PROGRAMMA DI ALGEBRA 2
prof. Valentina Barucci
a.a. 2015-2016

Richiami di teoria dei gruppi. Gruppi ciclici e loro sottogruppi, gruppi simmetrici, gruppi alterni, gruppi diedrali, gruppi di matrici. Sottogruppi normali e gruppi quozienti. Teoremi di isomorfismo. Elementi coniugati. Automorfismi interni. Prodotto diretto di gruppi. Quando un gruppo è prodotto diretto di due suoi sottogruppi propri. Definizione di azione di un gruppo su un insieme. Orbite e stabilizzatori. Azione di coniugio di un gruppo su sé stesso, classi di coniugio, centralizzante. L'equazione delle classi. p-gruppi. Un p-gruppo ha centro non banale. Un gruppo di ordine p^2 è abeliano. Il teorema di Cauchy. I tre teoremi di Sylow: dimostrazione ed esempi. Gruppi di ordine $2p$, con p primo dispari. Il teorema di Cayley. Un gruppo di ordine $2m$, con m dispari contiene almeno un sottogruppo di indice due. Classificazione dei gruppi abeliani finitamente generati. Gruppi semplici. Definizione di serie di composizione. Cenno al programma di Hölder: 1) Classificare i gruppi semplici 2) Problema di ampliare un gruppo N tramite un gruppo H, cioè trovare un gruppo G tale che N sia un sottogruppo normale di G e $G/N \cong H$. Prodotto semidiretto di due gruppi. Quando un gruppo è prodotto semidiretto di due sottogruppi propri. Esempi. Gruppi risolubili. Un p-gruppo è risolubile. Derivato di un gruppo e sue proprietà, serie derivata. Un gruppo G è risolubile se e soltanto se per qualche n, il derivato n-esimo $G^{(n)}$ è il sottogruppo banale $\{e\}$. Un sottogruppo di un gruppo risolubile è risolubile. Un quoziente di un gruppo risolubile è risolubile. Dimostrazione (tramite l'equazione delle classi) che A_5 è un gruppo semplice. Conseguenza: per $n \geq 5$ il gruppo simmetrico S_n non è risolubile. Richiami di Algebra 1: anelli, ideali, quozienti di anelli, ideali primi e massimali, domini euclidei, quozienti di anelli di polinomi. Caratteristica di un campo.

Elementi algebrici e trascendenti su un campo. Estensioni semplici. Esempi

Chiusura algebrica di F in K, dove $F \subseteq K$ sono campi. Ogni estensione finita è algebrica, ma il viceversa non vale. Un'estensione algebrica di un'estensione algebrica è algebrica. Campi algebricamente chiusi.

Definizione di campo di spezzamento. Esempi. Richiami: radici n-esime dell'unità e polinomi ciclotomici. F-omomorfismi. Come estendere un omomorfismo di campi $F \to \tilde{F}$ ad un'estensione algebricia semplice $E = F(\alpha)$ di F.

Radici multiple e criterio della derivata. Definizione di polinomi separabili e campi perfetti. Un campo a caratteristica zero è perfetto. Esempio di polinomio non separabile. F-omomorfismi di estensioni algebriche finitamente generate di un campo F. Unicità a meno di isomorfismi del campo di spezzamento di un polinomio. Il gruppo moltiplicativo di un campo finito è ciclico.

Per ogni primo p e ogni intero $n \geq 1$ esiste un campo K con p^n elementi (unico a meno di isomorfismi). K è il campo di spezzamento di $x^{p^n} - x$ su $\mathbb{Z}_p$ ed è costituito esattamente dalle radici di $x^{p^n} - x$. Il gruppo degli automorfismi di un campo finito è ciclico, generato dall'automorfismo di Frobenius. Un campo finito è perfetto. Esercizio 3 della lista del 25 aprile. Richiamo del teorema cinese del resto per un anello commutativo unitario.

Teorema dell'elemento primitivo: ogni estensione finita di un campo a caratteristica zero è semplice. Costruzioni con riga e compasso. Caratterizzazione dei numeri reali costruibili. I problemi classici della quadratura del cerchio, della duplicazione del cubo e della trisezione dell'angolo.

Elementi coniugati su un campo ed estensioni normali. Condizioni equivalenti per un'estensione finita e normale di campi perfetti. Definizione di estensione di Galois e gruppo di Galois. Esempi. Irriducibilità dell'n-esimo polinomio ciclotomico.

Il teorema di corrispondenza di Galois. Dimostrazione ed esempi.

Il gruppo di Galois di un polinomio (a radici distinte) come gruppo di permutazioni sulle radici. Il gruppo di Galois di un'estensione ciclotomica di $\mathbb{Q}$. Un poligono regolare con n lati è costruibile con riga e compasso se e soltanto se $\phi(n)$ è una potenza di 2 (dove ϕ indica la funzione di Eulero).

Primi di Fermat e ulteriore caratterizzazione dei poligoni regolari costruibili. Polinomi simmetrici e polinomi simmetrici elementari. I coefficienti di un polinomio sono, a meno del segno, i polinomi simmetrici elementari nelle sue radici. Discriminante di un polinomio. Il discriminante di $f(x) \in F[x]$ è un quadrato in F se e soltanto se Gal_f, come gruppo di permutazioni sulle radici di $f(x)$ è contenuto nel gruppo alterno, cioè contiene solo permutazioni pari.

Polinomi di terzo grado: discriminante e gruppo di Galois, formule risolutive per la corrispondente equazione algebrica. Il "casus irriducibilis" e la sua importanza storica. Una dimostrazione del teorema fondamentale dell'algebra, usando la teoria di Galois.

Estensioni radicali e polinomi risolubili per radicali. Un polinomio è risolubile per radicali (su un campo a caratteristica zero)se e soltanto se il suo gruppo di Galos è risolubile (Teorema di Abel - Ruffini). Lemma di Dedekind. Esempi di polinomi non risolubili per radicali.

Se p è un primo dispari il discriminante di $x^p - 1 \in \mathbb{Q}[x]$ è $\Delta = (-1)^{\frac{p-1}{2}} p^p$, da cui $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}} p})$ è l'unica estensione quadratica di $\mathbb{Q}$ contenuta nella p-esima estensione ciclotomica $\mathbb{Q}(\zeta_p)$. Ogni estensione quadratica di $\mathbb{Q}$ è contenuta in un'estensione ciclotomica.