Corso di Laurea Specialistica in **Matematica** - a.a. 2010/11

programma di **TEORIA DI GALOIS** - prof. **Fabio Gavarini**

1 - ESTENSIONI DI CAMPI - [La], par. V.1

Estensioni di campi. Grado di un'estensione, moltiplicatività; estensioni finite, infinite, finitamente generate. Elementi algebrici ed elementi trascendenti. Estensioni semplici. Estensioni algebriche, trascendenti, trascendenti pure.

Classi distinte di estensioni di campi. Estensioni finite ed estensioni algebriche formano classi distinte.

2 - CHIUSURE ALGEBRICHE E ESTENSIONI DI IMMERSIONI - [La], par. V.2

Ogni endomorfismo (sul campo base) di un'estensione algebrica è un automorfismo. Campi algebricamente chiusi: definizione, esistenza. Ogni immersione di un campo k in un campo algebricamente chiuso si estende ad ogni estensione algebrica di k. Chiusura algebrica di un campo; definizione, esistenza, unicità (a meno di isomorfismi).

3 - ESTENSIONI NORMALI - [La], par. V.3

Campi di spezzamento: definizione, esistenza, unicità (a meno di isomorfismi). Condizioni di normalità: estensioni (algebriche) normali, definizione e proprietà di base. Chiusura normale di un'estensione: definizione, caratterizzazioni.

4 - ESTENSIONI SEPARABILI - [La], par. V.4

Grado di separabilità di un'estensione algebrica; moltiplicatività e maggiorazione caso finito. Elementi algebrici separabili; polinomi separabili. Criteri di separabilità di un elemento algebrico. Derivazione formale dei polinomi.

Morfismo di Frobenius per un campo di caratteristica positiva. Forma e proprietà di un polinomio irriducibile. Rapporto tra grado e grado di separabilità di un'estensione semplice. Grado di inseparabilità di un'estensione finita.

Estensioni algebriche separabili; criteri di separabilità. La classe delle estensioni (algebriche) separabili è distinta. Chiusura separabile di un campo in una sua estensione algebrica.

Teorema dell'Elemento Primitivo: *(a)* un'estensione finita è semplice se e soltanto se il numero di estensioni intermedie è finito; *(b)* ogni estensione finita separabile è semplice.

5 - ESTENSIONI PURAMENTE INSEPARABILI - [La], par. V.6

Eementi puramente inseparabili in un'estensione. Estensioni algebriche puramente inseparabili. La classe delle estensioni puramente inseparabili è distinta. Ogni estensione puramente inseparabile è normale, con gruppo di Galois banale.

6 - FATTORIZZAZIONE DI ESTENSIONI - [La], par. V.6

Un'estensione algebrica è separabile e puramente inseparabile se e soltanto se è banale.

Fattorizzazione k-E_s-E di un'estensione algebrica E/k, con E_s := chiusura separabile di k in E; conservazione della normalità se E/k è normale. Fattorizzazione k-K^G-K di un'estensione algebrica normale K/k, con K^G := G-invarianti di K, per G := $Gal(K/k)$. Confronto con la fattorizzazione k-K_s-K. Estensioni di Galois.

7 - I CAMPI FINITI - [La], par. V.5

Campi finiti: caratteristica e cardinalità. Esistenza e unicità; teorema di struttura; normalità sui sottocampi.

Teorema: un campo è finito se e soltanto se il suo gruppo moltiplicativo è ciclico.

Il gruppo di Galois di un'estensione tra campi finiti (ciclicità, ordine, automorfismo di Frobenius). Corollario: le estensioni tra campi finiti sono tutte separabili. Criterio per l'esistenza di un'estensione tra campi finiti.

Descrizione della chiusura algebrica di un qualsiasi campo finito.

8 - TEORIA DI GALOIS: RISULTATI GENERALI - [La], par. VI.1

Il reticolo (completo) delle estensioni intermedie in un'estensione. Il reticolo completo dei sottogruppi di un gruppo.

Corrispondenze di Galois per un'estensione: proprietà fondamentali, restrizione alle estensioni normali, monomorfismo indotto $G(E/k)/G(E/F) \longrightarrow G(F/k)$ per F/k estensione intermedia normale. Corrispondenze di Galois generalizzate.

Relazioni tra gruppi di Galois di estensioni collegate per sollevamento o per prodotto composto.

Estensioni di Galois. In un'estensione di Galois, il sottocampo fissato dal gruppo di Galois è il campo base. Proprietà della corrispondenza di Galois per una estensione di Galois E/k : $F \longrightarrow G(E/F)$ è iniettiva, $H \longrightarrow E^H$ è suriettiva, la composizione delle due (in quest'ordine) è l'identità, la composizione inversa è idempotente.

Coniugazione nel gruppo di Galois di un'estensione di Galois. La corrispondenza di Galois per un'estensione di Galois associa a sottoestensioni di Galois sottogruppi normali, e viceversa. Biiezione tra lo spazio quoziente delle classi laterali di un sottogruppo $G(L/F)$ in un gruppo di Galois $G(L/k)$ di un'estensione di Galois L/k e insieme delle immersioni $I(F/k)$.

9 - TEORIA DI GALOIS: CASO FINITO - [La], par. VI.1

Lemma di Artin: se G è un sottogruppo finito del gruppo degli automorfismi di un campo K, allora K/K^G è di Galois finita con $G(K/K^G) = G$. Proprietà speciali della corrispondenza di Galois nel caso finito.

Il gruppo di Galois di un sollevamento si identifica ad un sottogruppo del gruppo di Galois dell'estensione di partenza. Rapporto tra fattorizzazione di un'estensione di Galois (finita) e fattorizzazione del suo gruppo di Galois.

Applicazione: il Teorema Fondamentale dell'Algebra.

10 - ESTENSIONI CICLOTOMICHE - [La], par. VI.3

Estensioni cicliche, estensioni abeliane; proprietà elementari rispetto alle torri, ai sollevamenti, ai prodotti.

Radici dell'unità: struttura ciclica e ordine del gruppo delle radici dell'unità (in una chiusura algebrica). Radici n-esime primitive dell'unità. Estensioni ciclotomiche, campi ciclotomici. Il prodotto di estensioni di un campo generate da una radice dell'unità di ordine r e una di ordine s è a sua volta generata da una radice dell'unità, di ordine il *m.c.m.* tra r e s.

Una radice primitiva n-esima dell'unità ha grado $\phi(n)$ su $\mathbf{Q}$.

Polinomi ciclotomici: definizione e proprietà fondamentali *(senza dimostrazioni)*.

Il gruppo di Galois del campo ciclotomico di ordine n su k è isomorfo ad un sottogruppo del gruppo (moltiplicativo) $\mathbf{Z}_n^*$. Se $k = \mathbf{Q}$, allora il suddetto gruppo è isomorfo a $\mathbf{Z}_n^*$. Ogni estensione ciclotomica è abeliana.

Teorema di Kronecker (soltanto l'enunciato!): ogni estensione abeliana di $\mathbf{Q}$ è ciclotomica.

11 - ESTENSIONI CICLICHE - [La], parr. VI.4-5-6

Lemma di Artin: caratteri distinti (su un semigruppo) sono linearmente indipendenti.

Norma e traccia di un'estensione finita: definizione, proprietà fondamentali. Norma e traccia di un elemento.

Il 90^o Teorema di Hilbert (forma moltiplicativa e forma additiva, con formula esplicita dei "risolventi di Lagrange").

Caratterizzazione delle estensioni cicliche (caso moltiplicativo e caso additivo).

12 - ESTENSIONI RISOLUBILI - [La], par. VI.7

Richiami sui gruppi risolubili: definizione, proprietà fondamentali, esempi.

Estensioni risolubili. Teorema: la classe delle estensioni risolubili è distinta.

Estensioni risolubili per radicali. Teorema: la classe delle estensioni risolubili per radicali è distinta.

Teorema *(Abel-Ruffini)*: Se E/k è finita, allora E/k è separabile se e soltanto se è separabile per radicali.

Risolubilità per radicali di equazioni algebriche. Gruppo di Galois di un polinomio. Il gruppo di Galois di un polinomio di grado n si immerge nel gruppo simmetrico S_n. Lemma: *(a)* il campo delle funzioni razionali simmetriche in n variabili è generato dagli n polinomi simmetrici elementari; *(b)* il polinomio generico di grado n ha gruppo di Galois isomorfo a S_n.

Teorema: l'equazione algebrica generica di grado n è risolubile per radicali se e soltanto se $n < 5$.

Teorema di Shafarevich (soltanto l'enunciato!): ogni gruppo finito risolubile G è gruppo di Galois di un'estensione di Galois di $\mathbf{Q}$. In altre parole, esiste un'estensione di Galois di $\mathbf{Q}$, sia $\mathbf{K}$, tale che $G(\mathbf{K}/\mathbf{Q})$ sia isomorfo a G.

13 - GRUPPI TOPOLOGICI

Richiami di topologia generale. Gruppi topologici. Sistemi fondamentali di intorni in un gruppo topologico. Proprietà fondamentali dei quozienti e dei sottogruppi in un gruppo topologico. Proprietà di separabilità dei gruppi topologici.

Esempio: la topologia cofinita $\boldsymbol{T}^{cof}(G)$ in un gruppo G qualsiasi (cenni).

14 - TEORIA DI GALOIS: CASO ALGEBRICO - [Ka], par. 12; [Mo], Cap. IV; [Na], Cap VI

Il sottoreticolo **F'** , risp. **G'**, delle estensioni intermedie di grado finito, risp. di grado finito e di Galois sulla base, in un'estensione di Galois. I sottoreticoli **S'** e **N'** corrispondenti a **F'** e a **G'** rispetto alla corrispondenze di Galois.

Le corrispondenze tra **F'** e **S'** e tra **G'** e **N'** sono biunivoche, e in esse il grado corrisponde all'indice.

La topologia di Krull nel gruppo di Galois di un'estensione di Galois. Proprietà fondamentali delle corrispondenze di Galois rispetto alla topologia di Krull: in particolare, i gruppi di Galois di estensioni intermedie sono chiusi.

Esistenza di un rappresentante comune per classi laterali, compatibili con l'inclusione, rispetto a sottogruppi normali di $G(L/k)$ che formino una famiglia chiusa perl'intersezione. Proprietà topologiche (per la topologia di Krull) di un gruppo di Galois: compattezza, T_4-separabilità, sconnessione totale, coincidenza con la topologia indotta sui sottogruppi chiusi.

Il gruppo di Galois di un sollevamento è isomorfo e omeomorfo ad un sottogruppo del gruppo iniziale. Il gruppo di Galois di un prodotto è isomorfo e omeomorfo al prodotto diretto dei gruppi di Galois delle estensioni fattori, e viceversa.

Esempi di estensioni di Galois infinite, e loro gruppi di Galois:

(1) la chiusura quadratica di **Q**; *(2)* la chiusura algebrica del campo con p elementi (p primo); *(3)* l'estensione di **Q** ottenuta aggiungendo *tutte* le radici dell'unità (= unione di tutte le estensioni ciclotomiche di **Q**).

15 - COMPLETAMENTI E LIMITI - [Ka], par. 11; [Na], Cap VI

Insiemi diretti, sistemi inversi, limiti inversi: definizione, unicità. Esistenza (e descrizione) del limite inverso di un sistema inverso di gruppi (o di anelli); proprietà topologiche del limite. Gruppi (o anelli) profiniti.

Il sistema inverso di gruppi finiti - topologici discreti - associato ai quozienti di un gruppo di Galois per i sottogruppi (normali) in **N'**. Teorema: ogni gruppo di Galois $G(L/k)$ è isomorfo, come gruppo topologico, al limite inverso di: *(a)* tutti i suoi quozienti per i gruppi di Galois $G(L/K)$ delle estensioni L/K tali che K/k sia estensione normale e finita; *(b)* i gruppi di Galois $G(K/k)$ delle estensioni intermedie K/k che siano normali e finite. In particolare, $G(L/K)$ è un gruppo profinito.

Esempi di limiti inversi (di gruppi, di anelli, ecc.) o diretti:

(1) l'anello degli interi p-adici; *(2)* l'anello degli interi di Prüfer.

Esempi di gruppi di Galois infiniti, come limiti inversi di gruppi (finiti):

(1) il gruppo di Galois della chiusura quadratica di **Q**; *(2)* il gruppo di Galois della chiusura algebrica del campo con p elementi (p primo); *(3)* il gruppo di Galois dell'estensione di **Q** ottenuta aggiungendo *tutte* le radici dell'unità.

BIBLIOGRAFIA

[Ka] – G. Karpilovsky, "FIELD THEORY: Classical Foundations and Multiplicative Groups", Marcel Dekker, 1988.

[La] – S. Lang, "Algebra", Second Edition, Addison-Wesley Publishing Company, Inc., 1984.

[Mo] – P. Morandi, "Fields and Galois Theory", Graduate Texts in Mathematics **167**, Springer-Verlag, Berlin, 1996.

[Na] – M. Nagata, "Theory of commutative fields", Translations of Math. Monographs, AMS ed., Providence, 1993.

N.B.: sono anche disponibili *note manoscritte* del prof. Gavarini che coprono *tutto* il programma del corso.