ALGEBRA 2

ELENCO DEGLI ARGOMENTI TRATTATI DURANTE LE LEZIONI

1. MARTEDÌ 6 MARZO 2012

Informazioni sul corso. Panoramica sul programma.

Definizione delle nozioni di gruppo, omomorfismo di gruppi. Un gruppo possiede un unico elemento neutro. In un gruppo, ogni elemento possiede un unico inverso. $(gh)^{-1} = h^{-1}g^{-1}; (g^{-1})^{-1} = g; 1^{-1} = 1$. Ogni omomorfismo applica l'elemento neutro nell'elemento neutro, e l'inverso di un elemento nell'inverso della sua immagine. $g^m g^m = g^{m+n}, (g^m)^n = g^{mn}$. $(gh)^n \neq g^n h^n$.

Ordine di un gruppo. Esempi di gruppi e sottogruppi: $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ sono gruppi abeliani. Se A è un anello con unità, l'insieme A^* degli elementi invertibili possiede una struttura di gruppo rispetto alla moltiplicazione: i gruppi $(\mathbb{Z}^* = \{\pm 1\}, \cdot), (\mathbb{K}^*, \cdot)$.

Il gruppo simmetrico $(\mathrm{S}_n, \circ)$, il gruppo generale lineare $\mathrm{GL}(n, \mathbb{K})$. Esempi di omomorfismi: $\mathrm{id} : G \to G$, $\det : \mathrm{GL}(n, \mathbb{K}) \to \mathbb{K}^*$, $\mathrm{sgn} : \mathrm{S}_n \to \{\pm 1\}$, $\pi : \mathbb{Z} \to \mathbb{Z}/(n)$. Ogni omomorfismo di anelli è anche un omomorfismo dei corrispondenti gruppi abeliani. Gergo: monomorfismi, epimorfismi, isomorfismi, automorfismi.

2. MERCOLEDÌ 7 MARZO 2012

Isomorfismi e loro significato. Il gruppo $(\mathbb{R}, +)$ è isomorfo al gruppo $(\mathbb{R}^+, \cdot)$. Gruppo ciclico C_n: è isomorfo al gruppo $(\mathbb{Z}/(n), +)$.

Sottogruppi. Un sottoinsieme di un gruppo è un sottogruppo se e solo se contiene l'elemento neutro ed è chiuso rispetto a moltiplicazione ed inverso. L'immagine ed il nucleo di omomorfismi sono sottogruppi. Il nucleo di un omomorfismo controlla la sua iniettività, l'immagine la sua suriettività. L'omomorfismo $\det$ e il gruppo speciale lineare $\mathrm{SL}(n, \mathbb{K})$. L'omomorfismo sgn è il sottogruppo alterno $\mathrm{A}_n < \mathrm{S}_n$. Decomposizione di una permutazione nel prodotto di cicli disgiunti. Notazione ciclica di una permutazione. Il segno di una permutazione è determinato dalla parità del numero di trasposizioni che lo esprimono per composizione.

Potenze di un elemento e sottogruppo generato da un elemento. L'omomorfismo $n \mapsto g^n$. Sottogruppi di $\mathbb{Z}$: sono tutti ciclici. Ordine di $g \in G$ e nucleo di $n \mapsto g^n$.

3. GIOVEDÌ 8 MARZO 2012

Elementi di ordine finito e infinito. L'ordine di $g \in G$ è uguale all'ordine del sottogruppo $(g) < G$. Ordine degli elementi di S_3. Elementi di ordine 1 e 2. Ogni elemento di un gruppo finito ha ordine finito. Gruppi ciclici. I gruppi ciclici sono abeliani. Un gruppo di ordine n è ciclico se e solo se possiede un elemento di ordine n. $(\mathbb{Z}, +)$, $(\mathbb{Z}/(n), +)$ sono ciclici. S_3 non è ciclico. Esercizio: se $G, |G| = n$ è ciclico, quanti elementi di ordine n contiene?

Congruenze modulo n in $\mathbb{Z}$. Congruenze modulo un sottogruppo H in un gruppo G. La congruenza modulo un sottogruppo è una relazione di equivalenza. Classi di equivalenza $[\,a\,]$ e classi laterali sinistre aH. Indice di un sottogruppo. Ciascun laterale sinistro in G di un sottogruppo H possiede la stessa cardinalità di H.

Teorema di Lagrange: $|G| = [G : H]|H|$; in particolare, se G è un gruppo finito e H un suo sottogruppo, l'ordine di H divide l'ordine di G. Applicazioni del Teorema di Lagrange: l'ordine di ciascun elemento di un gruppo finito divide l'ordine del gruppo. Se G è un gruppo finito, e $g \in G$, allora $g^{|G|} = 1$. Se $(a, n) = 1$, $a^{\phi(n)} = 1\,(n)$. Esempio: classi laterali sinistre di $H = \{\mathrm{id}, (12)\}$ e $K = \{\mathrm{id}, (123), (132)\}$ in S_3.

Gruppi di ordine piccolo. Se $|G|$ è primo, allora G è ciclico. Un gruppo ciclico di ordine N è isomorfo a $(\mathbb{Z}/(N), +)$; pertanto C_N è l'unico gruppo ciclico di ordine N a meno di isomorfismo. I gruppi di ordine $2, 3, 5, 7$ sono ciclici. Gruppi di ordine 4: un gruppo nel quale ogni elemento ha quadrato identico è abeliano. Costruzione esplicita dei gruppi non ciclici di ordine 4. Gruppi non ciclici di ordine 6: possiedono sia elementi di ordine 2 che elementi di ordine 3.

Prodotto di sottogruppi. Se $H, K < G$, allora HK è un sottogruppo se e solo se $HK = KH$. Esempio in S_3.

4. MARTEDÌ 13 MARZO 2012

Se $H, K < G$, il sottoinsieme HK possiede $|HK| = |H||K|/|H \cap K|$ elementi. Gruppi non abeliani di ordine 6: se a è un elemento di ordine 2 e b è un elemento di ordine 3, allora $ab = ba$, oppure $ab = ba^2$. Nel primo caso, ab ha ordine 6, e si ottiene un assurdo. Calcolo della tavola moltiplicativa nel secondo caso. I gruppi non abeliani di ordine 6 sono tutti isomorfi (e quindi sono isomorfi a S_3).

Confronto tra classi laterali destre e sinistre. Se $H < G$, allora $|aH| = |H| = |Ha|$ per ogni $a \in G$. Le classi laterali destre di $H < G$ formano una partizione di G. Se $H < G$ ha indice 2, allora le sue classi laterali destre e sinistre coincidono. Definizioni equivalenti di sottogruppo normale. Se $N \lhd G$, allora l'operazione di G induce su G/N un'operazione ben definita. Esempio di operazione non ben definita su G/H quando $H = ((12)) < \mathrm{S}_3 = G$. Se $H, N < G$ e $N \lhd G$ allora $HN = NH$ e quindi $HN \lhd G$. $\{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ è un sottogruppo normale di A_4.

Sia $\sim$ una relazione di equivalenza su un gruppo G. Allora $[a][b] = [ab]$ ben definisce un'operazione su $G/\sim \Leftrightarrow [a][b] = [ab]$ ben definisce un'operazione di gruppo su $G/\sim \Leftrightarrow \sim$ è la congruenza modulo un sottogruppo normale di G.

5. MERCOLEDÌ 14 MARZO 2012

Il gruppo diedrale D_n. Definizione e cardinalità. Calcolo esplicito della struttura di D_n.

Richiami: il Teorema di omomorfismo per insiemi. Sua traduzione gruppale: se $f : G \to H$ è un omomorfismo di gruppi, e $N \lhd G$ è contenuto in $\ker f$, allora esiste un unico omomorfismo $F : G/N \to H$ tale che $f = F \circ \pi_N$, dove $\pi_N : G \to G/N$ è la proiezione al quoziente. Poiché $\mathrm{Im}\, f = \mathrm{Im}\, F$, F è suriettivo se e solo se f è suriettivo. Inoltre F è iniettivo se e solo se $N = \ker f$.

Esiste una corrispondenza biunivoca tra l'insieme degli omomorfismi di G/N in H e l'insieme degli omomorfismi di G in H che hanno N nel nucleo.

Il teorema di isomorfismo: se $f : G \to H$ è un omomorfismo di gruppi, allora $G/\ker f$ è isomorfo a $\operatorname{Im} f$. Applicazioni: un gruppo ciclico è isomorfo a $(\mathbb{Z}/(d), +)$ per esattamente un valore di $d \geq 0$. Il sottogruppo alterno $\mathrm{A}_n < \mathrm{S}_n$ è normale e ha indice 2; pertanto, $|A_n| = n!/2$. Se un sottogruppo $H < \mathrm{S}_n$ non è contenuto in A_n, allora $H \cap \mathrm{A}_n$ ha indice 2 in H.

6. Giovedì 15 Marzo 2012

$\mathrm{D}_n < \mathrm{S}_n$, $\mathrm{D}_3 = \mathrm{S}_3$. Controimmagini di un elemento attraverso un omomorfismo di gruppi. Compatibilità della nozione di sottogruppo con quella di omomorfismo. Corrispondenza tra sottogruppi di G e sottogruppi di G/N, $N \lhd G$. Secondo e terzo teorema di isomorfismo. Applicazioni: sottogruppi di $\mathbb{Z}/(n)$, ordine di elementi in $\mathbb{Z}/(n)$. Se un sottogruppo $H < \mathrm{S}_n$ non è contenuto in A_n, allora $H \cap \mathrm{A}_n$ ha indice 2 in H (seconda parte).

Teorema di Cayley. Struttura delle permutazioni descritte dal Teorema di Cayley. Ogni gruppo finito si immerge in un gruppo simmetrico finito. Segno di permutazioni.

7. Martedì 20 Marzo 2012

Elenco degli elementi di S_4 e individuazione di quelli pari. Struttura ciclica degli elementi di A_5 e loro numero.

Relazione di coniugio. Esempio di elementi coniugati. Un sottogruppo è normale se e solo se è unione di classi di coniugio. Classi di coniugio in gruppi abeliani, e classi di coniugio di elementi centrali in gruppi non abeliani. Calcolo esplicito delle classi di coniugio in S_3. Elementi coniugati hanno lo stesso ordine. Un elemento coniuga a in se stesso se e solo se commuta con a. Il centro di un gruppo: è un sottogruppo normale. Due elementi coniugano a nello stesso elemento se e solo se appartengono allo stesso laterale sinistro del centralizzatore di a. La cardinalità di una classe coniugata divide l'ordine del gruppo. Le classi coniugate di cardinalità 1 sono tutte e solo quelle centrali. Calcolo delle classi coniugate in S_3 (di nuovo!), Q_4, D_4.

L'equazione delle classi (di coniugio). Un p-gruppo finito ha centro non banale.

8. Mercoledì 21 Marzo 2012

Risoluzione di esercizi.

9. Giovedì 22 Marzo 2012

Il centro di un gruppo non ha mai indice primo. Se p è primo, un gruppo di ordine p, p^2 è necessariamente abeliano; un gruppo non abeliano di ordine p^3 ha centro di ordine p.

Azioni di gruppi su insiemi: due definizioni equivalenti. Esempi: azione di G su se stesso per moltiplicazione sinistra e coniugazione; azione di G per moltiplicazione sinistra su G/H; azione di $\mathrm{GL}(V)$ su V, di $\mathrm{GL}(U) \times \mathrm{GL}(V)$ su $\mathrm{Hom}(U, V)$, di G sui suoi sottogruppi per coniugazione, di V su uno spazio affine X modellato su V per traslazione. Gergo: azioni transitive, libere, semplicemente transitive, fedeli. Orbita e stabilizzatore di un elemento, elementi invarianti. Lo stabilizzatore G_x di un elemento $x \in X$ è sempre un sottogruppo di G. L'azione di G su X lo ripartisce in unione disgiunta di orbite. Se G agisce su X e $x \in X$, allora $|G.x| = [G : G_x]$. Esempi: cardinalità di classi coniugate di elementi e sottogruppi. Il normalizzatore di un sottogruppo.

Teorema di Cauchy: se un primo p divide l'ordine di un gruppo finito G, allora esiste almeno un elemento in G di ordine esattamente p. In questa situazione, il numero di elementi di ordine p è congruo a -1 modulo p.

10. Martedì 27 Marzo 2012

La dimostrazione del Teorema di Cauchy nel caso $p = 2$ è analoga a quella fatta precedentemente.

Classi coniugate in gruppi simmetrici. Elementi coniugati hanno la stessa struttura ciclica. Elementi con la stessa struttura ciclica sono coniugati: come determinare l'elemento che coniuga due permutazioni con la stessa struttura ciclica. Classi coniugate in $\mathrm{S}_3, \mathrm{S}_4, \mathrm{S}_5$. Sottogruppi normali di $\mathrm{S}_3, \mathrm{S}_4, \mathrm{S}_5$. Gli unici sottogruppi normali di $\mathrm{S}_n, n \geq 5$ sono $(\mathrm{id}), \mathrm{A}_n, \mathrm{S}_n$ (senza dimostrazione, per il momento.

Prodotti diretti di gruppi. Gruppi che sono prodotto diretto (interno) di propri sottogruppi. Se G è prodotto diretto (interno) di H e K, allora gli elementi di H commutano con gli elementi di K. Prodotto diretto (esterno) di gruppi. Se G è prodotto diretto (interno) di due sottogruppi H e K, allora è isomorfo al prodotto diretto (esterno) $H \times K$.

Automorfismi. Definizione. Esempi di automorfismi di gruppi abeliani. Automorfismi interni di gruppi (non abeliani). Gli automorfismi formano gruppo $\mathrm{Aut}(G)$ rispetto alla composizione; gli automorfismi interni ne sono un sottogruppo $\mathrm{Int}(G)$. $\mathrm{Aut}(V_4) \simeq \mathrm{S}_3$. $\mathrm{Int}(G) \simeq G/Z(G)$.

11. Mercoledì 28 Marzo 2012

Risoluzione di esercizi.

12. Giovedì 29 Marzo 2012

$\mathrm{Int}(G) \simeq G/Z(G)$. Sottogruppi normali e caratteristici. Sottogruppi caratteristici sono normali. Un sottogruppo normale di un sottogruppo normale non è necessariamente normale. Un sottogruppo caratteristico di un sottogruppo normale è sempre normale.

Prodotto semidiretto (interno) di sottogruppi. Gli elementi di due sottogruppi in prodotto semidiretto non commutano necessariamente tra loro. Il modo in cui gli elementi di $H < G$ coniugano gli elementi di $N \lhd G$ è codificato in un omomorfismo $\phi : H \to \mathrm{Aut}(N)$. La coniugazione di N indotta da un elemento di H non è necessariamente interna. Definizione del prodotto semidiretto (esterno) $N \rtimes_\phi H$. Il prodotto in $N \rtimes_\phi H$ definisce una struttura di gruppo. Se G è prodotto semidiretto (interno) di $N \lhd G$ con $H < G$, allora G è isomorfo a $N \rtimes_\phi H$.

Un'applicazione: gruppi non abeliani di ordine 21. L'unico elemento centrale di un gruppo non abeliano di ordine 21 è l'identità. Un gruppo non abeliano di ordine 21 ha un unico sottogruppo di ordine 7, che è quindi normale (perché è caratteristico); è quindi della forma $\mathrm{C}_7 \rtimes_\phi \mathrm{C}_3$ per qualche $\phi : \mathrm{C}_3 \to \mathrm{Aut}(\mathrm{C}_7)$. L'automorfismo $y \mapsto y^2$ ha ordine 3 in $\mathrm{Aut}(\mathrm{C}_7)$. Il gruppo $\langle x, y \mid x^3 = y^7 = 1, xyx^{-1} = y^2 \rangle$ è non abeliano e ha ordine 21. I gruppi di ordine 15 sono tutti abeliani (solo enunciato).

13. MARTEDÌ 3 APRILE 2012

Il teorema di Sylow. Enunciato. Alcuni casi particolari: p-gruppi finiti, S_3, gruppi abeliani, $\mathrm{GL}_n(\mathbb{F}_p)$. Ingredienti della dimostrazione: immersione di S_n in $\mathrm{GL}_n(\mathbb{K})$, laterali doppi, discesa da un gruppo ai suoi sottogruppi.

Matrici di permutazione: cosa sono, come si moltiplicano; immersione di S_n in $\mathrm{GL}_n(\mathbb{K})$. Ogni gruppo finito si realizza come sottogruppo di $\mathrm{GL}_n(\mathbb{K})$.

Laterali doppi: cosa sono, quanti elementi possiedono. Se H, K sono sottogruppi di G, G è unione disgiunta di $H - K$ laterali doppi.

Dimostrazione del teorema di Sylow: se P è un p-Sylow di un gruppo finito G, e $H < G$, allora esiste $x \in G$ tale che $xPx^{-1} \cap H$ è un p-Sylow di G. Conseguenze: due p-Sylow di G sono sempre coniugati in G. Se G possiede un solo p-Sylow, allora tale p-Sylow è normale. Il numero di p-Sylow di G divide $|G|$ ed è $\equiv 1 \mod p$ (solo enunciato, per il momento). Esempio: i gruppi di ordine 15 sono ciclici.

14. MERCOLEDÌ 4 APRILE 2012

Risoluzione di esercizi.

15. MERCOLEDÌ 11 APRILE 2012

Ancora risoluzione di esercizi.

Una nuova dimostrazione del Teorema di Sylow. Decomposizione di un gruppo G in laterali doppi rispetto a un p-Sylow $P < G$. Il numero dei p-Sylow è $\equiv 1 \mod p$ e divide $|G|$.

16. GIOVEDÌ 12 APRILE 2012

Se $p < q < r$ sono numeri primi, un gruppo di ordine pqr contiene sottogruppi normali non banali. Risolubilità dei gruppi di ordine < 60.

Struttura di $\mathbb{Z}/(N)^\times$. Quando N è primo, è ciclico. Utilizzo del Teorema cinese del resto per ottenere una decomposizione di $\mathbb{Z}/(N)^\times$ in prodotto diretto di gruppi. Struttura di $\mathbb{Z}/(p^n)^\times$ quando p è un primo dispari e $n > 0$.

17. MARTEDÌ 17 APRILE 2012

Ancora sulla struttura di $\mathbb{Z}/(p^n)^\times$. Differenze tra il caso $p \neq 2$ e il caso $p = 2$. Semplicità di A_n quando $n \geq 5$: idea della dimostrazione per induzione. Principio di inclusione esclusione. Lemma tecnico: ogni sottogruppo normale non banale di $\mathrm{A}_n, n \geq 5$ contiene permutazioni non identiche con almeno un punto fisso.

18. MERCOLEDÌ 18 APRILE 2012

$\mathbb{Z}/(N)^\times$ è ciclico quando $N = 1, 2, 4,$ è potenza di un primo dispari o due volte una potenza di un primo dispari. $\mathrm{Aut}\,\mathrm{C}_N$ è isomorfo a $\mathbb{Z}/(N)^\times$.

Dimostrazione del lemma tecnico enunciato la volta precedente. Le permutazioni con almeno un punto fisso in $\mathrm{A}_{n+1}, n \geq 5$ sono strettamente più della metà. A_n è semplice quando $n \geq 5$. Sottogruppi normali di $\mathrm{S}_n, n \geq 5$: sono solamente $(\mathrm{id}), \mathrm{A}_n, \mathrm{S}_n$.

Semplicità di $\mathrm{GL}_3(\mathbb{F}_2)$: calcolo delle classi di coniugio attraverso la forma canonica razionale. Calcolo esplicito della cardinalità di una delle sei classi di coniugio.

19. GIOVEDÌ 19 APRILE 2012

Risoluzione di esercizi. Esempio: ogni gruppo semplice di ordine 60 è isomorfo a A_5.

20. MERCOLEDÌ 2 MAGGIO 2012

Correzione dell'esonero. Commenti.

21. GIOVEDÌ 3 MAGGIO 2012

Presentazioni di gruppi. Sottogruppo normale generato da un sottoinsieme. Identificazione di elementi in un gruppo. Esempi: l'abelianizzato di un gruppo. Gruppi liberi (su un alfabeto). Proprietà universale del gruppo libero. Quoziente di un gruppo libero per il sottogruppo normale generato da un sottoinsieme. Presentazione di un gruppo. Notazione compatta per la presentazione di un gruppo. Esempi: presentazione del gruppo abeliano libero $\mathbb{Z}^n$, del gruppo diedrale D_n; presentazione di Artin del gruppo simmetrico S_n.

Estensioni di campo. Ogni omomorfismo di un campo di un anello con 1 è iniettivo. Comunque si scelga un anello A con 1, esiste un unico omomorfismo $\mathbb{Z} \to A$ ($\mathbb{Z}$ è un oggetto iniziale nella categoria degli anelli con 1). Caratteristica di un dominio d'integrità: i domini di caratteristica prima $p \neq 0$ possiedono un sottoanello isomorfo a $\mathbb{F}_p$; i domini di caratteristica 0 possiedono un sottoanello isomorfo a $\mathbb{Z}$.

Proprietà universale di $A[x]$, dove A è un anello commutativo con 1. Omomorfismo di valutazione. Se $K \subset L$ è un'estensione di campi, e $\alpha \in L$, allora il nucleo dell'omomorfismo di valutazione $\mathrm{ev}_\alpha : K[x] \to L$ è un ideale primo di $K[x]$; se è $\neq (0)$, allora è anche massimale, e l'immagine $\mathrm{Im}\ \mathrm{ev}_\alpha = K[\alpha]$ è un sottocampo di L.

22. MARTEDÌ 8 MAGGIO 2012

Campo delle frazioni K_D di un dominio d'integrità D: costruzione e sua proprietà universale. Se D è un campo, allora K_D è naturalmente isomorfo a D. D si immerge in K_D e ogni altra immersione di D in un campo K fattorizza attraverso $D \hookrightarrow K_D$.

Il campo delle frazioni di $\mathbb{Z}$ è $\mathbb{Q}$. Se K è un campo di caratteristica 0, allora esiste un'unica immersione $\mathbb{Q} \hookrightarrow K$. Il sottocampo di un campo K generato da 1 è isomorfo a $\mathbb{Q}$ o a $\mathbb{F}_p$, con p primo, a seconda della caratteristica di K: tale sottocampo è detto campo primo di K.

Se $K \subset L$ è un'estensione di campi, allora L è uno spazio vettoriale su K. Grado $[L : K]$ dell'estensione. $[\mathbb{C} : \mathbb{R}] = 2$. $[\mathbb{R} : \mathbb{Q}] = \infty$. Se $\alpha \in L$ è algebrico su K, allora $K[\alpha] = K(\alpha)$, e $K[\alpha]$ ha grado finito su K. Se $\alpha \in L$ è trascendente su K, allora $K[\alpha] \subsetneq K(\alpha)$; in particolare, $K[\alpha] \simeq K[x]$, e $K(\alpha) \simeq K(x)$. $\mathbb{Q}(e) \simeq \mathbb{Q}(\pi)$. Ogni elemento di un'estensione di grado finito è algebrico: in altre parole, ogni estensione finita è algebrica (il viceversa è falso in generale). Ogni campo è un'estensione algebrica di se stesso. $\mathbb{C}$ è un'estensione algebrica di $\mathbb{R}$.

Se $F \subset K \subset L$ sono campi, allora $[L : F] = [L : K][K : F]$. Grado di un elemento algebrico. Il grado di un algebrico divide il grado di ogni estensione nella quale sia contenuto.

23. MERCOLEDÌ 9 MAGGIO 2012

Risoluzione di esercizi.

24. GIOVEDÌ 10 MAGGIO 2012

Riassunto delle cose fatte a proposito delle estensioni di campi. Se α, β sono algebrici su K, allora $K(\alpha, \beta)$ è un'estensione finita di K. In particolare, $\alpha + \beta, \alpha\beta$ sono algebrici, e così anche gli inversi di α e β quando questi ultimi sono diversi da 0.

Campi di spezzamento: come aggiungere ad un campo K una radice di un polinomio $f(x) \in K[x]$. Esempio: il campo $\mathbb{R}[x]/(x^2 + 1)$ estende $\mathbb{R}$ e contiene una radice (in effetti entrambe) del polinomio $x^2 + 1$. Se K è un campo, e $f(x) \in K[x]$ è un polinomio di grado n, allora esiste un'estensione L di K tale che $[L : K] \leq n!$ e $f(x)$ si spezza in $L[x]$ in fattori lineari.

$\overline{\mathbb{Q}}$ è un'estensione algebrica di $\mathbb{Q}$, ma non è finita.

Campi finiti. Esempi di campi con $4, 8, 27$ elementi. I campi finiti non hanno caratteristica 0. Ogni campo finito ha p^n elementi, per un'opportuna scelta di p primo e $n > 0$: due dimostrazioni. E' vero che per ogni scelta di p primo e $n > 0$ esiste un campo con esattamente p^n elementi? Sì, se so che $\mathbb{F}_p[x]$ possiede almeno un polinomio irriducibile di grado n (ma non lo so). Come è fatto un campo K con p^n elementi? Il gruppo moltiplicativo $K^\times$ è ciclico di ordine $p^n - 1$. In particolare ogni elemento di K soddisfa l'equazione $x^{p^n} = x$. Un campo con p^n elementi è necessariamente un campo di spezzamento di $x^{p^n} - x$ su $\mathbb{F}_p$.

L'omomorfismo di Frobenius: $\alpha \mapsto \alpha^p$ definisce un endomorfismo (iniettivo) su ogni campo K di caratteristica p. Se K è finito, allora è anche suriettivo, ed è quindi un automorfismo. Le potenze dell'omomorfismo di Frobenius sono anch'esse omomorfismi. Un polinomio che è prodotto di fattori lineari è libero da quadrati se e solo se è primo con la sua derivata.

Se L è un campo di spezzamento di $x^{p^n} - x$ su $\mathbb{F}_p$, allora l'insieme $X \subset L$ delle radici di $x^{p^n} - x$ ha cardinalità esattamente p^n, e costituisce un sottocampo di L. In particolare, X è un campo di cardinalità p^n. Se K è un campo con p^n elementi, ed α è un generatore ciclico di $K^\times$, allora $\mathbb{F}_p(\alpha) = K$ e quindi $K \simeq \mathbb{F}_p[x]/(q(x))$ dove $q(x)$ è il polinomio minimo di α. Di conseguenza, $q(x)$ è un polinomio irriducibile di grado n.

25. MARTEDÌ 15 MAGGIO 2012

Unicità del campo di spezzamento di un polinomio dato. Campi finiti con la stessa cardinalità sono isomorfi.

Se $a > 1$, allora $a^d - 1 | a^n - 1$ se e solo se $d|n$. $x^d - 1$ divide $x^n - 1$ se e solo se $d|n$. Se $K \subset F$ sono campi finiti, allora $|F|$ è una potenza di $|K|$. Se $|F| = p^n$, e $d|n$, allora esiste un unico sottocampo di F di cardinalità p^d.

26. MERCOLEDÌ 16 MAGGIO 2012

Risoluzione di esercizi.

27. GIOVEDÌ 17 MAGGIO 2012

Un polinomio irriducibile $q(x) \in \mathbb{F}_p[x]$ divide $x^{p^n} - x$ se e solo se ha grado che divide n.

Chiusura algebrica di un campo. Costruzione della chiusura algebrica di $\mathbb{Q}$. Se $K \subset L$ sono campi, e L è algebricamente chiuso, allora l'insieme $\overline{K}$ degli elementi di L algebrici su K è chiusura algebrica di K. Se $K \subset E \subset L$ sono campi, E è un'estensione algebrica di K, L è un'estensione algebrica di E, allora anche L è un'estensione algebrica di K.

Conti di cardinalità: se L è un'estensione finita di K, allora K, L sono entrambi finiti, oppure hanno la stessa cardinalità. Se L è un'estensione algebrica di K, allora $|L| \leq \max(|\mathbb{N}|, |K|)$. Costruzione, con il Lemma di Zorn, della chiusura algebrica di un campo K.

28. MARTEDÌ 22 MAGGIO 2012

Due chiusure algebriche di un campo K sono necessariamente isomorfe.

Costruzioni con riga e compasso. I numeri reali costruibili con riga e compasso sono chiusi per somma, differenza, prodotto, inverso e radice quadrata. Se un reale α è costruibile con riga e compasso, allora è algebrico su $\mathbb{Q}$ è il suo grado è una potenza di 2. Impossibilità dei problemi di: costruzione dell'n-agono regolare, quando $n = 7$; duplicazione del cubo; trisezione dell'angolo θ, quando $\cos\theta = 3/4$; rettificazione della circonferenza; quadratura del cerchio.

Automorfismi di campi finiti. Se $K \subset L$ sono campi finiti, $|K| = q$, $[L : K] = n$, allora esistono al più n automorfismi di L che fissano K elemento per elemento.

29. MERCOLEDÌ 23 MAGGIO 2012

Risoluzione di esercizi.

30. GIOVEDÌ 24 MAGGIO 2012

Gruppo di Galois $\mathrm{Gal}(L/K)$ di un'estensione $K \subset L$ di campi: definizione; è un gruppo; se $L = K(\alpha)$, dove $\alpha \in L$ è algebrico su K di grado n, allora $\mathrm{Gal}(L/K)$ ha al più n elementi. Esempi: il gruppo di Galois dell'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ possiede 2 elementi; il gruppo di Galois dell'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ possiede un solo elemento. Se $K \subset L$ sono campi finiti, $|K| = q$, $[L : K] = n$, allora $\mathrm{Gal}(L/K)$ è ciclico di ordine n, ed è generato da $\alpha \mapsto \alpha^q$.

Separabilità. Se $q(x) \in K[x]$ è un polinomio irriducibile, allora $\mathrm{MCD}(q(x), q'(x)) = 1$ se e solo se $q'(x) \not\equiv 0$. Se K ha caratteristica 0, la derivata di $q(x) \in K[x]$ irriducibile non è mai identicamente nulla. Se K ha caratteristica $p \neq 0$, allora $q'(x) \equiv 0$ se e solo se $q(x)$ contiene solo monomi di grado multiplo di p.

Campi perfetti: i campi di caratteristica 0, quelli finiti e quelli algebricamente chiusi sono perfetti. Se K è un campo perfetto, un polinomio irriducibile $q(x) \in K[x]$ non ha mai derivata nulla; in particolare è primo con la sua derivata, e quindi ha radici distinte nel suo campo di spezzamento.

Polinomi separabili, elementi algebrici separabili, estensioni separabili. Se L è il campo di spezzamento di un polinomio separabile $f(x) \in K[x]$, allora $\mathrm{Gal}(L/K)$ possiede esattamente $[L : K]$ elementi. In generale, se $K \subset L$ è un'estensione finita, $|\mathrm{Gal}(L/K)| \leq [L : K]$.

31. MARTEDÌ 29 MAGGIO 2012

Definizione di estensione (finita) normale. Se $K \subset L$ è un'estensione finita, normale, separabile, allora L è campo di spezzamento di un polinomio separabile $f(x) \in K[x]$. Se L è un campo, e G è un gruppo di automorfismi di L, allora il campo fisso L^G è il sottocampo degli elementi di L fissati da G. Se $K \subset L$ è un'estensione finita, e $G = \mathrm{Gal}(L, K)$ soddisfa $L^G = K$, allora L è un'estensione normale e separabile di K.

Se l'estensione finita $K \subset L$ soddisfa $|\mathrm{Gal}(L/K)| = [L : K]$, allora $L^{\mathrm{Gal}(L/K)} = K$. Idea della dimostrazione: se $G < \mathrm{Aut}(L)$ è un gruppo finito, allora $[L : L^G] \leq |G|$; pertanto $[L : L^G] = |G|$ e $G = \mathrm{Gal}(L/L^G)$; se $G = \mathrm{Gal}(L/K)$ e $|G| = [L : K]$, allora $K = L^G$. Dimostrazione del risultato tecnico: se G è un gruppo finito di automorfismi di L, e $n = |G|$, allora $m > n$ elementi $\alpha_1, \ldots, \alpha_m \in L$ sono necessariamente K-linearmente indipendenti.

32. MERCOLEDÌ 30 MAGGIO 2012

Risoluzione di esercizi.

33. GIOVEDÌ 31 MAGGIO 2012

Corrispondenza di Galois. Il grado di estensioni si traduce nell'indice dei corrispondenti sottogruppi. La normalità è conservata. Esempi di estensioni di Galois e non, e delle loro estensioni intermedie.

34. LUNEDÌ 5 GIUGNO 2012

Estensioni ciclotomiche. Il polinomio ciclotomico $\Phi_p(x)$ è irriducibile di grado $p - 1$ quando p è primo; allora l'estensione $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$ ha grado $p - 1$, ed è di Galois; il suo gruppo di Galois è isomorfo a $\mathbb{Z}/(p)^\times$.

Irriducibilità del polinomio ciclotomico $\Phi_n(x)$. L'estensione ciclotomica $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$ è di Galois e ha grado $\phi(n)$ ed il suo gruppo di Galois è isomorfo a $\mathbb{Z}/(n)^\times$. Caratterizzazione degli n per i quali è possibile costruire l'n-agono regolare con riga e compasso. Primi di Fermat.

Calcolo del gruppo di Galois del campo di spezzamento di $x^5 - 80x + 5 \in \mathbb{Q}[x]$ (incompleto).

35. MERCOLEDÌ 6 GIUGNO 2012

Risolubilità per radicali. Estensioni di Kummer. Teorema di Abel. Un'equazione non risolubile per radicali. Il ruolo delle estensioni ciclotomiche.

36. VENERDÌ 7 GIUGNO 2012

Risoluzione di esercizi.

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI DI ROMA – "LA SAPIENZA"
E-mail address: dandrea@mat.uniroma1.it