1 Gruppi Profiniti

1.1 Definizioni

Nota: Le seguenti definizioni possono essere date in generale per gli elementi di una categoria qualunque.

Definizione 1.1 (Insieme diretto). *Un* insieme diretto *è un insieme I dotato di una relazione $\leq$ riflessiva, transitiva, e tale che per ogni $i_1, i_2 \in I$ esiste $i \in I$ tale che $i_1 \leq i$ e $i_2 \leq i$.*

Definizione 1.2 (Sistema diretto). *Un* sistema diretto di gruppi abeliani *è un oggetto della forma (I, A_i, τ_{ij}) dove:*

(a) *$(I, \leq)$ è un insieme diretto;*

(b) *A_i è un gruppo abeliano per ogni $i \in I$;*

(c) *per ogni $i \leq j$ in I, $\tau_{ij} : A_i \to A_j$ è un omomorfismo di gruppi abeliani tale che per ogni $i \in I$ τ_{ii} è l'identità e per ogni $i \leq j \leq k$ in I si ha $\tau_{jk} \circ \tau_{ij} = \tau_{ik}$.*

Definizione 1.3 (Morfismo di sistemi diretti). *Supponiamo di avere (I, A_i, τ_{ij}), $(I', A'_{i'}, \tau'_{i'j'})$ sistemi diretti e sia $\psi : I \to I'$ una mappa che preserva le relazioni d'ordine tale che per ogni $i \in I$ è dato un omomorfismo $\psi_i : A_i \to A'_{\psi(i)}$ tale che per ogni $i \leq j$ in I il diagramma*

$$\begin{array}{ccc} A_i & \xrightarrow{\psi_i} & A'_{\psi(i)} \\ {\scriptstyle \tau_{ij}}\downarrow & & \downarrow{\scriptstyle \tau'_{\psi(i)\psi(j)}} \\ A_j & \xrightarrow[\psi_j]{} & A'_{\psi(j)} \end{array}$$

commuti. Allora la terna (ψ, ψ_i, I) viene detta morfismo di sistemi diretti.

Definizione 1.4 (Limite diretto). *Sia (A_i) un sistema diretto di gruppi abeliani, e poniamo $S = \sqcup_{i \in I} A_i$. Consideriamo la relazione $\sim$ definita da*

$$x \sim y \text{ con } x \in A_i,\ y \in A_j \iff \exists k \in I \text{ tale che } k \geq i, j \text{ e } \tau_{ik}(x) = \tau_{jk}(x)$$

Così definita $\sim$ stabilisce una relazione di equivalenza su S, quindi possiamo porre

$$\varinjlim A_i = S/\sim$$

Dato un sistema diretto di gruppi abeliani (A_i), possiamo dare al limite diretto $A = \varinjlim A_i$ una naturale struttura di gruppo abeliano: siano $[x], [y]$ in A, e siano $x \in A_i$, $y \in A_j$ loro rappresentanti, $k \geq i,\ j$. Poniamo quindi

$$[x] + [y] = [\tau_{ik}(x) + \tau_{jk}(y)]$$

Definizione 1.5 (Sistema inverso). *Un* sistema inverso di gruppi topologici su I *è un oggetto della forma* (I, G_i, π_{ji}) *dove:*

(a) $(I, \leq)$ *è un insieme diretto;*

(b) G_i *è un gruppo topologico per ogni* $i \in I$*;*

(c) *per ogni* $i \leq j$ *in* I*,* π_{ji} *è un morfismo* $G_j \to G_i$ *di gruppi topologici tale che per ogni* $i \in I$ π_{ii} *è l'identità e per ogni* $i \leq j \leq k$ *in* I *si ha* $\pi_{ji} \circ \pi_{kj} = \pi_{ki}$*.*

Definizione 1.6 (Morfismo di sistemi inversi). *Supponiamo di avere* (I, G_i, π_{ji})*,* $(I', G'_{i'}, \pi'_{j'i'})$ *sistemi inversi e sia* $\phi : I' \to I$ *una mappa che preserva le relazioni d'ordine tale che per ogni* $i' \in I'$ *è dato un morfismo* $\phi_{i'} : G_{\phi(i')} \to G'_{i'}$ *tale che per ogni* $i' \leq j'$ *in* I' *il diagramma*

$$\begin{array}{ccc} G_{\phi(i')} & \xrightarrow{\phi_{i'}} & G'_{i'} \\ {\scriptstyle \pi_{\phi(j')\phi(i')}}\uparrow & & \uparrow{\scriptstyle \pi_{j'i'}} \\ G_{\phi(j')} & \xrightarrow[\phi_{j'}]{} & G'_{j'} \end{array}$$

commuti. Allora la terna $(\phi, \phi_{i'}, I')$ *viene detta* morfismo di sistemi inversi*.*

D'ora in poi ogni gruppo G verrà considerato un gruppo topologico per mezzo della topologia discreta.

Sia ora (G_i) un sistema inverso di gruppi, e consideriamo il prodotto cartesiano $\prod_i G_i$. Possiamo mettere su questo insieme la topologia che ha come sistema fondamentale di intorni di 1 i nuclei delle proiezioni $\prod_i G_i \to G_i$.

Definizione 1.7 (Limite inverso). *Sia* (G_i) *un sistema inverso di gruppi. Allora*

$$L = \left\{ (x_i) \in \prod G_i \,|\, i \leq j \Rightarrow \pi_{ji}(x_j) = x_i \right\}$$

con la topologia di sottospazio viene detto limite inverso *del sistema* G_i*. Indicheremo*

$$L = \varprojlim G_i$$

Osserviamo che se $\Phi : (G_i) \to (G'_{i'})$ è un morfismo di sistemi inversi allora possiamo definire una mappa

$$\psi : \prod_i G_i \to \prod_{i'} G_{i'}$$

in questo modo: dato $x \in G_i$ e $i' \in I'$, $\psi(x)$ è l'elemento di $\prod G_{i'}$ la cui componente i'-esima è uguale a $\phi_{i'}(x_{\phi(i')})$. Chiaramente ψ è un omomorfismo di gruppi topologici, quindi per restrizione definisce un omomorfismo

$$\widetilde{\Phi} : \varprojlim G_i \to \varprojlim G_{i'}$$

Definizione 1.8 (Gruppo profinito). *Un gruppo G si dice* profinito *se è isomorfo a $\varprojlim G_i$ per un certo sistema inverso (G_i) di gruppi finiti.*

Teorema 1.1. *Un gruppo topologico G è profinito se e solo se è compatto e totalmente disconnesso.*

In [6] troviamo il seguente risultato sui gruppi profiniti.

Teorema 1.2. *Se G è un gruppo topologico compatto e totalmente disconnesso e se U è un intorno dell'identità, allora esiste un sottogruppo normale e aperto H di G tale che H è contenuto in U e G/H è finito.*

1.2 Coomologia di un gruppo profinito

Sia G un gruppo profinito e A un G-modulo sinistro. Se U è un sottogruppo aperto di G denoteremo con A^U l'insieme dei punti di A fissi sotto l'azione di G.

Definizione 1.9. *Sia G un gruppo profinito. Un G-modulo A è un* modulo discreto *se*

$$A = \cup A^U$$

dove l'unione è fatta al variare di tutti i sottogruppi normali e aperti U di G.

Sia quindi A un G-modulo discreto e sia $(U_i, i \in I)$ la famiglia dei sottogruppi normali e aperti di G. Consideriamo su I l'ordine parziale $i \leq j \Leftrightarrow U_j \subseteq U_i$. Allora presi i, j qualunque $U_i \cap U_j$ è ancora un sottogruppo normale e aperto di G, quindi $(I, \leq)$ è un insieme diretto. Inoltre se $i \leq j$ si hanno mappe naturali

$$\delta_{ji} : G/U_j \to G/U_i$$

$$\epsilon_{ji} : A_i \to A_j$$

Consideriamo quindi, per q intero non negativo, la composizione delle seguenti mappe:

$$\begin{array}{ccccc} H^q(G/U_i, A_i) & \to & H^q(G/U_j, A_i) & \to & H^q(G/U_j, A_j) \\ f & \to & f \circ \delta_{ji} & \to & \epsilon_{ji} \circ f \circ \delta_{ji} \end{array} \tag{1}$$

Otteniamo così applicazioni

$$\lambda_{ij} : H^q(G/U_i, A_i) \to H^q(G/U_j, A_j)$$

che sono omomorfismi di G-moduli, e che ci permettono di considerare il sistema diretto di gruppi abeliani $(I, H^q(G/U_i, A_i), \lambda_{ij})$.

Definizione 1.10 (Coomologia di un gruppo profinito). *Dato un gruppo profinito G ed un G-modulo discreto A, il limite*

$$\widetilde{H}^q(G, A) = \varinjlim H^q(G/U_i, A_i)$$

è detto q-esimo gruppo di omologia di G a coefficienti in A.

Adesso vogliamo far vedere che la coomologia di un gruppo profinito così definita è effettivamente associata ad un complesso, e quindi gode di tutte le proprietà dei normali gruppi di coomologia. In particolare consideriamo gli insiemi $C^n = C^n(G, A)$ delle mappe continue di G^n in A, dove su A si considera sempre la topologia discreta. Daremo a $C^n(G, A)$ una struttura di G-modulo considerando l'azione

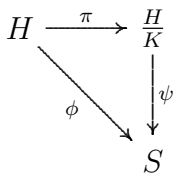
$$(g \cdot f)(g_1, \ldots, g_n) = g \cdot f(g_1, \ldots, g_n)$$

Definiamo una mappa di frontiera d nel seguente modo:

$$\begin{array}{rl} (df)(g_1, \ldots, g_{n+1}) = & g_1 f(g_2, \ldots, g_{n+1}) + \\ & + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) + \\ & + (-1)^{n+1} f(g_1, \ldots, g_n) \end{array} \tag{2}$$

Grazie a d abbiamo un complesso di G-moduli $C(G, A)$. Vorremmo dimostrare che la coomologia del gruppo profinito G come definita sopra coincide con quella del complesso $C(G, A)$. Per prima cosa useremo il seguente lemma.

Lemma 1.1. *Una mappa $\phi : H \to S$ dove H è un gruppo profinito e S è uno spazio discreto è continua se e solo se esiste un sottogruppo normale e aperto K ed una mappa ψ del gruppo finito H/K in S tale che commuti il diagramma*



Dim: ($\Leftarrow$) Supponiamo che esistano K e ψ come nel lemma. Allora ϕ si fattorizza come $\psi \circ \pi$. Devo dimostrare che allora ϕ è continua, cioè che la controimmagine di ogni punto è un insieme aperto di H. Sia quindi $p \in S$. Allora $\psi^{-1}(p)$ è un insieme finito perché è contenuto in H/K che è finito. Quindi

$$\phi^{-1}(p) = \pi^{-1}(\psi^{-1}(p)) = \bigcup_{g \in \psi^{-1}(p)} gK \tag{3}$$

che è aperto perché è unione finita di insiemi aperti.
($\Rightarrow$) Supponiamo ora che ϕ sia continua. Poiché G è compatto e ϕ continua, $\phi(G) \subseteq S$ sarà compatto e discreto e quindi finito. Dunque ϕ assume un numero finito di valori. Sappiamo dal teorema 1.2 che esiste un sottogruppo normale e aperto K di H tale che H/K è finito. Vogliamo far vedere che possiamo scegliere K in modo che se $\pi(h) = \pi(g)$ allora $\phi(h) = \phi(g)$. Dopodiché ottengo la tesi ponendo $\psi(\overline{h}) = \phi(h)$. Siano quindi $s_0, \ldots, s_n$ i valori assunti da ϕ, e poniamo $V_i = \phi^{-1}(s_i)$. Poiché ϕ è continua i V_i sono tutti aperti. Quindi, se $h \in V_i$, esiste un intorno aperto dell'identità U_h^i tale che $hU_h^i \subseteq V_i$, con hU_h^i aperti. Quindi

$$V_i = \bigcup_{h \in V_i} hU_h^i \tag{4}$$

Ma V_i è un sottoinsieme aperto di un compatto, quindi è anch'esso compatto, e pertanto posso scegliere punti $h_1^i, \ldots, h_{n_i}^i \in V_i$ tali che

$$V_i = \bigcup_{j=1}^{n_i} h_j^i U_j^i \tag{5}$$

e

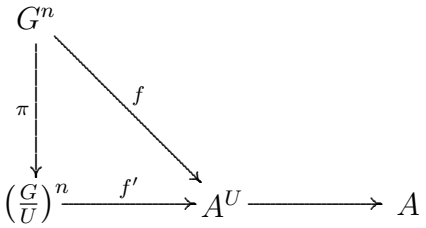
$$G = \bigcup_{i=1}^{n} \bigcup_{j=1}^{n_i} h_j^i U_j^i \tag{6}$$

Sia ora $U = \cap U_j^i$. Questo è un intorno aperto dell'identità, quindi per il teorema 1.2 possiamo scegliere un sottogruppo normale e aperto $K \subseteq U$ tale che H/K è finito. Vogliamo dimostrare che questo è il sottogruppo giusto. Siano quindi $h \in H$ e $k \in K$. Devo far vedere che $\phi(gk) = \phi(g)$. Per quanto scritto sopra e per definizione di K, avremo che esistono i, j tali che $g \in h_j^i U_j^i$ e $k \in U_j^i$. Allora $gk \in h_j^i U_j^i$, cioè $g, gk \in V_i$, e questo conclude la dimostrazione. □

Sia ora $f \in C^n(G, A)$, e sia $\{U_i\}$ la famiglia dei sottogruppi di G aperti e normali. Sappiamo dalla dimostrazione del lemma che f deve assumere un numero finito di valori, quindi essendo A un G-modulo discreto, abbiamo

$$im(f) \subseteq A^{U_1} \cap \ldots \cap A^{U_n} \subseteq A^{\cap U_i} \tag{7}$$

Ripercorrendo ancora la dimostrazione del lemma vediamo che possiamo scegliere $U \subseteq \cap U_i$ sottogruppo normale aperto di G tale che f si fattorizza. Ma allora $im(f) \subseteq A^{\cap U_i} \subseteq A^U$, e quindi possiamo scrivere



In questo modo a partire da $f \in C^n(G, A)$ ho ottenuto $f' \in C^n(G/U, A^U)$, per un certo U sottogruppo normale e aperto di G, e questo mi dà un'applicazione

$$C^n(G, A) \xrightarrow{\phi} \varinjlim C^n(G/U, A^U) \tag{8}$$

che è chiaramente un omomorfismo iniettivo di G-moduli. La surgettività discende direttamente dal lemma. Quindi effettivamente

$$C^n(G, A) \cong \varinjlim C^n(G/U, A^U) \tag{9}$$

A questo punto abbiamo complessi $C^n(G, A)$, $C^n(G/U, A^U)$, di cui possiamo calcolare i gruppi di coomologia. Per il teorema di Grothendieck abbiamo che la coomologia di G/U in A^U è proprio quella associata al complesso $C^n(G/U, A^U)$. Quindi, utilizzando l'equazione 9 abbiamo che

$$\begin{aligned} H^q(C^n(G, A)) \cong H^q(\varinjlim C^n(G/U, A^U)) \cong \varinjlim H^q(C^n(G/U, A^U)) \cong \\ \cong \varinjlim H^q(G/U, A^U) \cong \widetilde{H}^q(G, A) \end{aligned} \tag{10}$$

e questo dimostra quello che volevamo.

Per concludere la sezione, osserviamo che questa costruzione ci permette di parlare del gruppo di coomologia di un gruppo profinito G sia a partire dalla definizione classica, sia come limite diretto di gruppi di coomologia classici di quozienti di G. Questa duplicità di punti di vista permetterà, come vedremo, di calcolare la coomologia di G sfruttando sia proprietà note dei suoi quozienti, sia quelle di G come gruppo classico.

2 Il Teorema 90 di Hilbert

2.1 Gruppi profiniti in teoria dei campi

Sia E/F un'estensione di Galois di campi, e sia $G = Gal(E/F)$. Sia poi $(K_i, i \in I)$ la famiglia di tutte le estensioni di Galois finite di F contenute in E. Allora

$$E = \bigcup_i K_i$$

Infatti naturalmente $\cup K_i \subseteq E$. Inoltre se $x \in E$ allora la chiusura normale $\overline{F(x)}$ di $F(x)$ è un'estensione finita perché è ottenuta aggiungendo a F tutti i coniugati di x, che sono algebrici su F perché stanno in E. Inoltre $\overline{F(x)}/F$ è separabile perché è una sottoestensione di E. Quindi $x \in \overline{F(x)} \subseteq E$ ed è di Galois finita, e questo ci dà l'altra inclusione. Poniamo ora

$$G_i = Gal(K_i/F)$$

Vogliamo dimostare che i G_i, insieme ad un'opportuna famiglia di omomorfismi, formano un sistema inverso di gruppi, di cui è possibile calcolare il limite inverso. Osserviamo quindi:

(i) Se $K_i \subseteq K_j$ allora abbiamo un naturale omomorfismo tra gruppi di Galois $\pi_{ji} : G_j \to G_i$;

(ii) Se $i_1,\ i_2 \in I$, allora $K_{i_1}K_{i_2} = K_j$ per un certo $j \in I$, e quindi $K_{i_1},\ K_{i_2} \subseteq K_j$.

A questo punto per ottenere un sistema inverso basta prendere la terna (I, G_i, π_{ji}), dove su I consideriamo la relazione $i \leq j \Leftrightarrow K_i \subseteq K_j$. Con queste notazioni abbiamo la seguente:

Proposizione 2.1.

$$G = Gal(E/F) \ \cong \ \varprojlim G_i$$

dove l'isomorfismo è un isomorfismo di gruppi.

Dim: Per ogni $i \in I$ abbiamo un omomorfismo di gruppi $\theta_i : G \to G_i$. Questi inducono un omomorfismo di gruppi

$$\begin{array}{rccc} \theta : & G & \to & \prod_i G_i \\ & x & \to & (\theta_i(x)) \end{array} \tag{11}$$

Ovviamente $\theta(G) \subseteq L = \varprojlim G_i$. Facciamo vedere che θ definisce un isomorfismo di G con L.

Sia quindi $g \neq 1$ in G. Allora esiste $x \in E$ tale che $g(x) \neq x$, e supponiamo $x \in K_i$ per un certo i. Pertanto $(\theta(g))_i \in G_i$ manda x in $g(x)$, quindi $\theta(g)$ non è l'identità in $\prod G_i$. Dunque θ è iniettiva.

Sia ora (g_i) in L. Se $x \in E$ e $x \in K_i$, poniamo $g(x) = g_i(x)$. Questa è una buona definizione perché (g_i) sta in L, quindi se $K_i \cap K_j \neq$ allora g_i e g_j coincidono sull'intersezione. Quindi abbiamo ben definito una mappa da E in E che lascia fisso F. Ma chiaramente $\theta(g) = (g_i)$, quindi θ è anche surgettiva. □

Usiamo l'isomorfismo θ utilizzato nella dimostrazione della proposizione precedente per mettere una topologia su G. In questo modo $G = Gal(E/F)$ è un gruppo profinito, e se poniamo $U_i = Gal(E/K_i)$, (U_i) definisce un sistema fondamentale di intorni aperti di 1. Sappiamo come sono costruiti gli intorni aperti di 1 in $\prod_i G_i$. Consideriamo quindi l'applicazione composta

$$G \xrightarrow{\theta} \varprojlim G_i \to G_i$$

Allora un sistema fondamentale di intorni aperti di 1 sarà dato dai nuclei di queste applicazioni al variare di i. Ma, dato i, il nucleo di questa applicazione non è altro che gli elementi di G che sono l'identità sul campo fissato da G_i, cioè K_i, da cui si ottiene quello che volevamo.

2.2 Il Teorema 90 di Hilbert

Sia E/F un'estensione di Galois, $G = Gal(E/F)$. Sia $(K_i, i \in I)$ la famiglia delle estensioni finite di Galois di F contenute in E, e poniamo $U_i = Gal(E/K_i)$. Allora $G/U_i \cong Gal(K_i/F)$, quindi per la proposizione 2.1 si ha

$$G \cong \varprojlim G/U_i \tag{12}$$

Quindi, per la topologia indotta su G da questo isomorfismo e per la corripondenza di Galois, gli U_i sono sottogruppi aperti e normali di G. Inoltre l'azione di G fa di E un G-modulo, e poiché $E^{U_i} = K_i$ si ha che

$$E = \cup K_i = \cup E^{U_i} \subseteq \cup E^U \subseteq E \tag{13}$$

e quindi E è un G-modulo discreto. Ora possiamo calcolare la coomologia di E come G-modulo discreto. Inoltre K_i è un $Gal(K_i/F)$-modulo e $Gal(K_i/F) \cong G/U_i$, quindi abbiamo

$$H^q(G, E) \cong \varinjlim H^q(Gal(K_i/F), K_i) \tag{14}$$

Proposizione 2.2. *Se $q \geq 1$ allora*

$$H^q(G, E) = 0$$

Per l'equazione 14 basta dimostrare il risultato per estensioni finite, e quindi la proposizione 2.2 è diretta conseguenza del seguente lemma.

Lemma 2.1. *Sia E/F un'estensione finita di Galois con $G = Gal(E/F)$. Allora $H^q(G, E) = 0$ per ogni $q \geq 1$.*

Dim: Poiché E è un'estensione di Galois finita, allora ammette una base normale. Questo significa che esiste $x \in E$ tale che $E = F(x, \sigma_1(x), \ldots, \sigma_h(x))$ per certi $\sigma_1, \ldots, \sigma_h \in G$. Questo significa che E è libero come G-modulo, da cui segue la tesi. □

Consideriamo adesso il gruppo moltiplicativo E^* come G-modulo. Si ha chiaramente $(E^*)^{U_i} = K_i^*$, $E^* = \cup K_i^*$, e quindi E^* è un G-modulo discreto e

$$H^q(G, E^*) = \varinjlim H^q(Gal(K_i/F), K_i^*) \tag{15}$$

Proposizione 2.3.

$$H^1(G, E^*) = \{1\}$$

Dim: Osserviamo innanzitutto che per l'equazione 15 basta dimostrare l'asserto per estensioni finite di campi. Sia quindi f un 1-cociclo di G in E^*. Per il teorema sull'indipendenza dei caratteri deve esistere c tale che

$$b = \sum_{x \in G} f(x) \cdot x(c) \neq 0 \tag{16}$$

Applichiamo alla precedente equazione un elemento $y \in G$:

$$\begin{aligned} y(b) &= \sum\nolimits_{x \in G} [y(f(x))][yx(c)] = \\ &= \sum\nolimits_{x \in G} f(y)^{-1} f(yx) yx(c) = \\ &= f(y)^{-1} \sum\nolimits_{z \in G} f(z) z(c) = f(y)^{-1} b \end{aligned} \tag{17}$$

perché f è un cociclo quindi $f(yx) = f(y) \cdot y(f(x))$ (ricordarsi che stiamo usando la notazione moltiplicativa). Ma allora $f(y) = b \cdot y(b)^{-1}$, cioè f è un cobordo, e quindi si annulla come elemento di $H^1(G, E^*)$. □

Corollario 2.1 (Teorema 90 di Hilbert). *Sia $G = Gal(E/F)$ ciclico finito con generatore σ, e sia $a \in E^*$. Allora $Norm_{E/F}(a) = 1$ se e solo se esiste $b \in E^*$ tale che $a = b/\sigma(b)$.*

Dim: In generale, dato un gruppo ciclico finito $G =< \sigma >$ ed un G-modulo A, il primo gruppo di coomologia può essere calcolato considerando l'isomorfismo

$$H^1(G, A) \cong \frac{\{\alpha \in A \mid N\alpha = 0\}}{IA} = \frac{\{\alpha \in A \mid N\alpha = 0\}}{\{(1-\sigma)a \mid a \in A\}} \tag{18}$$

dove $N = \sum_{g \in G} g$ è la norma del gruppo, e I è l'ideale di augumentazione. In questo caso $A = E^*$, quindi usando la notazione moltiplicativa e ricordando la proposizione 2.3 si ottiene

$$H^1(G, E^*) \cong \frac{\left\{a \in E^* \mid Norm_{E/F}(a) = 1\right\}}{\{b/\sigma(b) \mid b \in E^*\}} = \{1\} \tag{19}$$

cioè la tesi. □

Corollario 2.2 (Teorema 90 di Hilbert-versione additiva). *Sia $G = Gal(E/F)$ ciclico finito con generatore σ e sia $a \in E$. Allora $Tr_{E/F}(a) = 0$ se e solo se esistono $b \in E$ e $g \in G$ tali che $a = b - g(b)$.*

Dim: Riscrivendo la 18 con $A = E$ ed utilizzando la notazione additiva si ha

$$H^1(G, E) \cong \frac{\left\{a \in E \mid Tr_{E/F}(a) = 0\right\}}{\{b - \sigma(b) \mid b \in E\}} = 0 \tag{20}$$

per il teorema 2.2. E questo prova il teorema. □

3 Alcune variazioni

Sia K un campo di numeri, cioè un'estensione finita del campo dei razionali, e sia $\gamma \in \mathbb{C}$ algebrico su K. Indicheremo con $Norm_{K(\gamma)}$ e $Tr_{K(\gamma)}$ rispettivamente la norma e la traccia di $K(\gamma)$ su K, e con N_γ la chiusura normale di $K(\gamma)$ su K. Inoltre poniamo $G_\gamma = Gal(N_\gamma/K)$. Infine, per $\sigma \in G_\gamma$ e $\delta \in N_\gamma$ definiamo

$$O(\sigma, \delta) = \{\tau(\delta) |\ \tau \in < \sigma >\}$$

$$P(\sigma, \delta) = \prod_{\delta' \in O(\sigma, \delta)} \delta'$$

$$S(\sigma, \delta) = \sum_{\delta' \in O(\sigma, \delta)} \delta'$$

Con queste notazioni abbiamo i due seguenti teoremi, che generalizzano le due versioni del Teorema 90 di Hilbert dimostrate nella precedente sezione.

Teorema 3.1. *Sia K un campo di numeri, e sia $\beta \neq 0$ algebrico su K. Allora β può essere scritto come quoziente α/α' con α e α' algebrici coniugati su K, se e soltanto se esiste $\sigma \in G_\beta$ tale che $P(\sigma, \beta)$ è una radice dell'unità.*

Inoltre, se questo è il caso, con $P(\sigma, \beta)$ radice l-esima dell'unità, $n = ord(\sigma)$, $m = |O(\sigma, \beta)|$ e $k = l/(l, n/m)$, allora α e α' possono essere scelti in modo che α^k stia in N_β.

Teorema 3.2. *Sia K un campo di numeri, e sia $\beta \neq 0$ algebrico su K. Allora β può essere scritto come differenza $\alpha - \alpha'$ con α e α' algebrici coniugati su K, se e soltanto se esiste $\sigma \in G_\beta$ tale che $S(\sigma, \beta) = 0$. Se tali α, α' esistono allora possono essere scelti in N_β.*

3.1 Conseguenze del teorema moltiplicativo

Corollario 3.1. *Sia K un campo di numeri e β algebrico su K. Supponiamo $|O(\sigma, \beta)| = deg(\beta)$ per qualche $\sigma \in G_\beta$ e che $Norm_K(\beta)$ sia una radice dell'unità. Allora $\beta = \alpha/\alpha'$, con α, α' algebrici coniugati.*

Corollario 3.2. *Sia K un campo di numeri e sia β algebrico su K. Supponiamo che $Norm_K(\beta)$ sia una radice dell'unità ma che nessun sottoprodotto di coniugati di β su K lo sia. Allora $\beta = \alpha/\alpha'$ con α, α' algebrici coniugati se e solo se G_β contiene un ciclo di lunghezza $deg(\beta)$.*

Abbiamo visto che la condizione $Norm_K(\beta)$ è necessaria affinché β sia scrivibile come quoziente di algebrici coniugati. Il prossimo esempio mostra che non è anche sufficiente.

Sia $K = \mathbb{Q}$ e sia $\beta = 1+\sqrt{2}+\sqrt{6}$, con coniugati $\beta_2 = 1-\sqrt{2}+\sqrt{6}$, $\beta_3 = 1+\sqrt{2}-\sqrt{6}$, $\beta_4 = 1-\sqrt{2}-\sqrt{6}$. Allora $Norm(\beta) = 1$, $N_\beta = \mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ e $|G_\beta = 4$. Le orbite $O(\sigma, \beta)$, al variare di $\sigma \in G_\beta$, sono $\{\beta\}$, $\{\beta, \beta_2\}$, $\{\beta, \beta_3\}$, $\{\beta, \beta_4\}$, con $P(\sigma, \beta)$ che assume rispettivamente i valori β, $5+2\sqrt{6}$, $-3+2\sqrt{2}$ e $-7+4\sqrt{3}$, nessuno dei quali è una radice dell'unità. Quindi β non può essere scritto come quoziente di algebrici coniugati, nonostante abbia norma 1.

Allo stesso modo si può dimostrare che $\beta = (2+\sqrt{3})(\sqrt{2}-1)(\sqrt{2}\sqrt{3})$, dove ognuno dei tre numeri alla destra dell'uguale sono esprimibili come quoziente di algebrici coniugati. Quindi in generale l'insieme dei numeri algebrici che godono di questa proprietà non formano un gruppo moltiplicativo.

3.2 Conseguenze del teorema additivo

Corollario 3.3. *Se $|O(\sigma, \beta)| = deg(\beta)$ per qulache $\sigma \in G_\beta$ e β ha traccia zero, allora $\beta = \alpha - \alpha'$ per certi $\alpha, \alpha' \in N_\beta$ coniugati su K.*

Corollario 3.4. *Supponiamo che β abbia traccia 0, ma che nessuna sottosomma propria di coniugati di β su K sia zero. Allora $\beta = \alpha - \alpha'$ per certi α, α' algebrici e coniugati su K se e solo se G_β contiene un ciclo di lunghezza $deg(\beta)$.*

4 Teoria di Kummer

Abbiamo visto che nel caso di estensioni di Galois cicliche finite il teorema 90 di Hilbert è perfettamente equivalente alla proposizione 2.3. In realtà a volte come teorema 90 si considera la stessa proposizione 2.3 (considerata però nel caso generale di estensioni di Galois qualunque), ed il risultato di Hilbert un suo corollario. È per questo che la teoria di Kummer che verrà illustrata in questa sezione viene spesso considerata conseguenza del teorema 90 di Hilbert, benché sfrutti non questo ma la proposizione 2.3.

Sia F un campo contenente il gruppo μ_n delle radici n-esime dell'unità, dove n è un intero primo con la caratteristica di F.

Definizione 4.1 (Estensione di Kummer). *Un'*estensione di Kummer *del campo F è un'estensione di F della forma $E = F(\sqrt[n]{\Delta})$, dove Δ indica un sottogruppo di F^* contenente il gruppo F^{*n} delle potenze n-esime.*

Osserviamo innanzitutto che un'estensione di Kummer E di un campo F è un'estensione abeliana di esponente n, cioè è di Galois con gruppo $Gal(E/F)$ abeliano tale che $\sigma^n = 1$ per ogni $\sigma \in Gal(E/F)$. Infatti se $E = F(\sqrt[n]{\Delta})$, allora E è generato da tutti gli elementi della forma $\sqrt[n]{a}$, con $a \in \Delta$. Inoltre la sottoestensione $F(\sqrt[n]{a})/K$ è ciclica di ordine che divide n, quindi $(\sigma|_{F(\sqrt[n]{a})})^n = 1$. Poiché questo vale per ogni $a \in \Delta$, abbiamo anche $\sigma^n = 1$.

Viceversa abbiamo la seguente

Proposizione 4.1. *Se E/F è un'estensione abeliana di esponente n, allora $E = F(\sqrt[n]{\Delta})$, con $\Delta = E^{*n} \cap F^*$.*

Dim: Chiaramente $F(\sqrt[n]{\Delta}) \subseteq E$. D'altra parte E/F è il composto di tutte le sue sottoestensioni cicliche. Infatti E/F è la composizione di tutte le sottoestensioni finite, ognuna delle quali è galoisiana con gruppo di Galois abeliano finito, che quindi è prodotto diretto di sottogruppi ciclici. Ma ad ognuno di questi corrisponde una sottoestensione ciclica finita di E/F. A questo punto basta fare il composto di tutte queste sottoestensioni per riottenere E/F. Sia ora M/F una sottoestensione ciclica di E/F. Allora $Gal(M/F)$ ha ordine che divide n, quindi $M = F(\sqrt[n]{a})$ per un certo $a \in E^{*n} \cap F^*$. Quindi $M \subseteq F(\sqrt[n]{\Delta})$ per ogni sottoestensione ciclica di E, da cui la tesi. □

Abbiamo così ottenuto che le estensioni di Kummer di F sono tutte e sole le estensioni abeliane di un certo esponente n. Il teorema che dimostreremo adesso è il contenuto principale di quella che viene detta *teoria di Kummer*.

Teorema 4.1. *Le estensioni di Kummer E/F sono in corrispondenza biunivoca con i sottogruppi Δ di F^* contenenti F^{*n}. Se $E = F(\sqrt[n]{\Delta})$ allora $\Delta = E^{*n} \cap F^*$, ed abbiamo un isomorfismo canonico*

$$Char(Gal(E/F)) = \{\text{omomorfismi continui } \chi : Gal(E/F) \to \mu_n\} \cong \Delta/F^{*n}$$

che associa ad un elemento $a \in \Delta/F^{*n}$ il carattere $\chi_a : Gal(E/F) \to \mu_n$ definito da

$$\chi_a(\sigma) = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$$

Dim: Sia E/F un'estensione di Kummer. Allora per la prop 4.1 $E = F(\sqrt[n]{\Delta})$, dove $\Delta = E^{*n} \cap F^*$. Definiamo l'omomorfismo

$$\begin{array}{ccc} \Delta & \stackrel{\psi}{\to} & Char(G) \\ a & \to & \chi_a \end{array} \tag{21}$$

dove χ_a è definito come nel testo del teorema e $G = Gal(E/F)$. Controlliamo innanzitutto che l'applicazione ψ sia ben definita, cioè che χ_a così definito sia effettivamente un omomorfismo continuo da G in μ_n. Chiaramente $\chi_a(\sigma)$ è una radice n-esima dell'unità, infatti

$$\chi_a(\sigma)^n = \frac{\sigma(\sqrt[n]{a})^n}{\sqrt[n]{a}} = \frac{\sigma(a)}{a} = 1 \tag{22}$$

perché $a \in F$, quindi $\sigma(a) = a$. Inoltre, visto che per ogni $\sigma \in G$ e per ogni $a \in \Delta$ si ha $\sigma(\sqrt[n]{a}) = \zeta\sqrt[n]{a}$ per una certa radice dell'unità $\zeta \in \mu_n \subseteq F$, possiamo scrivere

$$\begin{aligned} \chi_a(\sigma\tau) = \tfrac{\sigma\tau(\sqrt[n]{a})}{\sqrt[n]{a}} = \tfrac{\sigma\tau(\sqrt[n]{a})}{\tau(\sqrt[n]{a})}\tfrac{\tau(\sqrt[n]{a})}{\sqrt[n]{a}} = \tfrac{\sigma(\zeta\sqrt[n]{a})}{\zeta\sqrt[n]{a}}\tfrac{\tau(\sqrt[n]{a})}{\sqrt[n]{a}} = \\ = \tfrac{\sigma(\zeta)}{\zeta}\tfrac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}\tfrac{\tau(\sqrt[n]{a})}{\sqrt[n]{a}} = \chi_a(\sigma)\chi_a(\tau) \end{aligned} \tag{23}$$

e quindi χ_a è effettivamente un omomorfismo per ogni $a \in \Delta$. Vediamo se è anche continuo. Poiché su μ_n si considera la topologia discreta, basta controllare che l'insieme $\chi_a^{-1}(\zeta)$ sia aperto per ogni $\zeta \in \mu_n$. Sia quindi $\sigma \in \chi_a^{-1}(\zeta)$. Vogliamo dimostrare che l'intorno di σ dato dall'insieme aperto $\sigma Gal(E/F(\sqrt[n]{a}))$ è tutto contenuto in $\chi_a^{-1}(\zeta)$. Ma questo è banale perché se τ sta in $Gal(E/F(\sqrt[n]{a}))$ allora

$$\sigma\tau(\sqrt[n]{a}) = \sigma(\sqrt[n]{a})) = \zeta\sqrt[n]{a} \Rightarrow \sigma\tau \in \chi_a^{-1}(\zeta) \tag{24}$$

Così abbiamo dimostrato che χ_a è un omomorfismo continuo per ogni $a \in \Delta$, e pertanto ψ è ben definita come applicazione. Inoltre $\chi_{ab} = \chi_a \chi_b$, quindi ψ è anche un omomorfismo di gruppi. Il nucleo di ψ è chiaramente F^{*n} perché $\chi_a = 1 \Leftrightarrow \sigma(\sqrt[n]{a}) = \sqrt[n]{a}$ per ogni $\sigma \in G \Leftrightarrow \sqrt[n]{a} \in F^* \Leftrightarrow a \in F^{*n}$. Quindi ψ induce un omomorfismo iniettivo

$$\overline{\psi} : \frac{\Delta}{F^{*n}} \to Char(G)$$

Proviamo adesso che $\overline{\psi}$ così ottenuto è suriettivo prima nel caso in cui E/F sia finita. Sia $\chi \in Char(G)$. Allora $\chi(\sigma\tau) = \chi(\sigma)\chi(\tau) = \chi(\sigma)\sigma(\chi(\tau))$ perché $\chi(\tau) \in \mu_n \subseteq F^*$. Quindi χ è un elemento di $H^1(G, E^*)$, che è banale per il teorema 90 di Hilbert. Quindi esisterà $b \in E^*$ tale che

$$\chi(\sigma) = \frac{\sigma(b)}{b} \quad \forall \sigma \in G \tag{25}$$

Poiché $\sigma(b^n) = \sigma(b)^n = \chi(\sigma)^n b^n = b^n$ per ogni $\sigma \in G$, allora $a = b^n \in F^* \cap E^{*n}$, da cui abbiamo la suriettività nel caso finito.
In generale, siano Δ_i/F^* i sottogruppi finiti di Δ/F^*, e poniamo $E_i = F(\sqrt[n]{\Delta_i})$. Allora

$$\frac{\Delta}{F^*} = \bigcup_i \frac{\Delta_i}{F^*} \text{ e } E = \bigcup_i E_i$$

Quindi i gruppi $Gal(E/E_i)$ formano una base di intorni aperti di 1 in G, ed allora il nucleo di $\chi \in Char(G)$, che è aperto perché è la controimmagine di 1, deve contenere un sottogruppo $Gal(E/E_i)$ per un certo i. Possiamo quindi considerare l'omomorfismo continuo $\overline{\chi} : Gal(E/E_i) \to \mu_n$ tale che $\overline{\chi}(\sigma|_{E_i}) = \chi(\sigma)$. Ma allora per quanto già dimostrato per estensioni finite si ha

$$\chi(\sigma) = \overline{\chi}(\sigma|_{E_i}) = \chi_a(\sigma|_{E_i}) = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} = \chi_a(\sigma) \tag{26}$$

per un certo $a \in \Delta/F^{*n}$.

Abbiamo quindi ottenuto l'isomorfismo che cercavamo. Resta da dimostrare soltanto che le estensioni di Kummer di F sono in corrispondenza biunivoca con i sottogruppi Δ di F^* che contengono F^{*n}. Consideriamo quindi la mappa che associa ad un tale sottogruppo Δ l'estensione di Kummer $F(\sqrt[n]{\Delta})$. Per definizione di estensione di Kummer tale mappa è surgettiva. Per dimostrare che è iniettiva basta far vedere che se $E = F(\sqrt[n]{\Delta})$, allora $\Delta = E^{*n} \cap F^*$. Poniamo $\Delta' = E^{*n} \cap F^*$. Per quanto abbiamo appena dimostrato abbiamo che

$$\frac{\Delta'}{F^{*n}} \cong Char(G) \tag{27}$$

Attraverso questo isomorfismo il sottogruppo $\Delta/F^{*n} \subseteq \Delta'/F^{*n}$ corrisponde al sottogruppo $Char(G/H) \leq Char(G)$ dove

$$H = \{\sigma \in G \mid \chi_a(\sigma) = 1 \ \ \forall a \in \Delta\}$$

Ma poiché $\sigma(\sqrt[n]{a}) = \chi_a(\sigma)\sqrt[n]{a}$, si vede che H lascia fissi gli elementi di $\sqrt[n]{\Delta}$. Ma $\sqrt[n]{\Delta}$ genera E su F, quindi deve essere $H = 1$, cioè $\Delta = \Delta'$. □

Sia ora $\overline{F}$ la chiusura separabile del campo F (in particolare sarà normale, perché se un elemento algebrico su F è separabile, anche tutti i suoi coniugati lo sono), ed indichiamo con G il gruppo $Gal(\overline{F}/F)$. Abbiamo la successione esatta corta

$$1 \to \mu_n \to \overline{F} \xrightarrow{n} \overline{F}^* \to 1 \tag{28}$$

da cui si ottiene la successione esatta di gruppi di coomologia

$$F^* \xrightarrow{n} F^* \to H^1(G, \mu_n) \to H^1(G, \overline{F}^*) = 1 \tag{29}$$

dove l'ultima uguaglianza è conseguenza della proposizione 2.3. Abbiamo quindi un isomorfismo

$$H^1(G, \mu_n) \cong \frac{F^*}{F^{*n}} \tag{30}$$

Osserviamo adesso che il composto di due estensioni di Kummer è ancora un'estensione di Kummer, e che tutte le estensioni di Kummer di esponente n sono contenute nell'estensione *massimale* $\widetilde{F} = F(\sqrt[n]{F^*})$. Concludendo

$$Char(Gal(\widetilde{F}/F)) \cong \frac{F^*}{F^{*n}} \cong H^1(G, \mu_n) \tag{31}$$

da cui per dualità otteniamo il seguente

Teorema 4.2. *Se $n \geq 1$ è primo con la caratteristica di F e $\mu_n \subseteq F$, allora*

$$Gal(\widetilde{F}/F) \cong Hom(F^*/F^{*n}, \mu_n)$$

Riferimenti bibliografici

[1] Cassels, J. W. S.; Frölich, A.: *Algebraic Number Theory*, Academic Press, London and New York, 1967

[2] Dubickas, A.; Smith, C. J.: *Variation on the theme of Hilbert's Theorem 90*, Glasgow Mathematical Journal, No. 44, 2002, pp. 435-441

[3] Neukirch, J: *Class Field Theory*, Springer-Verlag Berlin, 1986

[4] Neukirch, J; Schmidt, A.; Wingberg, K.: *Cohomology of Number Fields*, Springer-Verlag Berlin Heidelberg, 2000

[5] Bourbaki, N.: *Algèbre*, Capitolo 5, Hermann Paris, 1959

[6] Montgomery, D.; Zippin, L.: *Topological transformation groups*, Interscience Publishers Inc., New York and London, 1955