DIARIO DEL CORSO DI ALGEBRA B

A.A. 2020/21

DOCENTE: ANDREA CARANTI

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

Lezione 1. lunedí 14 settembre 2020 (2 ore)

(Lezione tenuta da Simone Ugolini)

Quadrati modulo p (ripasso). Se $b \in \mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ è un quadrato non nullo e $p \equiv 3 \pmod 4$, allora $b^{\frac{p+1}{4}}$ è una radice quadrata di b modulo p. Testa o croce per telefono e radici quadrate modulo pq, con p, q primi distinti (congrui a 3 modulo 4). Esempio di testa o croce per telefono (inizio).

Lezione 2. mercoledí 16 settembre 2020 (2 ore)

(Lezione tenuta da Simone Ugolini)

Esempio di testa o croce per telefono (conclusione). Gruppo delle permutazioni su un insieme. Il gruppo simmetrico S_n. Il gruppo S_n non è abeliano se $n \geq 3$. Notazione matriciale e ciclica per le permutazioni. Scrittura di una permutazione come prodotto di cicli disgiunti. Esempi. Scrittura di una permutazione come prodotto di trasposizioni (non disgiunte). Se una permutazione si scrive come prodotto di h e k trasposizioni, allora $h \equiv k \pmod 2$ (solo enunciato).

Lezione 3. lunedí 21 settembre 2020 (2 ore)

Il gruppo diedrale.

Classi laterali sinistre e destre. La classi laterali sinistre e destre sono le classi di certe relazioni di equivalenza, e dunque formano una partizione del gruppo in cui si prendono.

Lezione 4. mercoledí 23 settembre 2020 (2 ore)

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 $n \geq 0$.

Le classi laterali di $n\mathbf{Z}$ sono le classi di congruenza modulo n.

I sottogruppi di $\mathbf{Z}$ sono anche sottoanelli. Ideali. I sottogruppi di $\mathbf{Z}$ sono anche ideali.

Date: Trento, A. A. 2020/21.

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

(1) $[0]$ è un ideale di A;

Lezione 5. lunedí 28 settembre 2020 (2 ore)

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

(1) le classi di equivalenza sono le classi laterali di $[0]$ in A;
(2) 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 6. mercoledí 30 settembre 2020 (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: il polinomio minimo.

Lezione 7. lunedí 5 ottobre 2020 (2 ore)

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 $F[\alpha]$. La dimensione di $F[\alpha]$ come spazio vettoriale su F (detta grado di $F[\alpha]$ su F, e denotata con $|F[\alpha : F|$) coincide con il grado n del polinomio minimo di α su F: una base di $F[\alpha]$ come spazio vettoriale su F è data da $1, \alpha, \ldots, \alpha^{n-1}$.

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

Irriducibilità di polinomi di grado basso in termini di radici.

Un esempio di polinomio minimo non irriducibile.

Lezione 8. mercoledí 7 ottobre 2020 (2 ore)

Il polinomio minimo di i su $\mathbf{R}$, e una costruzione dei numeri complessi.

Si ha

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

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.

Polinomio minimo su $\mathbf{Q}$ di $\sqrt{2}$.

Come si comportano i polinomi minimi al variare del campo su cui li si considera.

Lezione 9. lunedí 12 ottobre 2020 (2 ore)

Polinomio minimo su $\mathbf{Q}$ di $\sqrt[3]{2}$; razionalizzazione.

Il polinomio minimo di $\sqrt{2} + \sqrt{3}$ su $\mathbf{Q}$.

Prima dimostrazione. 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. Il polinomio candidato non ha neanche fattori irriducibili di secondo grado.

Seconda dimostrazione. Estensioni ripetute.

Lezione 10. mercoledí 14 ottobre 2020 (2 ore)

Conclusione della determinazione del polinomio minimo di $\sqrt{2} + \sqrt{3}$ su $\mathbf{Q}$.

Formula dei gradi (senza dimostrazione).

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 (solo enunciato su $\mathbf{Z}$) e conseguenze.

Lezione 11. lunedí 19 ottobre 2020 (2 ore)

Lemma di Eisenstein. Due dimostrazioni: diretta, e mediante la riduzione dei coefficienti modulo p.

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 $0 < i < n$.

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

Lezione 12. mercoledí 21 ottobre 2020 (2 ore)

Campo dei quozienti di un dominio.

Esistenza di una radice di un polinomio in una estensione: metodo con un quoziente dell'anello dei polinomi.

Lezione 13. lunedí 26 ottobre 2020 (2 ore)

Esistenza di una radice di un polinomio in una estensione: metodo con la matrice compagna.

Campo di spezzamento di un polinomio.

Esistenza, cenno all'unicità.

Lezione 14. mercoledí 28 ottobre 2020 (2 ore)

Cayley-Hamilton.

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 $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$).

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

Lezione 15. lunedí 2 novembre 2020 (2 ore)

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 $G = \langle \alpha \rangle$.

Costruzione di un campo di ordine 4. Polinomi irriducibili su $\mathbf{F}_2$ di grado 3.

Lezione 16. mercoledí 4 novembre 2020 (1 ora)

Le radici del polinomio $x^2 + x + 1 \in \mathbf{Q}[x]$ in $\mathbf{C}$: le due radici sono coniugate.

Le radici del polinomio $x^2 + x + 1 \in \mathbf{F}_2[x]$ nel suo campo di spazzamento sopra $\mathbf{F}_2$: se α è una radice, l'altra è $\alpha^2 = 1 + \alpha$.

Logaritmo discreto e protocollo di scambio delle chiavi di Diffie-Hellman.

Logaritmo discreto nel campo con 8 elementi ottenuto mediante il polinomio $x^3 + x + 1$.

Lezione 17. lunedí 9 novembre 2020 (2 ore)

Polinomi minimi su $\mathbf{F}_2$ di tutti gli elementi di un campo con 8 elementi.

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

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.

Lezione 18. mercoledí 11 novembre 2020 (2 ore)

Morfismo di Frobenius: manda radici in radici di un polinomio in $\mathbf{F}_p[x]$. Ordine del morfismo di Frobenius.

Un campo con p^n elementi contiene un campo con p^m elementi se e solo se $m \mid n$.

Codici a rivelazione e correzione d'errore.

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

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

Lezione 19. lunedí 16 novembre 2020 (2 ore)

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

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

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.

Lezione 20. mercoledí 18 novembre 2020 (2 ore)

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

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.

Codifica e decodifica mediante operazioni lineari che coinvolgono una matrice del codice, e una matrice di controllo della parità.

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

Lezione 21. lunedí 23 novembre 2020 (2 ore)

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

Ciclicità del codice.

Il codice di Hamming basato sul polinomio $x^2 + x + 1 \in \mathbf{F}_2[x]$ è il codice a ripetizione tre volte.

Il codice di Hamming in generale.

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

Lezione 22. mercoledí 25 novembre 2020 (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.

Immagini e controimmagini sotto una funzione.

Terzo teorema di isomorfismo per i gruppi.

Applicazione:

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

Lezione 23. lunedí 30 novembre 2020 (2 ore)

Sottogruppi dei gruppi ciclici: col terzo teorema.

Secondo e terzo teorema di isomorfismo per anelli.

Unione di due ideali: quando è un ideale.

L'unione crescente di ideali è un ideale.

Ideali finitamente generati. Elementi massimi e massimali in un insieme parzialmente ordinato.

Anelli noetheriani: caratterizzazione.

Lezione 24. mercoledí 2 dicembre 2020 (2 ore)

Teorema della base di Hilbert.

Se A è un dominio, allora l'anello dei polinomi $A[x]$ è un PID se e solo e A è un campo.

Se A è un dominio, e $0 \neq p \in A$ non è una unità, allora $A/(p)$ è un dominio se e solo se p è primo.

Se A è un PID, e $0 \neq p \in A$ non è una unità, allora p è irriducibile se e solo se $A/(p)$ è un campo.

In un PID, gli irriducibili sono primi.

Lezione 25. mercoledí 9 dicembre 2020 (2 ore)

$\mathbf{Z}[x]$ non è un PID: $(2, x)$ non è un ideale principale, e 2 è irriducibile, ma $\mathbf{Z}[x]/(2)$ non è un campo.

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.

Interi algebrici: la somma e il prodotto di due interi algebrici è ancora un intero algebrico.

Lezione 26. lunedí 14 dicembre 2020 (2 ore)

(Lezione tenuta da Simone Ugolini)

Se D è un UFD e $a \in D$ è diverso da 0 e non unità, allora $a = \varepsilon p_1^{e_1} \dots p_k^{e_k}$ ove ε è un'unità in D, i p_i sono irriducibili e a due a due non associati in D e ogni e_i è un intero positivo. Tale fattorizzazione inoltre è unica a meno di riordinamento dei fattori irriducibili e a meno di unità. Massimo comune divisore (MCD) di n elementi in un dominio. Un MCD non esiste sempre. Quando esiste, il MCD è unico a meno di invertibili.

Siano $a_1, \dots, a_n$ elementi di un dominio D in cui è possibile calcolare il MCD. Se $c \in D$, allora $\gcd(ca_1, \dots, ca_n) = c \gcd(a_1, \dots, a_n)$. Inoltre, se gli a_i non sono tutti nulli, si ha che $d = \gcd(a_1, \dots, a_n) \neq 0$ e $\gcd\left(\frac{a_1}{d}, \dots, \frac{a_n}{d}\right) = 1$.

Sia D un UFD e siano $a_1, \dots, a_n$ elementi non nulli in D la cui fattorizzazione è

$$a_i = \varepsilon_i \prod_{j=1}^{k} p_j^{e_{ij}}$$

ove ogni ε_i è un'unità, i p_j sono irriducibili a due a due non associati in D e ogni e_{ij} è un intero non negativo. Allora, definito $m_j = \min\{e_{ij} : i = 1, \dots n\}$ per $j = 1, \dots, n$, si ha che

$$d = \prod_{j=1}^{k} p_j^{m_j}$$

è un MCD di $a_1, \dots, a_n$.

Se D è un UFD e $a = a_n x^n + \dots + a_1 x + a_0 \in D[x]$ è un polinomio non nullo, allora il contenuto $C(a)$ di a è un MCD di $a_1, \dots, a_n$. Se $C(a) = 1$ diciamo che a è primitivo.

Se $f \in D[x]$ è un polinomio non nullo, allora $f = cf_1$, ove $c = C(f)$ e f_1 è un polinomio primitivo in $D[x]$.

Se $f, g \in D[x]$ sono due polinomi non nulli e primitivi e $cf = dg$, ove $c, d \in D$ sono non nulli, allora $d = cu$ per qualche unità $u \in D$.

Lezione 27. mercoledí 16 dicembre 2020 (2 ore)

(Lezione tenuta da Simone Ugolini)

Sia D un UFD e sia F il suo campo dei quozienti.

Sia $f \in F[x]$ un polinomio non nullo. Allora esiste $\alpha \in F$ tale che $f = \alpha f_1$ per qualche polinomio primitivo $f_1 \in D[x]$. Inoltre, se $f = \alpha f_1 = \beta f_2$ con $\alpha, \beta \in F$ e f_1, f_2 primitivi in $D[x]$, allora $\beta = \alpha u$ con u unità in D.

Siano $f, g \in D[x]$ due polinomi non nulli e primitivi. Se $g = \alpha f$ per qualche $\alpha \in F$, allora $\alpha \in D$ e α è un'unità in D.

Lemma di Gauss: se $f, g \in D[x]$ sono primitivi, allora fg è primitivo.

Se $f \in D[x]$ è un polinomio di grado positivo e irriducibile in $D[x]$, allora

- f è primitivo in $D[x]$;
- f è irriducibile in $F[x]$.

Se D è un UFD, allora $D[x]$ è un UFD.

Lezione 28. lunedí 21 dicembre 2020 (2 ore)

Sette domande, una menzogna: il codice di Hamming di lunghezza 7 e il piano di Fano.

Dipartimento di Matematica, Università degli Studi di Trento, via Sommarive 14, 38123 Trento

Email address: andrea.caranti@unitn.it

URL: http://www.science.unitn.it/∼caranti/