DIARIO DEL CORSO DI ALGEBRA B

A.A. 2018/19

DOCENTE: ANDREA CARANTI

Nota. L'eventuale descrizione di lezioni non ancora svolte si deve intendere come una previsione/pianificazione.

Lezione 1. lunedí 17 settembre 2018 (2 ore)

(Lezione tenuta da Simone Ugolini)

Un polinomio di grado n a coefficienti in un campo F ha al più n radici distinte in F.

Quadrati in $F = \mathbf{Z}/p\mathbf{Z}$. Se p è dispari, ci sono $(p-1)/2$ quadrati non nulli in F, e questi sono le radici del polinomio $x^{(p-1)/2} - 1$.

Se p è un primo dispari e $a \not\equiv 0 \pmod{p}$, allora

$$a^{(p-1)/2} \equiv \begin{cases} 1 & \text{se } a \text{ è un quadrato, e} \\ -1 & \text{se } a \text{ non è un quadrato.} \end{cases}$$

-1 è un quadrato modulo il primo dispari p se e solo se $p \equiv 1 \pmod{4}$.

Lemma dei cassetti (versione generalizzata).

Lezione 2. mercoledí 19 settembre 2018 (2 ore)

(Lezione tenuta da Simone Ugolini)

Algoritmo probabilistico per trovare una radice quadrata di -1 modulo $p \equiv 1 \pmod{4}$.

Scrittura di un primo dispari $p \equiv 1 \pmod{4}$ come somma di due quadrati. Esempio.

Lezione 3. lunedí 24 settembre 2018 (2 ore)

Radici quadrate modulo un primo congruo a 3 modulo 4.

Testa o croce per telefono, e radici quadrate modulo pq, con p, q primi distinti (congrui a 3 modulo 4).

Gruppo delle permutazioni su un insieme.

Lezione 4. mercoledí 26 settembre 2018 (2 ore)

Esempio svolto di testa/croce per telefono.

Permutazioni. Il gruppo simmetrico S_n. Notazione ciclica. Scrittura di una permutazione come prodotto di cicli disgiunti. Esempi.

S_n non è abeliano se $n \geq 3$.

Classi laterali sinistre.

Date: Trento, A. A. 2018/19.

Lezione 5. lunedí 1 ottobre 2018 (2 ore)

Le classi laterali sinistre formano una partizione. Due classi laterali hanno lo stesso numero di elementi. Teorema di Lagrange. L'ordine di un elemento di un gruppo finito divide l'ordine del gruppo.

Classi laterali destre.

In generale, classi laterali sinistre e destre differiscono. Sottogruppi normali: gruppi abeliani, esempi in S_3.

I sottogruppi di $\mathbf{Z}$ sono tutti e soli della forma $n\mathbf{Z}$, per $n \geq 0$. I sottogruppi di $\mathbf{Z}$ sono anche sottoanelli. Ideali. I sottogruppi di $\mathbf{Z}$ sono anche ideali.

Lezione 6. mercoledí 3 ottobre 2018 (2 ore)

Se R è una relazione di equivalenze compatibile con le operazioni di un anello A, allora

(1) $[0]$ è un ideale di A;
(2) le classi di equivalenza sono le classi laterali di $[0]$ in A;
(3) aRb se e solo se $a - b \in [0]$.

Viceversa, se I è un ideale dell'anello A, allora

(1) la congruenza modulo I

$$aRb \quad \text{se e solo se} \quad a - b \in I$$

è un relazione di equivalenza compatibile con le operazioni;
(2) $[0] = I$;
(3) le classi di equivalenza sono le classi laterali di $[0]$ in A.

Dunque l'insieme A/R delle classi di equivalenza è la stessa cosa dell'insieme A/I delle classi laterali, ed è un anello con le operazioni

$$(a + I) + (b + I) = (a + b) + I, \qquad (a + I) \cdot (b + I) = ab + I,$$

Siano A, C anelli, e $f : A \to C$ un morfismo suriettivo. La relazione su A data da aRb se e solo se $f(a) = f(b)$ ha $[0] = \{\, a \in A : aR0 \,\} = \{\, a \in A : f(a) = 0 \,\} = \ker(f)$, dunque $\ker(f)$ è un ideale di A, e si ha il primo teorema di isomorfismo, con $A/\ker(f)$ al posto di A/R.

Moltiplicazione di un sottoinsieme per un elemento in un gruppo. Se G è un gruppo, e N un suo sottogruppo, sono equivalenti:

(1) per ogni $a \in G$, si ha $aN = Na$;
(2) per ogni $a \in G$, si ha $a^{-1}Na = N$;
(3) per ogni $a \in G$, si ha $a^{-1}Na \subseteq N$;
(4) per ogni $a \in G$ e ogni $n \in N$, si ha $a^{-1}na \in N$.

Se R è una relazione di equivalenza compatibile su un gruppo G, allora $[1]$ è un sottogruppo normale, e poi come per gli anelli.

Viceversa. Primo teorema di isomorfismo per i gruppi.

Lezione 7. lunedí 8 ottobre 2018 (2 ore)

Estensioni di un campo. Estensioni come spazi vettoriali.

Ideali principali, legami con la divisione e la relazione di "essere associato".

Gli ideali di un dominio euclideo sono principali.

Lemma: un morfismo fra anelli è iniettivo se e solo se il nucleo è contiene il solo 0.

Valutazione dei polinomi in un elemento. Caso trascendente e caso algebrico.

Lezione 8. mercoledí 10 ottobre 2018 (2 ore)

Il caso algebrico: polinomio minimo, teoria della struttura delle estensioni semplici.

Struttura dell'anello quoziente $F[x]/(m)$, con m polinomio di grado positivo. Come per gli interi, si ha che ogni elemento di $F[x]/(m)$ si scrive in modo unico nella forma $r + (m)$, ove $N(r) < N(m)$ (qui N è la norma euclidea sui polinomi).

Basi e dimensioni di $F[x]/(m)$ e di $F[\alpha]$. Grado di una estensione.

Se un polinomio monico si annulla su α, ed è irriducibile, allora è il polinomio minimo. Un esempio di polinomio minimo non irriducibile.

Lezione 9. lunedí 15 ottobre 2018 (2 ore)

Se B è un dominio (dunque a maggior ragione se B è un campo), allora ogni polinomio minimo di $\alpha \in B$ algebrico su F è irriducibile, e $F[\alpha]$ è un campo.

Si ha

$$F[x]/(m) \begin{cases} \text{è un campo,} & \text{se } m \text{ è irriducibile;} \\ \text{non è un dominio,} & \text{se } m \text{ è riducibile.} \end{cases}$$

Irriducibilità di polinomi di grado basso.

Polinomi minimi su $\mathbf{Q}$ di $\sqrt{2}$ e $\sqrt[3]{2}$, e di i su $\mathbf{R}$.

Lezione 10. mercoledí 17 ottobre 2018 (2 ore)

$\mathbf{Q}[\sqrt[3]{2}]$ e la razionalizzazione.

Il polinomio minimo di $\sqrt{2} + \sqrt{3}$ su $\mathbf{Q}$. Il candidato è di quarto grado: le sue radici sono $\pm\sqrt{2} \pm \sqrt{3}$: nessuna di loro è razionale, per il teorema della radice razionale.

Estensioni ripetute. Formula dei gradi (senza dimostrazione).

Lezione 11. lunedí 22 ottobre 2018 (2 ore)

In una estensione di grado finito ogni elemento è algebrico, di grado (del polinomio minimo) che divide il grado dell'estensione.

Estensioni algebriche.

Lemma di Gauss e conseguenze.

Lemma di Eisenstein.

I numeri algebrici (sottointeso: su $\mathbf{Q}$) formano una estensione algebrica, di grado infinito sui razionali.

Lezione 12. mercoledí 24 ottobre 2018 (2 ore)

Lemma di Eisenstein e polinomio minimo di una radice primitiva p-sima dell'unità, per p primo. Cambio di variabile in un anello di polinomi.

Per un intero $n > 0$ sono equivalenti:

(1) n è primo, e

(2) n divide $\binom{n}{i}$ per ogni $0 < i < n$.

L'insieme dei numeri algebrici è numerabile.

Campo dei quozienti di un dominio. (Inizio.)

Lezione 13. venerdí 26 ottobre 2018 (3 ore)

Prima provetta intermedia.

Lezione 14. lunedí 29 ottobre 2018 (2 ore)

Campo dei quozienti di un dominio. (Fine.)

Esistenza di una radice di un polinomio in una estensione.

Matrice compagna.

Campo di spezzamento di un polinomio. (Inizio.)

Lezione 15. mercoledí 31 ottobre 2018 (2 ore)

Campo di spezzamento di un polinomio. (Fine.)

Esistenza, cenno all'unicità.

Caratteristica di un anello con unità. Sottoanello primo: il più piccolo sottoanello A con unità di un anello con unità è isomorfo a $\mathbf{Z}$ (e allora si dice che A ha caratteristica 0) o a $\mathbf{Z}/n\mathbf{Z}$ (e allora si dice che A ha caratteristica n). Se A ha caratteristica $n > 0$, allora $na = 0$ per ogni $a \in A$.

La caratteristica di un campo E è o 0 (e allora E è estensione di $\mathbf{Q}$) o un numero primo p (e allora E è estensione di $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$).

Lezione 16. lunedí 5 novembre 2018 (2 ore)

Un campo finito E di caratteristica $p > 0$ ha ordine p^n, ove $n = |E : \mathbf{F}_p|$.

Gli elementi di un campo E di ordine p^n, ove p è un primo, sono le radici di $x^{p^n} - x \in \mathbf{F}_p[x]$.

Derivata formale di un polinomio: proprietà. Radici semplici, radici multiple. Sia f un polinomio non nullo in $F[x]$, ove F è un campo, e sia L un campo di spezzamento di f su F. Allora $\alpha \in L$ è una radice multipla di f se e solo se α è radice di $\gcd(f, f')$. In particolare f ha tutte radici semplici (nel suo campo di spezzamento) se e solo se $\gcd(f, f') = 1$.

Le radici di $f = x^{p^n} - x \in \mathbf{F}_p[x]$ sono distinte. Le radici di f in un campo di spezzamento su F_p formano un campo, dunque un campo con p^n elementi. L'unicità del campo di spezzamento ci garantisce che questo campo è unico (in qualche senso).

Teorema (senza dimostrazione): Sia E un campo. Sia G un sottogruppo finito del gruppo moltiplicativo E^*. Allora G è ciclico, cioè esiste $\alpha \in G$ tale che $G = \langle \alpha \rangle$.

Lezione 17. mercoledí 7 novembre 2018 (2 ore)

Polinomi irriducibili in $\mathbf{F}[x]$ nei casi $\mathbf{F} = \mathbf{Q}, \mathbf{R}$ o $\mathbf{C}$.

Polinomi irriducibili di grado $2, 3, 4$ su $\mathbf{F}_2$. Costruzione di un campo di ordine 4 e di un campo di ordine 8. Polinomi minimi su $\mathbf{F}_2$ di tutti gli elementi.

Lezione 18. lunedí 12 novembre 2018 (2 ore)

I polinomi irriducibili di grado 4 su $\mathbf{F}_2$. Costruzione del campo con $2^4 = 16$ elementi.

Non sempre le radici del polinomio scelto generano il gruppo moltiplicativo: polinomi primitivi.

Morfismo di Frobenius e radici di un polinomio irriducibile. Le radici di un polinomio f di grado n irriducibile in $\mathbf{F}_p[x]$ sono gli elementi α^{p^i} dove $0 \leq i \leq n-1$ e α è una radice qualunque di f (senza dimostrazione).

Polinomi irriducibili di grado 2 su $\mathbf{F}_3$. Costruzione di un campo di ordine 9: dipendenza dalla scelta del polinomio irriducibile. Polinomi minimi di tutti gli elementi.

Logaritmo discreto. Polinomi minimi di tutti gli elementi.

Codici a rivelazione e correzione d'errore (inizio).

Lezione 19. mercoledí 14 novembre 2018 (2 ore)

Codice $\mathcal{C}_2$ a ripetizione due volte e $\mathcal{C}_3$ a ripetizione tre volte.

L'introduzione di un errore equivale a passare da $c \in \mathcal{C}$ a $c + e_i$ per qualche i.

Distanza di Hamming e sue proprietà. Distanza minima di un codice: caso dei codici lineari.

Un codice $\mathcal{C}$ rivela un errore se $d(\mathcal{C}) > 1$.

Lezione 20. lunedí 19 novembre 2018 (2 ore)

Un codice $\mathcal{C}$ corregge un errore se $d(\mathcal{C}) > 2$.

Codice a controllo di parità. Matrice di un codice e matrice di controllo di parità.

Un codice rivela un errore se e solo se le colonne di una matrice di controllo di parità sono tutte diverse da zero.

Lezione 21. mercoledí 21 novembre 2018 (2 ore)

Un codice corregge un errore se e solo se le colonne di una matrice di controllo di parità sono tutte diverse da zero, e distinte.

Codice di Hamming basato sul polinomio di $x^3 + x + 1 \in \mathbf{F}_2[x]$.

Ciclicità del codice.

Lezione 22. venerdí 23 novembre 2018 (3 ore)

Seconda provetta intermedia.

Lezione 23. lunedí 26 novembre 2018 (2 ore)

Codice di Hamming basato sul polinomio di $x^3 + x^2 + 1 \in \mathbf{F}_2[x]$, e relazioni col precedente.

Il codice di Hamming in generale. I codici di Hamming basasti su $x^4 + x^1 + 1 \in \mathbf{F}_2[x]$ e su $x^2 + x + 1 \in \mathbf{F}_2[x]$.

Lezione 24. mercoledí 28 novembre 2018 (2 ore)

Se $H, K \leq G$, in generale HK può non essere un sottogruppo: esempio in S_3.
Se $H \leq G$ e $N \trianglelefteq G$, allora $HN \leq G$.
Secondo teorema di isomorfismo per i gruppi.
Applicazione:

$$ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b).$$

Immagini e controimmagini sotto una funzione.
Terzo teorema di isomorfismo per i gruppi: prima parte.

Lezione 25. lunedí 3 dicembre 2018 (2 ore)

Terzo teorema di isomorfismo: seconda e terza parte.
Sottogruppi dei gruppi ciclici: col terzo teorema.
Ancora

$$ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b).$$

Secondo e terzo teorema di isomorfismo per anelli.
Divisibilità e ideali principali in un dominio.
Anelli noetheriani.
L'unione cresce di ideali è un ideale.
Un PID è noetheriano. (Inizio.)

Lezione 26. mercoledí 5 dicembre 2018 (2 ore)

Un PID è noetheriano. (Fine.)
Sottogruppi dei gruppi ciclici: direttamente.
In un PID, un elemento $a \neq 0$, a non una unità, è divisibile per un irriducibile.
In un PID, ogni elemento si scrive come prodotto di irriducibili.
In un PID, gli irriducibili sono primi.
Un PID è un UFD.

Lezione 27. lunedí 10 dicembre 2018 (2 ore)

Lemma di Gauss e questioni collegate. (Inizio.)

Lezione 28. mercoledí 12 dicembre 2018 (2 ore)

Lemma di Gauss e questioni collegate. (Fine.)
Presentazione relativa al codice di Hamming. Piano di Fano.

Lezione 29. mercoledí 19 dicembre 2018 (2 ore)

Lezione tenuta da Simone Ugolini.

Lezione 30. venerdí 21 dicembre 2018 (3 ore)

Terza provetta intermedia.

Dipartimento di Matematica, Università degli Studi di Trento, via Sommarive 14, 38123 Trento
E-mail address: andrea.caranti@unitn.it
URL: http://www.science.unitn.it/∼caranti/