. Analizziamo come commuta la `res` con i singoli isomorfismi di cui è composto l'isomorfismo inv. Siano e l'indice di ramificazione e f l'indice d'inerzia dell'estensione. Quando c'è ramificazione la valutazione viene rinormalizzata in modo che $(v_L)_{|K} = e \cdot v_K$, dunque

$$v_L^* \,\mathtt{res} = e \cdot v_K^* \,\mathtt{res} = e \cdot \mathtt{res}\, v_K^*,$$

dove possiamo effettuare l'ultima commutazione perché `res` è un morfismo di complessi per costruzione. Analogamente, la restrizione commuta anche con l'omomorfismo di collegamento δ. L'indice f coincide con il grado della relativa estensione del campo residuo, che dunque è proprio il generatore di $G_L = f\hat{\mathbb{Z}} < \hat{\mathbb{Z}} = G_K$; abbiamo così, ricordando che γ coincide con la valutazione nel generatore, che

$$\gamma(\mathtt{res}\, h) = (\mathtt{res}\, h)(1) = h(\mathtt{res}(1)) = h(f) = f \cdot h(1) = f \cdot \gamma(h).$$

Componendo i tre risultati, si ottiene la tesi.

$$\begin{array}{ccccccc} \mathrm{H}^2(G_K,\, K_{\mathtt{nr}}^{\times}) & \xrightarrow{v_K^*} & \mathrm{H}^2(G_K,\, \mathbb{Z}) & \xrightarrow{\delta} & \mathrm{H}^1(G_K,\, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\gamma} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathtt{res}} & & \downarrow{\scriptstyle \cdot e\,\mathtt{res}} & & \downarrow{\scriptstyle \cdot e\,\mathtt{res}} & & \downarrow{\scriptstyle \cdot ef} \\ \mathrm{H}^2(G_L,\, K_{\mathtt{nr}}^{\times}) & \xrightarrow{v_L^*} & \mathrm{H}^2(G_L,\, \mathbb{Z}) & \xrightarrow{\delta} & \mathrm{H}^1(G_L,\, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\gamma} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

□

Siamo ora pronti per dimostrare che il gruppo di Brauer relativo all'estensione non ramificata massimale è in realtà già tutto $\operatorname{Br} K$.

■ **Teorema 3.4.3.** *Il gruppo* $\operatorname{Br} K$ *è isomorfo a* $\operatorname{Br}(K_{\mathtt{nr}}/K) = \mathbb{Q}/\mathbb{Z}$.

Dimostrazione. Dimostreremo che il gruppo di Brauer relativo ad ogni estensione di Galois di grado n coincide, come sottogruppo di $\operatorname{Br} K$, con il Brauer relativo all'unica estensione non ramificata di grado n: $K^n_{\mathtt{nr}}$. È conveniente dividere la dimostrazione in due lemmi; fissiamo un'estensione L/K di Galois di grado $n = [L : K]$ e gruppo G.

Lemma 3.4.4. *La cardinalità del gruppo* $\mathrm{H}^2(G,\, L^\times)$ *divide* n.

Dimostrazione. Arriveremo alla tesi per approssimazione. Il caso in cui G sia ciclico segue immediatamente dall'Assioma del Campo di Classe (3.3.3). Affrontiamo ora il problema per G p-gruppo: grazie alla formula delle classi sappiamo che il centro è non banale, questo è abeliano e ha pertanto un sottogruppo di ordine p che chiamiamo H, normale in G. A questo gruppo sarà associata un'estensione intermedia L^H, anch'essa di Galois. Dalla successione spettrale di Hochschild-Serre, o meglio per quanto dice il corollario 1.3.3, ricaviamo la successione esatta

$$0 \longrightarrow \mathrm{H}^2(G/H,\, \left(L^H\right)^\times) \xrightarrow{\mathtt{inf}} \mathrm{H}^2(G,\, L^\times) \xrightarrow{\mathtt{res}} \mathrm{H}^2(H,\, L^\times),$$

da cui deduciamo la tesi per induzione. Segue immediatamente il caso generale: scelto un Sylow per ogni primo p, la restrizione produce degli omomorfismi iniettivi

$$0 \longrightarrow T_p\, \mathrm{H}^2(G,\, L^\times) \xrightarrow{\mathtt{res}} \mathrm{H}^2(G_p, L^\times),$$

grazie ai quali deduciamo che la cardinalità del gruppo di destra divide $|G_p|$, ovvero la massima potenza di p che compare nella fattorizzazione di n. □

Lemma 3.4.5. $\mathrm{H}^2(G,\, L^\times)$ *e* $\mathrm{H}^2(\mathcal{G}al\,(K_n^{\mathtt{nr}}/K)\,,\, K_n^{\mathtt{nr}\,\times})$ *sono lo stesso sottogruppo di* $\operatorname{Br} K$.

Dimostrazione. La cardinalità di $\mathrm{H}^2(\mathcal{G}al\,(K_n^{\mathtt{nr}}/K)\,,\, K_n^{\mathtt{nr}\,\times})$ è esattamente n: per la ciclicità del gruppo di Galois è la stessa del gruppo di Tate in grado zero, che è quella voluta per l'Assioma del Corpo di Classe. È quindi sufficiente mostrare che $\mathrm{H}^2(\mathcal{G}al\,(K_n^{\mathtt{nr}}/K)\,,\, K_n^{\mathtt{nr}\,\times})$ è un sottogruppo di $\mathrm{H}^2(G,\, L^\times)$, grazie al risultato sulla cardinalità appena stabilito. Prendiamo un elemento $x \in \mathrm{H}^2(\mathcal{G}al\,(K_n^{\mathtt{nr}}/K)\,,\, K_n^{\mathtt{nr}\,\times}) < \operatorname{Br} K_{\mathtt{nr}} < \operatorname{Br} K$. Questo vive in un gruppo di n-torsione e pertanto viene mandato in 0 dalla restrizione

$$\begin{array}{ccc}
\operatorname{Br} K & \xrightarrow{\mathtt{res}} & \operatorname{Br} L \\
\uparrow & & \uparrow \\
\mathrm{H}^2(G_K,\, K_{\mathtt{nr}}^\times) & \xrightarrow{\mathtt{res}} & \mathrm{H}^2(G_L,\, K_{\mathtt{nr}}^\times) \\
\downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\
\mathbb{Q}/\mathbb{Z} & \xrightarrow{\cdot n} & \mathbb{Q}/\mathbb{Z},
\end{array}$$

il cui nucleo è proprio $\mathrm{H}^2(G,\, L^\times)$ per la solita successione esatta dei Brauer relativi (3.1.4):

$$0 \to \mathrm{H}^2(G,\, L^\times) \to \operatorname{Br} K \to \operatorname{Br} L.$$

□

Torniamo ora alla dimostrazione del teorema. Abbiamo già osservato che $\operatorname{Br} K = \mathrm{H}^2(\Gamma_K, \bar{K}^\times)$ è unione dei Brauer relativi alle sottoestensioni di Galois finite, che per il secondo lemma coincidono con i soli Brauer relativi alle estensioni non ramificate:

$$\begin{aligned}\operatorname{Br} K &= \varinjlim_{L/K} \mathrm{H}^2(\mathcal{G}al\,(L/K)\,,\, L^\times) \\ &= \varinjlim_{n} \mathrm{H}^2(\mathcal{G}al\,(K_{\mathtt{nr}}^n/K)\,,\, K_{\mathtt{nr}}^{n\times}) \\ &= \operatorname{Br}(K_{\mathtt{nr}}/K) \\ &= \mathbb{Q}/\mathbb{Z}.\end{aligned}$$

□

3.5 Tutto il resto

In questa sezione concluderemo lo studio della coomologia di Γ_K, mostrando che questo ha dimensione coomologica 2: tutti i gruppi di coomologia rimanenti saranno dunque nulli. Quasi. Ad essere precisi, solo quelli con coefficienti in moduli di torsione.

Lemma 3.5.1. *Sia k un campo e p un numero primo. I seguenti sono equivalenti:*

i. La p-dimensione coomologica $\operatorname{cd}_p(k)$ è al più 1.

ii. Per ogni estensione finita separabile L/k, la p-torsione del $\operatorname{Br} L$ è nulla.

La p-torsione è, per definizione, il nucleo della moltiplicazione per p e non l'intera componente p-primaria, si proceda con attenzione: denoteremo la p-torsione con delle parentesi quadre $(\operatorname{Br} K)[\,p\,]$.

Dimostrazione. Assumiamo i. Per ogni L, la p-dimensione coomologica del sottogruppo $\mathcal{G}al\left(\bar{k}/L\right)$ è al più quella del gruppo $\mathcal{G}al\left(\bar{k}/k\right)$ (per 2.3.3), ne segue che

$$(\operatorname{Br} L)[\,p\,] = \mathrm{H}^2(L,\, \mu_p) = 0.$$

Assumiamo dunque ii. Sia G_p un p-Sylow di $\mathcal{G}al\left(\bar{k}/k\right)$ e L il sottocampo corrispondente. L contiene le radici dell'unità μ_p: infatti l'indice $[L(\mu_p) : L]$ deve dividere sia $p-1$, perché campo di spezzamento di $x^p - 1$, che p, per costruzione. Ne segue che

$$\mathrm{H}^2(L,\, \mathbb{Z}/p\mathbb{Z}) = \mathrm{H}^2(L,\, \mu_p) = (\operatorname{Br} L)[\,p\,],$$

che è nullo per ipotesi; da cui, sfoderando tutti i teoremi sulla dimensione coomologica a nostra conoscenza, deduciamo che $\operatorname{cd}_p(k) = \operatorname{cd}_p(L) = 1$. □

■ **Teorema 3.5.2.** *La dimensione coomologica di un campo locale è 2.*

Dimostrazione. Mostreremo preliminarmente che il gruppo di Galois assoluto $\mathcal{G}al\left(\bar{K}/K_{\mathtt{nr}}\right)$ dell'estensione non ramificata massimale $K_{\mathtt{nr}}$ ha dimensione coomologica 1. Per il lemma appena enunciato sarà sufficiente dimostrare che, per ogni primo p e ogni estensione finita e separabile $L/K_{\mathtt{nr}}$, il gruppo di Brauer $\operatorname{Br} L$ non ha componente p-primaria: questo gruppo è limite diretto dei gruppi di Brauer $\operatorname{Br} E$ delle estensioni intermedie finite $K \subseteq E \subseteq L$, per il solito teorema di passaggio al limite (1.2.7); mostreremo pertanto che ogni elemento di p^α-torsione viene eventualmente ucciso dalle mappe del sistema induttivo (che ricordiamo

essere restrizioni). Nel sistema induttivo si trova infatti, sopra E, un'estensione F per cui l'indice $[F : E] = p^\alpha$, che produce la mappa assassina che cercavamo:

$$\begin{array}{ccc} \operatorname{Br} E & \xrightarrow{\operatorname{inv}_E} & \mathbb{Q}/\mathbb{Z} \\ \Big\downarrow{\scriptstyle \mathtt{res}} & & \Big\downarrow{\scriptstyle \cdot p^\alpha} \\ \operatorname{Br} F & \xrightarrow{\operatorname{inv}_F} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Riusciamo ad ottenere l'estensione F richiesta, per esempio, componendo E con un'estensione di K non ramificata del giusto grado.

Possiamo ora concludere: l'estensione $K_{\mathtt{nr}}/K$ non ramificata massimale ha gruppo di Galois $\hat{\mathbb{Z}}$, che è un sottogruppo di $\mathcal{G}al\left(\bar{K}/K\right)$, il cui quoziente abbiamo appena mostrato avere dimensione coomologica 1; per il lemma 2.3.4, concludiamo che

$$\operatorname{cd}(K) \leq \operatorname{cd}(K_{\mathtt{nr}}) + \operatorname{cd}(\hat{\mathbb{Z}}) = 1 + 1.$$

Osserviamo infine che, per un primo p eventualmente diverso dalla caratteristica di K, il gruppo $\mathrm{H}^2(K, \mu_p) = (\operatorname{Br} K)[p]$ non è nullo; otteniamo così la disuguaglianza opposta. □

Questo teorema conclude il calcolo della coomologia di un campo locale, ma abbiamo tutt'altro che concluso lo studio. Che cosa ce ne facciamo di aver calcolato questi misteriosi gruppi di Tate? Ne ricaviamo qualcosa di comprensibile a livello di estensioni di campi? Il prossimo capitolo sarà dedicato all'interpretazione, o meglio alla decifrazione, di quanto calcolato in questo.

CAPITOLO 4

Risultati di Dualità

Il capitolo seguente è sicuramente il più tecnico, ma non poteva essere diversamente: fino ad ora non abbiamo fatto altro che introdurre il linguaggio dei funtori coomologici e tradurvici quanto già sapevamo, è giunto il momento di mettere in azione questo misterioso macchinario e vedere cosa ne possiamo ricavare.

Il grande vantaggio di una teoria coomologica è che possiamo definirci sopra un prodotto. Uno dei fondamentali problemi, è che dovremo effettivamente definirlo. Ci lanceremo dunque in un tentativo di presentare con cura la definizione, in modo che si riesca a credere ai risultati tecnici di buon comportamento del prodotto che seguiranno. Al lettore affamato di dettagli consigliamo [NSW08].

Seguirà la dimostrazione del teorema di dualità di Tate-Nakayama, risultato che, tramite il prodotto appena definito (dunque in maniera piuttosto oscura), mette in comunicazione gruppi di coomologia con coefficienti in moduli diversi. Questo ci permetterà di reinterpretare la coomologia di un campo spostando i coefficienti su moduli più semplici, $\mathbb{Z}$ per esempio, e ricavare di conseguenza qualche informazione sul gruppo di Galois in questione.

L'ultimo paragrafo sarà il momento in cui tutti i nostri sforzi saranno ripagati: otterremo una descrizione del gruppo di Galois della massima estensione abeliana di un campo locale in termini della struttura del campo stesso, l'applicazione di reciprocità locale.

4.1 Tazza Prodotto

Costruiremo ora un'applicazione bilineare tra i gruppi di coomologia, donando al nostro strumento un prodotto e, dunque, una struttura di algebra. La costruzione del "tazza-prodotto", così come la presentazione delle relative proprietà, è fondamentalmente una tediosa, lunghissima, verifica: preannuncio solo che dovremo riesumare la descrizione in cocatene. Come ogni buon libro di algebra, presenteremo dettagliatamente la costruzione del prodotto e la lista delle proprietà che useremo in seguito, lasciando decidere al lettore se fidarsi ciecamente

di quanto presentato oppure dedicare un paio di pomeriggi alla verifica diretta.

Poniamoci nella dovuta generalità. Siano A, B due G-moduli e $K_{\mathtt{om}}(A)$ e $K_{\mathtt{om}}(B)$ i corrispondenti complessi di cocatene omogenee, che si ottengono omogeneizzando le usuali cocatene $K(A)$ e $K(B)$: presa $f\colon G^i \to A$, definiamo $F\colon G^{i+1} \to A$ in modo che

$$F(g_0, g_1, \ldots, g_i) = g_0 f(g_0^{-1}g_1, g_1^{-1}g_2, \ldots, g_{i-1}^{-1}g_i).$$

Questa presentazione è molto più comoda perché l'applicazione bilineare

$$\begin{aligned} \cup\colon K^p_{\mathtt{om}}(A) \times K^q_{\mathtt{om}}(B) &\to K^{p+q}_{\mathtt{om}}(A \otimes B) \\ (a, b) &\mapsto a(g_0, \ldots, g_p) \otimes b(g_p, \ldots, g_{p+q}) \end{aligned}$$

si comporta bene con i differenziali

$$d(a \cup b) = (da) \cup b + (-1)^p a \cup (db),$$

permettendoci di passare in coomologia.

□ **Definizione 4.1.1** (Tazza prodotto)**.** Chiamiamo tazza-prodotto l'applicazione $\mathbb{Z}$-bilineare indotta dal prodotto appena definito

$$\cup\colon \mathrm{H}^p(G, A) \times \mathrm{H}^q(G, B) \to \mathrm{H}^{p+q}(G, A \otimes B)$$

Il prodotto che abbiamo ottenuto è ovviamente funtoriale e compatibile con le successioni esatte lunghe:

■ **Proposizione 4.1.2.** *Se entrambe le successioni*

$$0 \to A \to A' \to A'' \to 0, \qquad 0 \to A \otimes B \to A' \otimes B \to A'' \otimes B \to 0$$

sono esatte, allora il tazza-prodotto, fissato $\beta \in \mathrm{H}^q(G, B)$, induce un morfismo di complessi

$$\begin{array}{ccccccc} \ldots & \longrightarrow & \mathrm{H}^p(G, A') & \longrightarrow & \mathrm{H}^p(G, A'') & \xrightarrow{\delta} & \mathrm{H}^{p+1}(G, A) \longrightarrow \ldots \\ & & \downarrow{\scriptstyle \cup\beta} & & \downarrow{\scriptstyle \cup\beta} & & \downarrow{\scriptstyle \cup\beta} \\ \ldots & \longrightarrow & \mathrm{H}^{p+q}(G, A' \otimes B) & \longrightarrow & \mathrm{H}^{p+q}(G, A'' \otimes B) & \xrightarrow{\delta} & \mathrm{H}^{p+q+1}(G, A \otimes B) \longrightarrow \ldots, \end{array}$$

equivalentemente $(\delta\alpha'') \cup \beta = \delta(\alpha'' \cup \beta)$.

Segue ovviamente una proposizione duale scambiando i ruoli di A e B. Queste due proprietà, assieme alla funtorialità, determinano in modo unico il prodotto trovato, fissata un'applicazione bilineare in grado 0. È pertanto possibile dare una definizione di tazza-prodotto per i gruppi di Tate [NSW08, proposizione 1.4.7].

Presa una qualunque applicazione $\mathbb{Z}[G]$-bilineare $\varphi\colon A \times B \to C$, componendo l'omomorfismo $\varphi\colon A \otimes B \to C$ con il tazza-prodotto otteniamo una più generale nozione di prodotto in coomologia. Dalla proposizione di compatibilità precedente possiamo dedurre una versione appena più generale, che ci tornerà utile in futuro.

Lemma 4.1.3. *Fissiamo due successioni esatte*

$$0 \to A' \to A \to A'' \to 0, \qquad 0 \to B' \to B \to B'' \to 0$$

e un'applicazione bilineare $\varphi\colon A \times B \to C$ *nulla su* $A' \times B'$*. Troviamo allora due accoppiamenti*

$$\varphi'\colon A' \times B'' \to C, \qquad \varphi''\colon A'' \times B' \to C,$$

che inducono prodotti in coomologia

$$\mathrm{H}^p(G,\, A'') \times \mathrm{H}^q(G,\, B') \to \mathrm{H}^{p+q}(G,\, C)$$
$$\mathrm{H}^{p+1}(G,\, A') \times \mathrm{H}^{q-1}(G,\, B'') \to \mathrm{H}^{p+q}(G,\, C)$$

compatibili a meno del segno con le frecce di bordo delle successioni esatte lunghe associate:

$$\delta\alpha \cup \beta + (-1)^p\, a \cup \delta\beta = 0.$$

4.2 Dualità di Tate-Nakayama

Ci addentreremo ora nell'argomento più tecnico di tutta la tesi: il teorema di dualità di Tate-Nakayama, che sarà preceduto da alcuni risultati di natura puramente algebrica e dal carattere incredibilmente generale. L'obbiettivo dei risultati seguenti è di trasformare i criteri di banalità, introdotti qualche capitolo addietro, in strumenti per costruire isomorfismi tra gruppi di coomologia con coefficienti diversi. Per fare questo cominceremo assumendo ipotesi ad hoc, della cui ragionevolezza ci preoccuperemo solo in futuro.

■ **Proposizione 4.2.1.** *Sia* $f\colon B \to C$ *una mappa tra* G *moduli. Supponiamo di conoscere per ogni primo* p *un indice* n_p *per cui*

$$\widehat{\mathrm{H}}^{n_p}(G_p,\, B) \twoheadrightarrow \widehat{\mathrm{H}}^{n_p}(G_p,\, C) \qquad \textit{sia suriettivo,}$$
$$\widehat{\mathrm{H}}^{n_p+1}(G_p,\, B) \to \widehat{\mathrm{H}}^{n_p+1}(G_p,\, C) \qquad \textit{sia un isomorfismo,}$$
$$\widehat{\mathrm{H}}^{n_p+2}(G_p,\, B) \hookrightarrow \widehat{\mathrm{H}}^{n_p+2}(G_p,\, C) \qquad \textit{sia iniettivo.}$$

Possiamo allora concludere che, per ogni modulo D *piatto e ogni sottogruppo* $H < G$*, la mappa indotta dal tensore*

$$\widehat{\mathrm{H}}^n(H,\, B \otimes D) \to \widehat{\mathrm{H}}^n(H,\, C \otimes D) \qquad \textit{è un isomorfismo, per ogni } n.$$

La tesi è sopraffacente. È utile pensare al risultato prima nella forma più semplice, con $H = G$ e $D = \mathbb{Z}$, in cui sono stati semplicemente prodotti degli isomorfismi infilando abbastanza zeri nella successione esatta lunghissima associata; a cui seguono due piccole aggiunte che, essendo gratuite, abbiamo deciso di includere per completezza: che sia valida per ogni sottogruppo non è sorprendente, dato che la definizione di "coomologicamente banale" è una condizione rispetto ai sottogruppi; che si possano estendere i coefficienti, segue invece dal fatto che i moduli piatti preservano gli indotti (2.2.8).

Dimostrazione. Le ipotesi sono scelte in modo da funzionare magnificamente una volta assunto che f sia iniettiva: in questo caso otteniamo una successione esatta corta

$$0 \longrightarrow B \xrightarrow{f} C \longrightarrow Q \longrightarrow 0$$

la cui successione esatta lunga associata, per ogni primo p, restituisce

$$\widehat{\mathrm{H}}^{n_p}(G_p,\, Q) = \widehat{\mathrm{H}}^{n_p+1}(G_p,\, Q) = 0,$$

da cui, per il criterio di banalità (2.2.4), deduciamo che Q è coomologicamente banale. Abbiamo già osservato che $Q \otimes D$ rimane tale (2.2.8), da cui la tesi.

Per concludere è pertanto sufficiente mostrare che ci si può ricondurre al caso precedente. Per fare questo consideriamo la classica immersione di B nel suo modulo indotto $j\colon B \hookrightarrow \mathrm{Ind}_1^G(B)$ e dunque la mappa iniettiva

$$(f, j)\colon B \hookrightarrow C \oplus \mathrm{Ind}_1^G(B),$$

la tesi segue dunque dal caso precedente e dalla banalità dell'indotto, che trasforma la successione esatta corta

$$0 \longrightarrow C \xrightarrow{f} C \oplus \mathrm{Ind}_1^G(B) \longrightarrow \mathrm{Ind}_1^G(B) \longrightarrow 0$$

in degli isomorfismi

$$\widehat{\mathrm{H}}^n(H,\, C \otimes D) = \widehat{\mathrm{H}}^n\left(H,\, \left(C \oplus \mathrm{Ind}_1^G(B)\right) \otimes D\right). \qquad \square$$

Ripreso il fiato, concessoci il tempo di capire quanto attentamente sono state scelte le ipotesi, procediamo verso una generalizzazione ancora più spinta. Vorremmo un risultato analogo per mappe indotte dal tazza-prodotto, che come unica differenza producono un cambio di dimensione in arrivo.

■ **Proposizione 4.2.2.** *Sia $\varphi\colon A \times B \to C$ una mappa bilineare tra G moduli; fissiamo un elemento $a \in \mathrm{H}^q(G,\, A)$. Supponiamo di conoscere, per ogni primo p, un indice n_p per cui l'omomorfismo indotto dal tazza prodotto per* `res` *a*

$$\begin{aligned}
\widehat{\mathrm{H}}^{n_p}(G_p,\, B) &\twoheadrightarrow \widehat{\mathrm{H}}^{n_p+q}(G_p,\, C) && \textit{sia suriettivo,}\\
\widehat{\mathrm{H}}^{n_p+1}(G_p,\, B) &\to \widehat{\mathrm{H}}^{n_p+q+1}(G_p,\, C) && \textit{sia un isomorfismo,}\\
\widehat{\mathrm{H}}^{n_p+2}(G_p,\, B) &\hookrightarrow \widehat{\mathrm{H}}^{n_p+q+2}(G_p,\, C) && \textit{sia iniettivo.}
\end{aligned}$$

Possiamo allora concludere che, per ogni modulo D piatto e ogni sottogruppo $H < G$, la mappa indotta dal tazza-prodotto per `res` *a*

$$\widehat{\mathrm{H}}^n(H,\, B \otimes D) \to \widehat{\mathrm{H}}^{n+q}(H,\, C \otimes D) \qquad \textit{è un isomorfismo, per ogni } n.$$

Dimostrazione. Giocando a trovare le differenze con la proposizione precedente, si scopre che queste coincidono quando $a \in \mathrm{H}^0(G,\, A)$, ovvero assumendo $q = 0$. Per concludere è pertanto sufficiente mostrare che ci si può ricondurre al caso precedente. Il modo naturale di farlo è passare ai moduli con coomologia traslata: cominciamo dal caso $q = 1$. Sostituendo A, C con A_1, C_1, otteniamo un'applicazione bilineare $\varphi_1\colon A_1 \times B \to C_1$ abbastanza naturalmente

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \longrightarrow & \mathrm{Ind}_1^G(A) & \longrightarrow & A_1 & \longrightarrow & 0\\
 & & \downarrow{\scriptstyle \cdot_\varphi \beta} & & \downarrow{\scriptstyle \cdot_\varphi \beta} & & \vdots{\scriptstyle \cdot_{\varphi_1} \beta} & & \\
0 & \longrightarrow & C & \longrightarrow & \mathrm{Ind}_1^G(C) & \longrightarrow & C_1 & \longrightarrow & 0.
\end{array}$$

Prendiamo l'elemento $a_1 \in \widehat{\mathrm{H}}^0(G,\, A_1)$ corrispondente ad a: l'unico per cui $\delta(a_1) = a$. La tesi è vera per il prodotto indotto da φ_1 e l'elemento a_1, abbiamo pertanto dei meravigliosi isomorfismi

$$\widehat{\mathrm{H}}^n(H,\, B \otimes D) \xrightarrow{a_1 \cup} \widehat{\mathrm{H}}^n(H,\, C_1 \otimes D)$$

a cui possiamo aggiungere il classico isomorfismo di collegamento

$$\widehat{\mathrm{H}}^n(H,\, B \otimes D) \xrightarrow{a_1 \cup} \widehat{\mathrm{H}}^n(H,\, C_1 \otimes D) \xrightarrow{\delta} \widehat{\mathrm{H}}^{n+1}(G,\, C \otimes D).$$

Deduciamo la tesi grazie al risultato di compatibilità del tazza-prodotto (4.1.2): l'isomorfismo trovato è infatti

$$x \mapsto \delta(\mathtt{res}\, a_1 \cup x) = \delta(\mathtt{res}\, a_1) \cup x = \mathtt{res}\, a \cup x.$$

Analogamente si procede per ogni q. □

Raggiunto il desiderato livello di astrazione, possiamo occuparci di riformulare le particolari ipotesi in una forma più accessibile, se non proprio comprensibile.

■ **Teorema 4.2.3** (Dualità di Tate-Nakayama)**.** *Sia A un G-modulo. Fissiamo un elemento $a \in \mathrm{H}^2(G,\, A)$. Supponiamo di sapere, per ogni numero primo p, che*

i. $\mathrm{H}^1(G_p,\, A) = 0$*;*

ii. il gruppo $\mathrm{H}^2(G_p,\, A)$ *ha la stessa cardinalità di* G_p*, diciamo* m_p*, ed è generato da* $\mathtt{res}\, a$*.*

Possiamo allora concludere che l'omomorfismo indotto dal tazza-prodotto con $\mathtt{res}\, a$ *induce, per ogni sottogruppo* $H < G$*, un isomorfismo*

$$\widehat{\mathrm{H}}^n(H,\, \mathbb{Z}) \to \widehat{\mathrm{H}}^{n+2}(H,\, A) \qquad \textit{per ogni } n.$$

Dimostrazione. Applichiamo la proposizione precedente con $B = \mathbb{Z}$, $C = A$ e $D = \mathbb{Z}$. Le ipotesi sono verificate per $n_p = -1$:

$$\begin{aligned}
\widehat{\mathrm{H}}^{-1}(G_p,\, \mathbb{Z}) \twoheadrightarrow \widehat{\mathrm{H}}^1(G_p,\, A) = 0 &\qquad \text{per l'ipotesi } i,\\
\mathbb{Z}/m_p\mathbb{Z} = \widehat{\mathrm{H}}^0(G_p,\, \mathbb{Z}) \to \widehat{\mathrm{H}}^2(G_p,\, A) = \mathbb{Z}/m_p\mathbb{Z} &\qquad \text{per l'ipotesi } ii,\\
0 = \widehat{\mathrm{H}}^1(G_p,\, \mathbb{Z}) \hookrightarrow \widehat{\mathrm{H}}^3(G_p,\, A) &\qquad \text{per l'ipotesi } i.
\end{aligned}$$

□

Al contrario delle proposizioni precedenti, le ipotesi del teorema di dualità sembrano avere qualcosa a che fare con quanto visto fin'ora. Il risultato dovrebbe però chiarire in parte perché abbiamo deciso di percorrere questa strada: cambiando i coefficienti da un modulo qualunque a $\mathbb{Z}$, riusciamo a spostare risultati specifici, per esempio le proprietà aritmetiche di un campo, a gruppi che invece conosciamo esplicitamente, per dire $\mathrm{H}_1(G,\, \mathbb{Z})$ che, classicamente, coincide con l'abelianizzato $G^{\mathtt{ab}}$. Nella sezione seguente ci addentreremo più approfonditamente nell'argomento.

4.3 Reciprocità Locale

Continuando nella nostra discesa dall'astrazione verso la Teoria del Corpo di Classe, applichiamo il teorema di dualità di Tate-Nakayama al caso dei campi locali: ne otterremo una descrizione dei gruppi di Galois in funzione della struttura del campo stesso. Siano K un campo locale e L/K un'estensione finita di Galois di grado $n = [L : K]$; chiamiamo G il gruppo di Galois dell'estensione e poniamo $A = L^\times$. Per Hilbert 90 la prima ipotesi del teorema di Tate-Nakayama è soddisfatta

$$i.\ \mathrm{H}^1(G_p,\, L^\times) = 0$$

e, grazie al nostro studio del gruppo di Brauer, anche la seconda: per uno dei lemmi comparsi nel calcolo del Brauer (in particolare 3.4.5) sappiamo che $\mathrm{H}^2(G,\, L^\times)$ coincide con il sottogruppo di n-torsione di $\operatorname{Br} K = \mathbb{Q}/\mathbb{Z}$, possiamo pertanto scegliere l'unico elemento $u \in \mathrm{H}^2(G,\, L^\times)$ per cui $\operatorname{inv}_K(u) = \frac{1}{n}$; per il lemma di compatibilità tra invarianti e restrizione (3.4.2), si ha che

$$ii.\ \mathrm{H}^2(G_p,\, L^\times) = T_p \operatorname{Br}(L/K) \ \text{ è generato da } \ \mathtt{res}\, u.$$

Il teorema di dualità produce allora un isomorfismo

$$\theta\colon \widehat{\mathrm{H}}^{-2}(G,\, \mathbb{Z}) \to \widehat{\mathrm{H}}^0(G,\, L^\times),$$

che coincide con il tazza-prodotto per u. Il primo gruppo è proprio con G^{ab}: la successione esatta lunga in omologia associata a

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

fornisce infatti l'isomorfismo richiesto: vi troviamo infatti $\mathrm{H}^1(G,\, \mathbb{Z}) \to I_G/I_G^2$, che ci permette di concludere perché la mappa

$$\begin{aligned} G^{\mathtt{ab}} &\to I_G/I_G^2 \\ g &\mapsto g - 1 \end{aligned}$$

è un isomorfismo; per esplicitare il secondo gruppo è invece sufficiente andare a riprendere la definizione (1.2). Ne segue dunque che

■ **Teorema 4.3.1** (Reciprocità Locale)**.** *Ogni estensione abeliana finita L/K è accompagnata da un isomorfismo*

$$\omega_L\colon \frac{K^\times}{NL^\times} \to \mathcal{G}al\,(L/K)\,,$$

dove N è, come al solito, la norma.

Questo conclude in un qualche senso lo studio delle estensioni abeliane di un campo locale. Per esempio, possiamo annunciare trionfanti di essere riusciti a calcolare il gruppo di Galois della massima estensione abeliana, ovvero l'abelianizzato del gruppo di Galois assoluto Γ_K: prendendo il limite inverso di ω_L sulle estensioni abeliane finite, otteniamo una mappa

$$\omega\colon K^\times \to \Gamma_K^{\mathtt{ab}},$$

detta *applicazione di reciprocità*, che su $\varprojlim_L K^\times/NL^\times$ è un isomorfismo:

$$\Gamma_K^{\mathtt{ab}} = \varprojlim_L \frac{K^\times}{NL^\times}. \tag{4.1}$$

Tornando con i piedi per terra, soffermiamoci su quella fastidiosa N al denominatore: come speriamo di calcolare esplicitamente questo gruppo? Come si calcola l'immagine tramite la norma di una data estensione? Studiando più approfonditamente l'applicazione di reciprocità è possibile raffinare il risultato, arrivando a mostrare che il limite in questione coincide proprio con la definizione di completamento profinito: sarà sufficiente mostrare che $NL^\times$ spazia fra tutti e soli i sottogruppi aperti (e di indice finito) di $K^\times$ ([Ser79, XIV.§6.1]). Nel paragrafo successivo ci concentreremo sul caso dei campi p-adici, per cui aggireremo il problema mostrando che

$$\Gamma_K^{\mathrm{ab}} = \varprojlim_n \frac{K^\times}{{K^\times}^n},$$

limite che a sua volta coincide con il completamento profinito $\hat{K}^\times$.

4.4 Dualità di Tate

Ci concentriamo ora sui campi p-adici, principalmente perché la struttura aritmetica presenta la seguente proprietà, di cui ometteremo la dimostrazione, essendo un risultato classico in teoria dei numeri [Har13, proposizione 4.11].

■ **Proposizione 4.4.1.** *Sia K un campo p-adico, i sottogruppi ${K^\times}^n$ sono aperti.*

Quest'osservazione è fondamentale qualunque strada si cerchi di intraprendere per calcolare il limite desiderato (4.1), stiamo infatti mostrando che i sottogruppi ${K^\times}^n$ sono aperti con l'obbiettivo di trovare una successione cofinale su cui calcolare sia il limite del completamento che il limite (4.1): che questa sia cofinale tra gli aperti è immediato, infatti ogni sottogruppo U aperto ha indice finito n e pertanto deve contenere ${K^\times}^n$. Se riuscissimo a mostrare che sono cofinali anche negli $NL^\times$ avremmo concluso, ma non è il percorso che intraprenderemo.

▼ **Corollario 4.4.2.** *Sia A un Γ_K-modulo finito. I gruppi $\mathrm{H}^i(K, A)$ sono finiti per ogni $i > 0$.*

Dimostrazione. Avendo ogni campo locale dimensione coomologica 2, sarà sufficiente concentrarsi sui gradi bassi $i = 0, 1, 2$. Osserviamo che per le radici n-esime dell'unità $A = \mu_n$ la tesi è già stata mostrata: in $i = 0$ per definizione, in $i = 1$ è la proposizione appena enunciata, in $i = 2$ si tratta della n-torsione del Brauer. Preso un modulo A di cardinalità n, troviamo un sottogruppo normale e aperto di $U < \Gamma_K$ che agisce banalmente sia su A che su μ_n, per esempio dentro l'intersezione degli stabilizzatori di tutti gli elementi. Pensato come U-modulo, A ha solo la struttura di gruppo abeliano, possiamo pertanto pensarlo come somma diretta di finiti μ_{n_i}, per qualche $n_i \mid n$. Avendo già mostrato il teorema per le radici dell'unità, scopriamo che $\mathrm{H}^i(U, A)$ è finito per ogni $i \geq 0$. Concludiamo sfruttando la successione spettrale di Hochschild-Serre, che in pagina due presenta solo moduli finiti

$$\mathrm{H}^p(G/U, \mathrm{H}^q(U, A)),$$

i cui quozienti, necessariamente finiti, filtrano $\mathrm{H}^{p+q}(G,\, A)$, che risulterà pertanto finito a sua volta. □

Prima di poter enunciare il teorema di dualità di Tate, dobbiamo introdurre una serie di dualità, diverse ma dallo stesso sapore: una per i gruppi, classica, e una meno nota per i moduli.

□ **Definizione 4.4.3** (Duale di Pontryagin)**.** Per ogni gruppo G, definiamo il duale secondo Pontryagin come

$$G^\vee = \mathrm{Hom}_{\mathsf{Gr}}(G,\, \mathbb{Q}/\mathbb{Z}).$$

Osserviamo innanzitutto che, in analogia alla classica dualità tra spazi vettoriali, la dualità tra due gruppi abeliani finiti A, B è equivalente all'esistenza di un accoppiamento perfetto

$$A \times B \to \mathbb{Q}/\mathbb{Z},$$

ovvero una mappa bilineare non degenere.

■ **Proposizione 4.4.4.** *Il biduale di un gruppo profinito è canonicamente isomorfo all'abelianizzato del gruppo stesso.*

Dimostrazione. Il risultato è evidente per i gruppi abeliani finiti, per cui possiamo costruire esplicitamente l'isomorfismo che associa ad ogni elemento la corrispondente valutazione

$$\begin{aligned} G &\to \mathrm{Hom}_{\mathbb{Z}}(G^\vee,\, \mathbb{Q}/\mathbb{Z}) \\ g &\mapsto \psi_g \colon \varphi \mapsto \varphi(g). \end{aligned}$$

Passando al limite raggiungiamo tutti i gruppi abeliani profiniti. Infine, osserviamo che

$$\mathrm{Hom}_{\mathsf{Gr}}(G,\, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}(G^{\mathsf{ab}},\, \mathbb{Q}/\mathbb{Z})$$

per la proprietà universale dell'abelianizzato, da cui la tesi. □

Passiamo ora alla dualità dei moduli: vorremo definire la dualità nello stesso modo, ma abbiamo bisogno quantomeno di una topologia su $\mathbb{Q}/\mathbb{Z}$. Poiché la scelta non è univoca, ci limitiamo a farlo in un caso in cui è quantomeno naturale: quando il gruppo in questione è un gruppo di Galois Γ, pensiamo $\mathbb{Q}/\mathbb{Z}$ come il gruppo di tutte le radici dell'unità $\mu_\infty < \bar{K}^\times$. Equivalentemente, possiamo pensare al duale come alle mappe in $K^\times$, che avranno però necessariamente immagine nel suo sottogruppo di torsione: μ_∞.

□ **Definizione 4.4.5** (Duale di Cartier)**.** Per ogni Γ-modulo A, definiamo il duale secondo Cartier come il gruppo

$$A^* = \mathrm{Hom}_{\Gamma}(A,\, \mu_\infty)$$

munito della sua naturale struttura di Γ-modulo, quella che si ottiene scegliendo la topologia della convergenza puntuale e lasciando agire Γ a sinistra sulle mappe: $g \cdot f \colon x \mapsto f(gx)$.

■ **Proposizione 4.4.6.** *Il biduale di un modulo finito è canonicamente isomorfo al modulo stesso.*

Presentiamo ora un risultato generale di algebra omologica, nella cui dimostrazione, pavidamente, non ci addentreremo [Ser02, I.3.6].

■ **Proposizione 4.4.7.** *Sia G un gruppo profinito di dimensione coomologica finita* $\mathrm{cd}(G) = d$. *Se il funtore* $\mathrm{H}^d(G, \bullet)$ *manda moduli finiti in gruppi finiti, il suo duale* $\mathrm{H}^d(G, \bullet)^\vee$ *è rappresentabile sulla sottocategoria dei moduli finiti: ovvero esiste un modulo I di torsione per cui*

$$\mathrm{H}^d(G, A)^\vee = \mathrm{Hom}_G(A, I) \qquad \text{per ogni } A \text{ finito.} \tag{4.2}$$

□ **Definizione 4.4.8.** Non contenti della quantità di dualità introdotto finora, chiamiamo *modulo dualizzante* di G uno G-modulo I per cui valga la (4.2).

L'ipotesi di finitezza è soffocante. Il meglio che riusciamo a fare è estendere (4.2) a moduli di torsione: scrivendo A di torsione come unione di moduli finiti $\varinjlim_i A_i$, tramite la solita proposizione 1.2.7 di passaggio al limite otteniamo infatti

$$\mathrm{H}^d(G, \varinjlim_i A_i)^\vee = \varprojlim_i \mathrm{H}^d(G, A_i)^\vee = \varprojlim_i \mathrm{Hom}_G(A_i, I) = \mathrm{Hom}_G(\varinjlim_i A_i, I).$$

Fissiamo ora un campo p-adico K e il suo gruppo di Galois assoluto Γ. Abbiamo calcolato, nel capitolo scorso (3.5.2), che la dimensione coomologica di Γ è 2: troviamo quindi un modulo dualizzante I per cui

$$\mathrm{H}^2(G, \bullet)^\vee = \mathrm{Hom}_G(\bullet, I).$$

Lemma 4.4.9. *Sia G un gruppo di dimensione coomologica n. Detto I un suo modulo dualizzante, questo è dualizzante per ogni sottogruppo $U < G$ aperto.*

Dimostrazione. Il risultato segue immediatamente dal Lemma di Shapiro (1.6.1):

$$\mathrm{H}^n(U, A)^\vee = \mathrm{H}^n(G, \mathrm{Ind}_U^G(A))^\vee = \mathrm{Hom}_G(\mathrm{Ind}_U^G(A), I) = \mathrm{Hom}_U(A, f^\times I). \qquad \square$$

■ **Proposizione 4.4.10.** *Il modulo dualizzante di Γ è canonicamente isomorfo al modulo di tutte le radici dell'unità μ_∞.*

Dimostrazione. Sia I un modulo dualizzante e $I[\,n\,]$ il sottomodulo di n-torsione, nucleo della moltiplicazione per n:

$$0 \longrightarrow I[\,n\,] \longrightarrow I \xrightarrow{\cdot n} I \longrightarrow 0.$$

Per definizione di modulo dualizzante, essendo I dualizzante per ogni sottgruppo aperto U di Γ, abbiamo un isomorfismo

$$\mathrm{Hom}_U(\mu_n, I) \to \mathrm{H}^2(U, \mu_n)^\vee; \tag{4.3}$$

avendo impiegato un'intero capitolo per calcolarlo, conosciamo ora il gruppo di Brauer dell'estensione finita relativa a U e sappiamo dunque che

$$\mathrm{H}^2(U, \mu_n) = (\mathrm{Br}\, \bar{K}^U)[\,n\,] = \mathbb{Z}/n\mathbb{Z}.$$

Osservando infine che essendo μ_n di n-torsione così sarà la sua immagine, possiamo riscrivere l'isomorfismo (4.3) di sopra come

$$\mathrm{Hom}_U(\mu_n, I_n) \to \mathrm{Hom}_U(\mu_n, I) \to \mathrm{H}^2(U, \mu_n)^\vee \to \mathbb{Z}/n\mathbb{Z}.$$

Ne deduciamo che l'azione di Γ su $\mathrm{Hom}_{\mathbb{Z}}(\mu_n, I_n)$ è sempre banale: se così non fosse lo stabilizzatore di un qualche elemento sarebbe un sottogruppo proprio aperto U, il che ci porterebbe

a concludere che questo elemento non può appartenere a $\mathrm{Hom}_U(\mu_n, I_n)$, contraddicendo l'isomorfismo appena ottenuto. Ne segue che un isomorfismo di gruppi $\mu_n \to I_n$ è automaticamente Γ-equivariante: possiamo prendere, per esempio, l'isomorfismo $f_n \in \mathrm{Hom}_U(\mu_n, I_n)$ che corrisponde a 1 in $\mathbb{Z}/n\mathbb{Z}$ (è chiaro che sia un isomorfismo non appena ci si dimentica della struttura di modulo su μ_n e I_n). Infine, assembliamo l'isomorfismo

$$\left(f = \bigcup f_n\right) : \left(\mu_\infty = \bigcup \mu_n\right) \to \left(I = \bigcup I_n\right). \qquad \square$$

Siamo finalmente pronti a enunciare il risultato principale di questo capitolo.

■ **Teorema 4.4.11** (Dualità di Tate)**.** *Sia K un campo p-adico e A un Γ-modulo finito. Il tazza-prodotto induce un accoppiamento di dualità tra gruppi finiti*

$$\mathrm{H}^i(\Gamma, A) \times \mathrm{H}^{2-i}(\Gamma, A^*) \to \mathrm{H}^2(\Gamma, \bar{K}^\times) = \mathbb{Q}/\mathbb{Z}$$

per $i = 0, 1, 2$.

Dimostrazione. Cominciamo osservando che, a rigore, l'immagine del tazza-prodotto dovrebbe avere i coefficienti in $A \otimes A^*$, che però con la mappa data dalla dualità di Cartier:

$$A \otimes \mathrm{Hom}(A, \mu_\infty) \to \mu_\infty.$$

Partiamo dal caso $i = 0$, da cui segue $i = 2$ per simmetria. Tutto il lavoro necessario è in realtà contenuto nella proposizione precedente, otteniamo infatti la tesi da

$$\begin{aligned} \mathrm{H}^2(\Gamma, A)^\vee &= \mathrm{Hom}_\Gamma(A, \mu_\infty) && \text{per via del dualizzante,} \\ &= \mathrm{Hom}_\mathbb{Z}(A, \mu_\infty)^\Gamma && \text{per definizione,} \\ &= \mathrm{H}^0(\Gamma, A^*) && \text{per definizione.} \end{aligned}$$

Affrontiamo ora il caso $i = 1$. Essendo i gruppi in questione finiti per quanto visto a inizio capitolo (4.4.2), è sufficiente mostrare che l'omomorfismo di dualità

$$\mathrm{H}^1(\Gamma, A) \to \mathrm{H}^1(\Gamma, A^*)^\vee$$

è iniettivo: per simmetria lo sarà anche nell'altra direzione. Abbiamo bisogno di applicare una delle misteriose proprietà del tazza-prodotto: la 4.1.3, in particolare. Le ipotesi sono facilmente verificate avendo, poiché $f^\times \mu_\infty$ è un modulo iniettivo, due successioni esatte corte

$$0 \to A \to \mathrm{Ind}_1^\Gamma(A) \to A_1 \to 0, \qquad 0 \to A_1^* \to \mathrm{Ind}_1^\Gamma(A)^* \to A^* \to 0$$

sui cui moduli iniziali il tazza-prodotto è evidentemente nullo:

$$A \otimes A_1^* = A \otimes \mathrm{Hom}(\mathrm{Ind}_1^\Gamma(A)/A, \mu_\infty) = 0.$$

Otteniamo dunque due accoppiamenti di dualità

$$\begin{gathered} \mathrm{H}^1(\Gamma, A_1) \times \mathrm{H}^1(\Gamma, A_1^*) \to \mathrm{H}^2(\Gamma, \bar{K}^\times), \\ \mathrm{H}^0(\Gamma, A) \times \mathrm{H}^2(G, A^*) \to \mathrm{H}^2(\Gamma, \bar{K}^\times) \end{gathered}$$

compatibili con le mappe di transizione, che quindi possiamo incastrare nel diagramma commutativo a meno del segno

$$\begin{array}{ccccccc} \mathrm{H}^0(\Gamma,\, \mathrm{Ind}_1^\Gamma(A)) & \longrightarrow & \mathrm{H}^0(\Gamma,\, A_1) & \longrightarrow & \mathrm{H}^1(\Gamma,\, A) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ \mathrm{H}^2(\Gamma,\, \mathrm{Ind}_1^\Gamma(A)^*)^\vee & \longrightarrow & \mathrm{H}^2(\Gamma,\, A_1^*)^\vee & \longrightarrow & \mathrm{H}^1(\Gamma,\, A^*)^\vee, & & \end{array}$$

in cui le mappe orizzontali sono parte delle solite successioni esatte lunghe associate alle due corte riportate sopra (quella sotto, dualizzata), mentre le mappe verticali sono i morfismi di dualità indotti dal tazza-prodotto; per la parte di teorema già dimostrata, i primi due omomorfismi verticali sono isomorfismi: se i due moduli in questione non fossero finiti, potremmo comunque estendere l'isomorfismo passando al limite, essendo i due duali di torsione. Segue la tesi per diagram-chasing. □

Con un piccolo trucco, riusciamo a sfruttare questo risultato di dualità per calcolare il gruppo Γ^{ab}, completando così lo studio della teoria del campo di classe per campi p-adici.

■ **Teorema 4.4.12.** *Γ^{ab} è isomorfo al completamento profinito $\hat{K}^\times$.*

Dimostrazione.

$$\begin{aligned} \Gamma^{\mathsf{ab}} &= \mathrm{Hom}_{\mathsf{Gr}}(\Gamma,\, \mathbb{Q}/\mathbb{Z})^\vee && \text{per dualità di Pontryagin} \\ &= \mathrm{Hom}_{\mathsf{Gr}}(\Gamma,\, \varinjlim_n \mathbb{Z}/n\mathbb{Z})^\vee && \text{piccolo trucco} \\ &= \varprojlim_n \mathrm{Hom}_{\mathsf{Gr}}(\Gamma,\, \mathbb{Z}/n\mathbb{Z})^\vee && \text{per abstract nonsense} \\ &= \varprojlim_n \mathrm{H}^1(\Gamma,\, \mathbb{Z}/n\mathbb{Z})^\vee && \text{perché l'azione è banale} \\ &= \varprojlim_n \mathrm{H}^1(\Gamma,\, \mu_n) && \text{per dualità di Tate} \\ &= \varprojlim_n K^\times/{K^\times}^n && \text{dalla successione esatta lunga} \\ &= \hat{K}^\times. && \text{per cofinalità di } {K^\times}^n \text{ negli aperti.} \end{aligned}$$

□

Bibliografia

[Har13] David Harari. Théorie du corps de classes, 2013.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[Ser02] Jean-Pierre Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2002. Translated from the French by Patrick Ion and revised by the author.

[Wei94] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.