Teoria di Galois

I riferimenti sono alle note in rete di Milne

Introduzione. Estensioni finite di campi. Prop. 1.20: moltiplicativita' dei gradi. Es. se $f(X)$ è polinomio irriducibile $F[X]/(f(X))$ è estensione di grado n di F. Anelli e campi generati da sottoinsiemi. Lemma 1.26.

Elementi algebrici e trascendenti. Caratterizzazione usando le mappe di valutazione ψ_α. Prop. 1.30 e Cor. 1.31: caratterizzazione delle estensioni finite. Campi algebricamente chiusi: caratterizzazione Prop. 1.42.

Prop. 1.44 e Def. 1.43, prop. 1.45 e Cor. 1.46: costruzione di chiusure algebriche. Es. $\overline{\mathbf{Q}}$.

Classificazione delle estensioni di campi di grado 1 e 2.

Numeri costruibili con riga e compasso (tutta la sezione "Constructions with straight-edge and compass" in Milne). Definizione e prime proprietà.

Dimostrazione che i numeri costruibili con riga e compasso sono un campo.

Caratterizzazione dei numeri costruibili tramite estensioni iterate di grado 2. Soluzione ai problemi greci classici. Primi di Fermat.

Prop. 2.1 e prop. 2.2: F-omomorfismi e estensioni semplici. Campi di spezzamento. Prop. 2.4: esistenza e limitazioni sul grado.

Prop. 2.7 e Cor. 2.8: estensione di automorfismi.

Radici semplici e multiple di polinomi. Prop. 2.12: caratterizzazione dei polinomi irriducibili non separabili. Esempi e controesempi: polinomi di grado 2. Def. 2.14: Campi perfetti. Prop. 2.15: caraterizzazione dei campi perfetti in caratteristica positiva tramite l'automorfismo di Frobenius. Esempi 2.16: campi di caratteristica 0, campi algebricamente chiusi, campi finiti. Controesempio: $F_p(T)$.

Gruppi di automorfismi di estensioni di campi. Prop. 3.2. Teo. 3.4 di Artin. Cor. 3.5: $G = Aut(E/E^G)$. Esempio: il p-esimo campo ciclotomico e il suo gruppo di automorfismi. Esempi di campi di spezzamento.

Def. 3.6: estensioni separabili. Esempi e controesempi. Def. 3.7: estensioni normali. Esempi e controesempi. Def. 3.9: estensioni di Galois. Teo. 3.10: Caratterizzazioni equivalenti di estensioni di Galois. Esempi: estensioni biquadratiche, campo di spezamento di $X^3 - 2$ su Q

Teo. 3.16: teorema fondamentale della Teoria di Galois. Esempi: estensioni biquadratiche: gruppo di Galois e reticolo dei sottogruppi e dei sottocampi.

Campo di spezzamento di un polinomio irriducibile di grado 3 su un campo di caratteristica $\neq 3$: gruppi di Galois possibili, reticolo dei sottocampi e dei sottogruppi. Nel caso in cui il gruppo sia S_3, realizzazione di tale gruppo come gruppo di permutazioni delle tre radici del polinomio di partenza. Es. campo di spezzamento di $X^3 - 2$ su Q.

Prop. 3.18: gruppo di Galois del composto di un campo e di un' estensione galoisiana. Prop. 3.20: gruppo di Galois di composto di estensioni galoisiane. Controesempio al Cor. 3.19 nel caso non di Galois.

Campi ciclotomici e loro gruppo di Galois: irriducibilità del polinomio ciclotomico su $\mathbf{Q}$. Grado e gruppo di Galois su $\mathbf{Q}$ dei campi ciclotomici (Prop. 5.8, lemma 5.9, Teorema

5.10).

Gruppo di Galois del campo di spezzamento di un polinomio separabile di grado n come sottogruppo del gruppo delle permutazioni S_n delle radici del polinomio.

Gruppo di Galois del campo di spezzamento del polinomio $X^n - a \in F[X]$ con $a \neq 0$ ed F campo di caratteristica 0 oppure di caratteristica positiva coprima con n. Prodotti semidiretti.

Campi finiti. Teoria di Galois di campi finiti, polinomi irriducibili su campi finiti (Proposizioni 4.18, 4.19, 4.22 e Corollari 4.20, 4.21).

Gruppi risolubili: definizioni, esempi e proprietà. I p-gruppi sono risolubili. Teorema fondamentale dell'algebra (Teorema 5.6, Corollario 5.7). Risolubilità per radicali e risolubilità di gruppi di Galois (Teorema 5.33 di Milne: enunciato).

Elementi di teoria dei Numeri:

I riferimenti sono alle note del sottoscritto e del collega Massimo Bertolini, disponibili su questa pagina web

Def 2.1: interi algebrici. Lemma 2.2 e Prop. 2.4: caratterizzazione degli interi algebrici. Cor 2.5: gli interi algebrici formano un anello.

Prop. 2.8: anelli di interi di estensioni qudratiche. Def. 3.1, Prop. 3.3, lemma 3.5, Prop 3.6: Definizione e proprietà di norma, traccia, polinomio carateristico di elementi (interi). Prop. 3.8: calcolo di $disc(1, \alpha, \ldots, \alpha^{n-1})$, Cor. 3.10: sottocampi quadratici di campi cicolotomici.

Teo 4.5: Gli anelli di interi di campi di numeri sono gruppi abeliani finitamente generati. Def. 4.6: Basi di anelli di interi. Lemma 4.8/ Def. 4.9: Definizione di discriminante di anelli di interi. Es: calcolo di discriminanti di campi quadratici. Es (Cor. 3.9): anello di interi e discriminante del p-esimo campo ciclotomico. Teo 4.12: anello di interi di campi composti. Calcolo dell'anello degli interi di campi ciclotomici. Esercizi: anelli di interi e discriminanti di estensioni biquadratiche.

Def 5.3: Domini di Dedekind. Teo. 5.4: anelli di interi di campi di numeri sono domini di Dedekind. Enunciato del Teo. 5.16 sulla fattorizzazione di ideali.

Def. 6.2: Indice di ramificazione e di inerzia di un primo. Prop 6.5: contrazione di primi. Esercizio 6.9. Lemma 6.7, Teorema 6.8 e Teorema 6.10. Esempi: campi ciclotomici (cor. 6.13), estensioni quadratiche (es. 6.12).