DIARIO DELLE LEZIONI DI ALGEBRA 2

a.a. 2013/2014

Nelle prime settimane di lezione, fino al 27 marzo, sono stati trattati i seguenti argomenti:

Richiami delle nozioni base di teoria dei gruppi. Teoremi di isomorfismo. Automorfismi e automorfismi interni. Classi di coniugio. Esempi: gruppi ciclici, gruppi simmetrici, gruppi alterni, gruppi diedrali, gruppi di matrici. Prodotti diretti. Il gruppo delle simmetrie di rotazione del tetraedro.

L'azione di un gruppo su un insieme. Orbite e stabilizzatori. L'equazione delle classi. A_5 è un gruppo semplice. Il teorema di Cauchy e i teoremi di Sylow. Gruppi abeliani finitamente generati.

1 aprile: Correzione del foglio di esercizi n. 4 del 27 marzo. Definizione di serie di composizione di un gruppo e cenno al programma di Holder. Definizione di prodotto semidiretto di due gruppi.

2 aprile: Prodotti semidiretti. Esempi. Quando un gruppo è prodotto diretto di due sottogruppi propri. Gruppi risolubili: Definizioni ed esempi. Un gruppo semplice non abeliano non è risolubile.

3 aprile: Un p-gruppo è risolubile. Commutatori e sottogruppo derivato. Un gruppo è risolubile se e soltanto se esiste un n tale che $G^{(n)} = \{e\}$ (dove $G^{(n)}$ è il derivato n-esimo). Ogni sottogruppo di un gruppo risolubile è risolubile. Ogni quoziente di un gruppo risolubile è risolubile. Se $n \geq 5$, il gruppo simmetrico S_n non è risolubile.

8 aprile: Correzione del foglio di esercizi n. 5. Richiami di teoria degli anelli. Ideali primi e massimali in anelli commutativi unitari e loro caratterizzazione al quoziente. Ideali primi e massimali di $\mathbb{Z}$ e di $K[x]$ (K campo).

9 aprile: Caratteristica di un campo e sottocampo fondamentale. Grado di un'estensione di campi. Esempi di anelli quoziente del tipo $K[x]/(f(x))$ (dove K è un campo): ogni classe è rappresentata da uno e un solo polinomio di grado minore del grado di $f(x)$, elementi invertibili e divisori dello zero. Esempi e conti in questo tipo di anelli.

10 aprile: Elementi algebrici e trascendenti su di un campo. Caratterizzazione delle estensioni algebriche e trascendenti semplici. Esempi.

15 aprile: Correzione del foglio di esercizi n. 6.

16 aprile: Radici dell'unità e polinomi ciclotomici. Se $F \subseteq K$ è un'estensione di campi, gli elementi di K algebrici su F formano un campo.

6 maggio: Correzione e commento della prima prova di esonero. Ogni estensione finita di campi è algebrica. Un'estensione algebrica di un'estensione algebrica è ancora algebrica.

7 maggio: Campi algebricamente chiusi. Se $f(x)$ è un polinomio di grado n a coefficienti in un campo F, allora esiste un campo E contenente F, con $[E : F] \leq n!$, dove $f(x)$ ha tutte le radici. Costruzione di un tale campo E in alcuni esempi: $x^3 - 2 \in \mathbb{Q}[x]$, $x^3 - 2 \in \mathbb{Z}_7[x]$, $x^8 - 1 \in \mathbb{Q}[x]$.

8 maggio: Definizione di campo di spezzamento di un polinomio. Date due estensioni E e $\tilde{E}$ di un campo F, un F-omomorfismo di E in $\tilde{E}$ è un omomorfismo che fissa tutti gli elementi del sottocampo F. Descrizione degli F-omomorfismi nel caso in cui $E = F(\alpha)$ (con α algebrico su F) e $E = F(\alpha_1, \ldots, \alpha_n)$ (con $\alpha_1, \ldots, \alpha_n$ radici di un polinomio $f(x) \in F[x]$). Due campi di spezzamento di un polinomio $f(x) \in F[x]$ sono isomorfi. Criterio della

derivata: $f(x) \in F[x]$ ha radici multiple nel suo campo di spezzamento se e soltanto se $\mathrm{MCD}(f(x), f'(x)) \neq 1$. Polinomi separabili e inseparabili con esempi. In un campo a caratteristica zero ogni polinomio è separabile, ovvero un campo a caratteristica zero è perfetto.

13 maggio: Correzione del foglio di esercizi n. 7.

14 maggio: Campi finiti: un campo finito ha p^n elementi. Per ogni primo p e $0 \neq n \in \mathbb{N}$ esiste, a meno di isomorfismi, un unico campo con p^n elementi, il campo di spezzamento di $x^{p^n} - x$ su $\mathbb{Z}_p$. Denotiamo questo campo con $\mathbb{F}_{p^n}$. Il gruppo degli automorfismi di $\mathbb{F}_{p^n}$ è ciclico di ordine n, generato dall'automorfismo di Frobenius. Un campo finito è perfetto. Teorema dell'elemento primitivo.

15 maggio: Costruzioni con riga e compasso. Caratterizzazione dei numeri reali costruibili. La quadratura del cerchio, la duplicazione del cubo e la trisezione dell'angolo sono problemi irrisolvibili con riga e compasso. Irriducibilità in $\mathbb{Q}[x]$ dell' n-esimo polinomio ciclotomico $\Phi_n(x)$.

20 maggio: Correzione del foglio di esercizi n. 8. Definizione di estensione normale di campi.

21 maggio: D'ora in poi tutti i campi che consideriamo sono perfetti e quindi vale il teorema dell'elemento primitivo. Un'estensione di campi $F \subseteq K$ è finita e normale se e soltanto se K è il campo di spezzamento di qualche polinomio $f(x) \in F[x]$. In questo caso l'estensione si dice di Galois (o Galoisiana). Data un'estensione finita di campi $F \subseteq K$, questa è di Galois se e soltanto se $|\mathrm{Aut}(K, F)| = [K : F]$. In questo caso denotiamo $\mathrm{Aut}(K, F)$ con $\mathrm{Gal}(K, F)$ e lo chiamiamo il gruppo di Galois di K su F. Teorema di corrispondenza di Galois (per ora abbiamo dimostrato soltanto che che la corrispondenza è biunivoca).

22 maggio: Dimostrazione del Teorema di corrispondenza di Galois. Esempio dettagliato della corrispondenza: $F = \mathbb{Q}$ e K campo di spezzamento di $x^4 - 2 \in \mathbb{Q}[x]$. Il gruppo di Galois $\mathrm{Gal}_{f(x)}$ di un polinomio $f(x) \in F[x]$ è $\mathrm{Gal}(K, F)$, dove K è il campo di spezzamento di $f(x)$. Il gruppo di Galois di un polinomio $f(x) \in F[x]$ con n radici distinte agisce sull'insieme delle sue radici e definisce un omomorfismo iniettivo di $\mathrm{Gal}_{f(x)}$ nel gruppo simmetrico S_n.

27 maggio: Correzione del foglio di esercizi n. 9. Sottocampi di un campo finito. Fattori irriducibili di $x^{p^n} - x \in \mathbb{Z}_p[x]$.

28 maggio: Estensioni ciclotomiche . Caratterizzazione dei poligoni regolari costruibili con riga e compasso. Polinomi simmetrici e polinomi simmetrici elementari. Discriminante $\Delta(f)$ di un polinomio $f \in F[x]$ come polinomio simmetrico nelle radici del polinomio. $\Delta(f)$ è un quadrato in F se e soltanto se $\mathrm{Gal}_f \subseteq A_n$.

29 maggio: Polinomi irriducibili di terzo grado in $\mathbb{Q}[x[$: il gruppo di Galois è S_3 o A_3. Esempi. Una dimostrazione del Teorema fondamentale dell'algebra usando la teoria di Galois.

3 giugno: Correzione del foglio di esercizi n. 10. Definizione di estensione radicale di campi e di polinomio risolubile per radicali.

4 giugno: I polinomi irriducibili di grado primo p su $\mathbb{Q}$ con esattamente due radici complesse coniugate hanno gruppo di Galois isomorfo a S_p. Se $f(x) \in F[x]$ (F campo a caratteristica zero) è risolubile per radicali, allora $\mathrm{Gal}_{f(x)}$ è un gruppo risolubile (parte diretta del Teorema di Abel Ruffini). Lemma di Dedekind: n omomorfismi iniettivi distinti di un campo F in una sua estensione K sono linearmente indipendenti su K.

5 giugno: Dimostrazione della parte inversa del Teorema di Abel Ruffini.

10 giugno: Correzione del foglio di esercizi n. 11.

11 giugno: Le formule risolutive per le equazioni di terzo grado (da non ricordare a memoria) e l'importanza storica del "casus irridicibilis ".

12 giugno: Seconda prova scritta di esonero.