Seminario di Algebra III, a.a. 2008/2009

Il teorema di Wedderburn per i corpi finiti

Giulio Battaglia

12 marzo 2009

Ricordiamo che un corpo (o anello con divisione) è un anello R in cui ogni elemento non zero ammette inverso in R.
Nel 1905 Wedderburn dimostrò il teorema per cui un corpo finito è necessariamente commutativo, ossia è un campo. A pensarci bene, questo risultato è del tutto inaspettato, perché lega due proprietà di un sistema algebrico, il suo numero di elementi e la moltiplicazione nel sistema stesso, apparentemente non correlate.
In questo seminario daremo una dimostrazione, prima del teorema di Wedderburn, poi di un risultato più generale dovuto a T. Grundhöfer, che permette di derivare il teorema di Wedderburn come corollario. Entrambe le dimostrazioni fanno uso della teoria dei polinomi ciclotomici, sviluppata nel capitolo 6 del corso. Faremo inoltre largo uso, a volte generalizzandoli, dei teoremi enunciati nel capitolo 7 sui campi finiti. Altro punto cardine di entrambe le dimostrazioni è costituito dall'equazione delle classi, dedotta nel corso di Algebra I a partire dalla relazione di coniugio su un gruppo, concetti che andremo ora a richiamare.

Richiami 1 (Un metodo di enumerazione)**.** Su un gruppo G definiamo la *relazione di coniugio* come segue: $a \sim b \Leftrightarrow \exists\, c \in G \quad \textit{tale che} \quad b = c^{-1}ac$.
Poiché si verifica facilmente essere una relazione di equivalenza, possiamo considerarne le classi di equivalenza (dette in questo caso classi di coniugio) che, come sappiamo, costituiscono una partizione di G.
Dunque, se indichiamo con n_a la cardinalità della classe di equivalenza di a, $[a]$, si ha:

$$|G| = \sum_{[a]} n_a \tag{1}$$

per opportuni $a \in G$, uno per ogni classe di equivalenza.

Vogliamo calcolare n_a. A tal fine, diamo la seguente definizione:
Sia $a \in G$. Si definisce *centralizzatore di a in G* l'insieme degli elementi di G che commutano con a: $C(a) = \{x \in G \,|\, xa = ax\}$.
Si dimostra facilmente che $C(a)$ è un sottogruppo di G; inoltre, se G è un gruppo finito, sussiste l'uguaglianza: $n_a = \frac{|G|}{|C(a)|}$ [MV Proposition 16.23]. Da tale proposizione, sostituendo in (1), otteniamo come corollario la seguente equazione (nota su alcuni testi come *equazione delle classi*):

$$|G| = \sum_{[a]} \frac{|G|}{|C(a)|}$$

dove la somma è estesa ad elementi a di G, uno per ogni classe di coniugio.
Dato un gruppo G, definiamo infine *centro di G* l'insieme degli elementi di G che commutano con ogni elemento del gruppo: $Z = \{z \in G | zx = xz \ \forall x \in G\}$.
Si verifica facilmente essere anch'esso un sottogruppo (abeliano) di G. Inoltre dato $z \in Z$, poiché esso commuta con ogni elemento di G , si ha che $c^{-1}zc = z$ per ogni $c \in G$, il che implica che $n_z = 1$ per ogni $z \in Z$ (infatti $n_z = \frac{|G|}{|C(z)|}$ e $|C(z)| = |G|$).
Possiamo allora riscrivere l'equazione delle classi come:

$$|G| = |Z| + \sum_{[a] \subseteq G \backslash Z} \frac{|G|}{|C(a)|} \tag{2}$$

per opportuni $a \in G \backslash Z$, uno in ogni classe di equivalenza (si osservi che $[a] \subset G \backslash Z$ per ogni $a \in G \backslash Z$).

Possiamo ora passare al risultato principale del seminario. Le nozioni introdotte costituiscono il ponte che cercavamo tra l'operazione di moltiplicazione definita su un gruppo e il numero di elementi del gruppo.
É da questi concetti che muoveremo i primi passi della dimostrazione.

Teorema 2 (Wedderburn)**.** *Sia K un corpo finito. Allora K è un campo.*

Dimostrazione. Sia $Z = \{z \in K | zx = xz \ \forall x \in K\}$ il centro di K. Si osserva facilmente che Z è un sottocorpo di K.
Infatti $1 \in Z$ (dunque Z è non vuoto) e, dati $y, z \in Z$: $(y - z)x = yx - zx = xy - xz = x(y - z)$. Questo dimostra che Z è un sottogruppo del gruppo additivo $(K, +, 0)$. Inoltre, dal sussistere delle relazioni:

$$\forall\, y, z \in Z \quad yzx = yxz = xyz$$

$$\forall\, z \in Z \backslash \{0\} \quad z^{-1}x = z^{-1}xzz^{-1} = z^{-1}zxz^{-1} = xz^{-1}$$

abbiamo che yz e z^{-1} appartengono a Z, da cui segue che Z^* è anche sottogruppo del gruppo moltiplicativo $(K^*, \cdot\,, 1)$. Poichè per definizione di Z

tale sottogruppo è commutativo, Z, con la struttura indotta dal corpo K, è un campo. Trattandosi di un campo finito, da 7.2, 7.3, 7.4 segue che $|Z| = q$, dove $q = p^s$ con p numero primo e $s \in \mathbb{N}\backslash\{0\}$. Inoltre per Teorema 7.10 $Z \cong \mathbb{F}_q$.
Ora, possiamo riguardare K come uno spazio vettoriale sul campo Z. É allora lecito applicare il lemma 7.2 prendendo $''K'' = Z$ e $''F'' = K$, anche se quest'ultimo non è un campo. Ciò che di necessario richiede la dimostrazione è infatti il poter dotare F di una struttura di K-spazio vettoriale.
Ancora per il lemma 7.2, se Z ha q elementi, allora K ha q^n elementi, con $n = [K : Z]$. Nostro scopo sarà dimostrare che Z coincide con K, o equivalentemente che $n = 1$.
Sia $a \in K$, e sia $C(a) = \{x \in K \,|\, xa = ax\}$ il centralizzatore di a in K. Ovviamente $C(a)$ contiene Z ($z \in Z$ commuta con ogni elemento di K, in particolare con a). In maniera analoga a quanto fatto per Z, si dimostra che $C(a)$ è un sottocorpo di K, in particolare è un gruppo abeliano rispetto all'operazione di addizione. É quindi possibile considerare $C(a)$ come uno spazio vettoriale su Z. Sempre per il lemma 7.2, $C(a)$ contiene allora $q^{n(a)}$ elementi, per qualche intero $n(a)$.
Mostriamo che $n(a)|n$. Si ha che gli elementi non nulli di $C(a)$ formano un sottogruppo di ordine $q^{n(a)} - 1$ del gruppo moltiplicativo K^*, avente $q^n - 1$ elementi. Dal teorema di Lagrange (per il quale dato un gruppo finito G e un sottogruppo $H \leqslant G$ si ha che $|H|\big||G|$) segue quindi che $q^{n(a)} - 1|q^n - 1$, da cui, per il lemma 7.17 $n(a)|n$ (nell'enunciato del lemma si richiede che q sia un numero primo, cosa che nel nostro caso non è vera; si osserva tuttavia che tale richiesta risulta superflua ai fini della dimostrazione).
Consideriamo ora, nel gruppo degli elementi non nulli di K, la relazione di coniugio introdotta all'inizio del seminario. Mantenendo le notazioni dei richiami, abbiamo allora che per ogni $a \in K^*$:

$$n_a = \frac{|K^*|}{|C(a)^*|} = \frac{q^n - 1}{q^{n(a)} - 1}$$

Ricordiamo ancora che $a \in Z \Leftrightarrow |C(a)| = |K| \Leftrightarrow n(a) = n \Leftrightarrow n_a = 1$.
Inserendo i risultati ottenuti finora nell'equazione (2), otteniamo:

$$q^n - 1 = q - 1 + \sum_{\substack{n(a)|n \\ n(a)\neq n}} \frac{q^n - 1}{q^{n(a)} - 1} \tag{3}$$

dove $q - 1 = |Z^*| = \sum_{z\in Z^*} n_z$. Riguardo agli indici sotto il simbolo di sommatoria nella (3), specifichiamo che gli interi $n(a)$ sono sempre vincolati alla condizione su a (un elemento per ogni classe di coniugio di $K\backslash Z$). Ci siamo così ridotti a dover dimostrare che l'equazione (3) non può valere per $n > 1$ (per $n = 1$ è chiaramente vera in quanto $\{n(a)\Big|n(a)|n \wedge n(a) \neq n\} = \varnothing$).

Finora abbiamo ricalcato la dimostrazione originale di Wedderburn. Il seguito della dimostrazione è dovuto a E. Witt (in un articolo del 1931), ed è qui che entrano prepotentemente in gioco i nuovi strumenti appresi durante il corso. Ciò che faremo sarà trovare un intero che divide $\frac{q^n-1}{q^{n(a)}-1}$ *per tutti gli* $n(a)$ *tali che* $n(a)|n$ *e* $n(a) \neq n$*, ma che non divide il termine* $q-1$*. Fatto ciò, l'equazione (3) sarà impossibile a meno di scegliere* $n = 1$*, e il teorema di Wedderburn sarà così dimostrato.*

Consideriamo l'n-esimo polinomio ciclotomico sul campo dei numeri razionali (per il lemma 6.5 ciò è possibile per ogni naturale positivo n, in quanto $char(\mathbb{Q}) = 0 \Rightarrow P_n \neq \varnothing$).
Per avere le idee chiare sulla struttura di questo polinomio, consideriamo la fattorizzazione di $X^n - 1$ in $\mathbb{C}[X]$:

$$X^n - 1 = \prod_{k=1}^{n} (X - \lambda_k) \tag{4}$$

dove $\lambda_k = e^{i\frac{2k\pi}{n}}$. Di queste radici, le radici primitive n-esime dell'unita sono tutti e soli i λ_k tali che $(n, k) = 1$, e l'n-esimo polinomio ciclotomico è proprio:

$$\phi_n = \prod_{\substack{1 \leqslant k \leqslant n \\ (k,n)=1}} (X - e^{i\frac{2k\pi}{n}})$$

Argomentando in maniera più astratta, tali radici esistono perché
$A = \{x \in \mathbb{C} \,|\, x^n = 1\}$ è un sottogruppo finito di $\mathbb{C}^*$. In base alla proposizione 5.2 A è allora ciclico, e ogni suo generatore è una radice primitiva n-esima dell'unità. Nella proposizione 6.10 abbiamo visto che $\phi_n(X)$ è un polinomio monico a coefficienti interi, conseguenza del fatto che, raggruppando le radici dello stesso ordine nella (4) possiamo scrivere:

$$X^n - 1 = \prod_{d|n} \phi_d(X) \tag{5}$$

unito a un semplice ragionamento induttivo.
Affermiamo ora che, per ogni divisore d di n, $d \neq n$, si ha che:

$$\phi_n(X) \left| \frac{X^n - 1}{X^d - 1} \right. \tag{6}$$

nel senso che il quoziente è un polinomio $f(X)$ a coefficienti interi. Infatti, dato che $X^d - 1 = \prod_{k|d} \phi_k(X)$, e che ogni divisore di d è anche divisore di n, raggruppando i termini nel secondo membro dell'equazione (5), otteniamo a destra il termine $X^d - 1$. Inoltre, essendo $d < n$, $X^d - 1$ non contiene $\phi_n(X)$. Pertanto $X^n - 1 = \phi_n(X)(X^d - 1)f(X)$, dove

$$f(X) = \prod_{k} \phi_k(X)$$

(con k tale che $k|n$, $k \nmid d$, $k \neq n$), è chiaramente un polinomio a coefficienti interi (i fattori $\phi_k(X)$ che lo compongono lo sono). Ciò dimostra la nostra asserzione. In particolare, la relazione (6) sussiste se ad X sostituiamo l'intero q; questo fatto, in riferimento all'equazione (3) ci porta ad affermare che $\phi_n(q) \,\Big|\, \frac{q^n-1}{q^{n(a)}-1}$ e $\phi_n(q) \,\big|\, (q^n-1)$.
Ora, $\phi_n(q) = \prod(q-\lambda_k)$, con $\lambda_k = e^{i\frac{2k\pi}{n}}$ che varia su tutte le radici primitive n-esime dell'unità. Poiché per ogni $\lambda_k \neq 1$ (i.e. per $k \neq n$) si ha:

$$|q-\lambda_k| = \sqrt{\left(q-\cos\left(\frac{2k\pi}{n}\right)\right)^2 + \left(0-\sin\left(\frac{2k\pi}{n}\right)\right)^2} > \sqrt{(q-1)^2} = q-1$$

otteniamo che $|\phi_n(q)| = \prod |q-\lambda_k| > q-1$. Abbiamo allora concluso, poichè è evidente che $\phi_n(q) \nmid q-1$, il che, per $n > 1$, costituisce una contraddizione della (3).
Dunque $n = 1$ è il solo caso accettabile. $\square$

Un'interessante applicazione del teorema di Wedderburn riguarda la geometria proiettiva. Si dimostra come le note configurazioni di Pappo e di Desargues, che caratterizzano quelle classi di piani proiettivi che soddisfano gli omonimi teoremi, siano legate all'esistenza di isomorfismi tra tali piani e i piani proiettivi numerici $\mathbb{P}^n(K)$; in tal caso un piano proiettivo si dice coordinabile su K. Per la precisione, un piano proiettivo è desarguesiano se e solo se è coordinabile su un corpo, mentre è pappiano se e solo se è coordinabile su un campo. Dunque, la validità del teorema di Pappo in un piano proiettivo implica quella del teorema di Desargues, ma in generale non è vero il viceversa. Nel caso in cui K sia un corpo finito il teorema di Wedderburn assicura che K è un campo, ovvero la completa simmetria tra le due configurazioni. [1]

Esercizio 3. Sul modello dei quaternioni reali (esempio di corpo sul campo dei numeri reali che non è un campo), definiamo i quaternioni sugli interi modulo p come:

$$H_p = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \big| \alpha_i \in \mathbb{Z}_p\}$$

Mostrare che si tratta di un anello con p^4 elementi che non ha ideali distinti da $\{0\}$ e dall'anello stesso.
Dimostrare che questo anello non è un corpo.

Il prossimo e ultimo passo consisterà nel dimostrare un teorema che generalizza il teorema di Wedderburn [2]*, fissando l'attenzione sulle proprietà del*

[1] Per maggiori dettagli rimandiamo al testo [6].
[2] il resto del seminario è tratto dall'articolo [2] di bibliografia.

gruppo K^* che ci hanno permesso di dedurre la tesi. Per fare questo passo necessitiamo però di alcune premesse.

Notazioni 4. Sia $A = \{a_1, \ldots, a_n\}$ un sottoinsieme non vuoto di $\mathbb{N}$, di cardinalità finita. Con $mcm(A)$ indicheremo il numero naturale $mcm(a_1, \ldots, a_n)$. Analoga posizione verrà assunta per il massimo comun divisore.

Lemma 5. *Sia G un gruppo finito, con centro Z, e sia $S = \{|C(g)| \big| g \in G \backslash Z\}$ l'insieme di tutti gli ordini dei centralizzatori di elementi "non centrali" di G. Allora:*

$$|G| \,\Big|\, |Z| \cdot mcm(S) \,\Big|\, MCD(S) \cdot mcm(S) \tag{7}$$

Osservazione 6. Per ogni $g \in G$ si ha $|C(g)| \geq 1$, dal momento che l'unità di G commuta con ogni elemento di del gruppo. Si osservi inoltre che nel caso in cui G sia commutativo $S = \varnothing$, e il lemma è vuoto.

Dimostrazione. Consideriamo l'equazione delle classi, (2). Per definizione di minimo comune multiplo, dal fatto che $|C(g)| \,\big|\, |G|$ per ogni $g \in G$, segue che $mcm(S) \,\big|\, |G|$. Allora esiste $k \in \mathbb{N}$ tale che:

$$|G| = mcm(S) \cdot k \Longrightarrow k = \frac{|G|}{mcm(S)} \,\Bigg|\, |G|$$

Inoltre, per ogni $g \in G$:

$$\frac{|G|}{mcm(S)} \,\Bigg|\, \frac{|G|}{|C(g)|}$$

Infatti $mcm(S) = k_g|C(g)|$ per definizione, da cui $\frac{|G|}{|C(g)|} = k_g \frac{|G|}{mcm(S)}$.
In base all'equazione (2) si deve allora avere che $\frac{|G|}{mcm(S)} \,\Big|\, |Z|$, e la prima relazione è dimostrata. La seconda relazione è un'immediata conseguenza della definizione di massimo comun divisore, tenuto conto del fatto che $|Z| \big| |C(g)|$ per il teorema di Lagrange (dopo aver osservato che Z è sottogruppo di $|C(g)|$ per ogni $g \in G$). $\square$

Osservazione 7. Da questo lemma segue che ogni p-gruppo, ossia un gruppo di cardinalità un potenza di p, ha centro non banale (teorema di *Burnside*). Infatti, se fosse $|Z| = 1$, in base alla (7) avremmo che $|G| = p^n \big| mcm(S)$, il che implicherebbe (avendo visto nella dimostrazione che si ha sempre $mcm(S) \big| |G|$) l'uguaglianza $mcm(S) = |G| = p^n$. Ma dall'essere la cardinalità dei centralizzatori di elementi non centrali strettamente minore di p^n, segue che $mcm(S) = p^s$, con $s < n$. Un assurdo. [3]

[3] Una altrettanto immediata dimostrazione si ottiene, sempre ragionando per assurdo, considerando l'equazione (2).

Teorema 8. *Un gruppo finito G è abeliano se e solo se esistono $q \in \mathbb{N}$ e, per ogni $g \in G$ un numero naturale $n(g)$, tali che $|C(g)| = q^{n(g)} - 1$.*

Dimostrazione. $\Rightarrow$) Se G è un gruppo abeliano, basta porre $q = |G| + 1$ e $n(g) = 1$.
$\Leftarrow$) Consideriamo un gruppo finito G che soddisfa alle condizioni sull'ordine dei centralizzatori. Sia $n = n(1)$, e sia Z il centro di G. Per ogni $g \in G \backslash Z$ l'intero $q^{n(g)} - 1$ è un divisore proprio di $|G| = |C(1)| = q^n - 1$,
($q^{n(g)} - 1 = |C(g)|$ e $|C(g)| \big| |G|$ per il teorema di Lagrange). Ma allora, per il lemma 7.17 (generalizzato a p arbitrario) $n(g)$ è un divisore proprio di n. Sia $e = MCD\{n(g) | g \in G\}$. Per definizione di massimo comun divisore, poiché $n(g)|n$ per ogni $g \in G$, possiamo scrivere $e = MCD\{n(g)|g \in G\backslash Z\}$. Possiamo sempre assumere che sia $e = 1$; qualora ciò non fosse, basta infatti sostituire q con q^e (osserviamo come, in questo modo, q risulti univocamente determinato).
Affermiamo ora che, comunque presi due numeri naturali a, b, si ha:

$$MCD(q^a - 1, q^b - 1) = q^{MCD(a,b)} - 1$$

Infatti, per il lemma 7.17 $q^{MCD(a,b)} - 1$ divide $q^a - 1$ e $q^b - 1$. Rimane da verificare che, preso un intero x tale che $x|q^a - 1$ e $x|q^b - 1$, allora x divide $q^{MCD(a,b)} - 1$. Ricordiamo che una proprietà del massimo comun divisore tra due numeri a e b è il poter essere scritto come combinazione lineare di tali numeri, ossia esistono λ,μ interi tali che $MCD(a, b) = \lambda a + \mu b$ [MV Corollary 10.27]. Possiamo quindi scrivere:

$$q^{MCD(a,b)} - 1 = q^{\lambda a + \mu b} - 1 = q^{\lambda a} q^{\mu b} - 1 = (q^{\lambda a} - 1)q^{\mu b} + q^{\mu b} - 1$$

E, dal momento che $x|q^{\lambda a} - 1$ e $x|q^{\mu b} - 1$, concludiamo che $x|q^{MCD(a,b)} - 1$, e la nostra affermazione è dimostrata. In base a queste considerazioni otteniamo:

$$MCD\{q^{n(g)} - 1 | g \in G\backslash Z\} = q^{MCD\{n(g)|g \in G\backslash Z\}} = q - 1 \tag{8}$$

Come nella dimostrazione di Witt, consideriamo a questo punto l'n-esimo polinomio ciclotomico, $\phi_n(X)$. Dall'equazione (5), valutando in q abbiamo che:

$$q^n - 1 = \prod_{d|n} \phi_d(q)$$

Ora, tenendo conto di tale uguaglianza, possiamo osservare che si ha

$$\phi_n(q) \left| \frac{q^n - 1}{mcm\{q^{n(g)} - 1 | g \in G\backslash Z\}} \right. \tag{9}$$

Questa relazione non salta all'occhio facilmente, ma mettiamoci in un campo di spezzamento di $X^n - 1$ (che contiene anche le radici di $X^{n(g)} - 1$ e di $\phi_n(X)$), e ragioniamo sulle radici di tali polinomi. Ogni radice del polinomio

$mcm\{X^{n(g)} - 1 | g \in G \backslash Z\}$ è anche radice di un certo $X^{n(g)} - 1$, ed essendo $n(g) < n$, tra di esse non possono comparire quelle di ϕ_n, che sono tutte e sole le radici primitive n-esime dell'unità. Per ottenere la formula (9) basta sostituire q alla variabile X nella relazione così ottenuta. Poiché $q^n - 1 = |G|$ e, per il lemma, $|G| \big| MCD\{q^{n(g)} - 1 | g \in G \backslash Z\} \cdot mcm\{q^{n(g)} - 1 | g \in G \backslash Z\}$, dalla (9) otteniamo:

$$\phi_n(q) \big| MCD\{q^{n(g)} - 1 | g \in G \backslash Z\} = q - 1$$

Potendo supporre $q > 1$ (altrimenti si avrebbe $|G| = q^n - 1 = 0$), si ha $|\phi_n(q)| \leq q - 1$. Ma nella dimostrazione del teorema di Wedderburn abbiamo visto che $|\phi_n(q)| > q - 1$ per ogni $n > 1$. Questo implica che $n = n(g) = 1$ per ogni $g \in G$, ossia il centralizzatore di ogni elemento del gruppo coincide con il gruppo stesso. G è quindi abeliano. $\square$

Possiamo osservare, in conclusione, come le linee guida di questa dimostrazione seguano i solchi tracciati dall'originale. Tuttavia, essa ha il pregio di focalizzare l'attenzione sul fatto che il teorema di Wedderburn derivi solamente da una caratterizzazione del numero di elementi di particolari sottogruppi di un gruppo abeliano finito. Esso segue come corollario dal teorema precedente applicato al gruppo moltiplicativo K^* di un corpo finito K.

Riferimenti bibliografici

[1] I.N Herstein, *Algebra*, Editori Riuniti, Roma (1982).

[2] T. Grundhöfer, *Commutativity of finite groups according to Wedderburn and Witt*, Arch. Math. 70(1998) 425–426, Birkhäuser Verlag, Basel (1998).

[3] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge (1997).

[4] C. Menini, F. Van Oystaeyen, *Abstract algebra. A comprehensive treatment*, Marcel Dekker, Inc., New York (2004).

[5] S. Mac Lane, G. Birkhoff, *Algebra*, Mursia, Milano (1975).

[6] A. Seidenberg, *Lectures in Projective Geometry*, Van Nostrand Company, Inc., Princeton (1962).