DIARIO DEL CORSO DI ALGEBRA B

A.A. 2022/23

DOCENTE: ANDREA CARANTI

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

Lezione 1. martedí 13 settembre 2022 (2 ore)

Quadrati modulo p (ripasso).

Dato un primo dispari, e un quadrato $b \in \mathbf{Z}/p\mathbf{Z}$, esiste un algoritmo per trovare una radice quadrata di b. Questo algoritmo richiede il passaggio (che si sa fare solo in termini probabilistici) di trovare prima un non-quadrato.

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.

Lezione 2. giovedí 15 settembre 2022 (2 ore)

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).

Parità di una permutazione: se una permutazione si scrive come prodotto di h e k trasposizioni, allora $h \equiv k \pmod 2$ (solo enunciato).

Il gruppo diedrale: inizio.

Lezione 3. martedí 20 settembre 2022 (2 ore)

Il gruppo diedrale.

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

Due classi laterali hanno lo stesso numero di elementi. Teorema di Lagrange.

Lezione 4. giovedí 22 settembre 2022 (2 ore)

Un gruppo di ordine un primo è ciclico.

L'ordine di un elemento di un gruppo finito divide l'ordine del gruppo.

D_3 e D_4 e (alcuni dei) loro sottogruppi.

Classi laterali destre.

Date: Trento, A. A. 2022/23.

In generale, classi laterali sinistre e destre differiscono. Definzione di sottogruppo normale: gruppi abeliani, esempi in D_3 e D_4.

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.

Lezione 5. martedí 27 settembre 2022 (2 ore)

Gruppi ciclici.

Un sottogruppo di indice 2 è normale. Già per indice 3 non vale più.

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

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

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

(1) $[0]$ è un ideale di A;
(2) xRa se e solo se $x - a \in [0]$;
(3) le classi di equivalenza sono le classi laterali di $[0]$ in A, cioè $[a] = a + [0]$.

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 (questo lo sappiamo già, è quella che dà luogo alle classi laterali, ma in più è) compatibile con le operazioni;
(2) $[0] = I$;
(3) le classi di equivalenza sono le classi laterali di I 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

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

Nucleo di un morfismo di anelli.

Siano A, C anelli, e $f : A \to C$ un morfismo suriettivo. Per la relazione su A data da aRb se e solo se $f(a) = f(b)$ si ha

$$[0] = \{\, a \in A : aR0 \,\} = \{\, a \in A : f(a) = f(0) = 0 \,\} = \ker(f),$$

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.

Gli ideali sono esattamente i nuclei dei morfismi.

Lezione 6. giovedí 29 settembre 2022 (2 ore)

Moltiplicazione di un sottoinsieme per un elemento in un gruppo.

Proprietà equivalenti all'essere un sottogruppo normale: 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,

(1) $[1]$ è un sottogruppo normale di G;
(2) xRa se e solo se $a^{-1}x \in [a]$;
(3) le classi di equivalenza sono le classi laterali di $[1]$ in G, cioè $[a] = a[1]$.

Viceversa, se N è un sottogruppo normale del gruppo G, allora

(1) la congruenza modulo N

$$aRb \quad \text{se e solo se} \quad a^{-1}b \in N$$

è un relazione di equivalenza (questo lo sappiamo già, è quella che dà luogo alle classi laterali, ma in più è) compatibile con le operazioni;
(2) $[1] = N$;
(3) le classi di equivalenza sono le classi laterali di N in G.

Dunque l'insieme G/R delle classi di equivalenza è la stessa cosa dell'insieme G/N delle classi laterali, ed è un gruppo con l'operazione

$$(aN) \cdot (bN) = (ab) \cdot N.$$

Nucleo di un morfismo di gruppi.

Siano G, H gruppi, e $f : G \to H$ un morfismo suriettivo. Per la relazione su G data da aRb se e solo se $f(a) = f(b)$ si ha

$$[1] = \{\, a \in G : aR1 \,\} = \{\, a \in G : f(a) = f(1) = 1 \,\} = \ker(f),$$

dunque $\ker(f)$ è un sottogruppo normale di G, e si ha il primo teorema di isomorfismo, con $G/\ker(f)$ al posto di G/R.

Riformulazione esplicita del primo teorema di isomorfismo per i gruppi, e di quello per gli anelli.

Lezione 7. martedí 4 ottobre 2022 (2 ore)

Estensioni di un campo. Estensioni come spazi vettoriali. Dimensione (grado) di una estensione.

Ideali principali in un anello commutativo con unità, legami con la relazione di divisibilità e la relazione di "essere associato".

Gli ideali di un dominio euclideo sono principali: un ideale diverso da zero è generato da un suo elemento m di norma minima. Caso particolare: se il dominio è l'anello dei polinomi $F[x]$, con F un campo, si può prendere m monico, e allora è unico.

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

Valutazione dei polinomi in un elemento. Caso trascendente e caso algebrico: il polinomio minimo.

Lezione 8. giovedí 6 ottobre 2022 (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.

Un esempio di polinomio minimo non irriducibile.

Si ha

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

Lezione 9. martedí 11 ottobre 2022 (2 ore)

In un PID c'è il MCD, anche se non è detto che ci sia un algoritmo per determinarlo. Unicità a meno di un'unità: il caso dei polinomi.

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.

Irriducibilità di polinomi di grado basso in termini di radici.

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

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

Lezione 10. giovedí 13 ottobre 2022 (2 ore)

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

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

Il polinomio minimo di $\sqrt{2} + \sqrt{3}$ su $\mathbf{Q}$ è $x^4 - 10x^2 + 1$.

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: calcolo del grado dell'estensione, e dunque del grado del polinomio minimo. Estensioni ripetute.

Lezione 11. martedí 18 ottobre 2022 (2 ore)

Formula dei gradi (quasi 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.

Una estensione di grado finito è algebrica.

Somma e prodotti di elementi algebrici sono algebrici; l'inverso di un elemento diverso da zero.

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

Lemma di Eisenstein (enunciato).

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

Prima dimostrazione diretta del Criterio di Eisenstein.

Lezione 12. giovedí 20 ottobre 2022 (2 ore)

Estensione della proprietà universale dell'anello dei polinomi, e dimostrazione del Criterio di Eisenstein mediante la riduzione dei coefficienti modulo p.

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

Cenno ai polinomi ciclotomici.

Per un intero $n > 0$ sono equivalenti:

(1) n è primo, e
(2) n divide $\binom{n}{i}$ per ogni $0 < i < n$.

Campo dei quozienti di un dominio.

Lezione 13. lunedí 24 ottobre 2022 (2 ore)

Ancora sul campo dei quozienti,

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

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

Polinomio minimo di i su $\mathbf{R}$, e due costruzioni dei numeri complessi.

Un campo in cui un polinomio (monico) non costante ha tutte le sue radici (inizio).

Lezione 14. martedí 25 ottobre 2022 (2 ore)

Campo di spezzamento di un polinomio.

Esistenza, cenno all'unicità.

Cayley-Hamilton mediante il campo di spezzamento.

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).

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 15. giovedí 27 ottobre 2022 (2 ore)

(Una parentesi sulla costruzioni degli insiemi di numeri.)

Se A ha caratteristica $n > 0$, allora $na = 0$ per ogni $a \in A$.

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

Se esiste un campo E di ordine p^n, ove p è un primo, allora i suoi elementi sono le radici di $f = x^{p^n} - x \in \mathbf{F}_p[x]$.

Le radici di f in un campo di spezzamento su F_p formano un sottoanello, che è dunque un campo, perché è un dominio finito., dunque un campo con p^n elementi.

Derivata formale di un polinomio: proprietà. Radici semplici, radici multiple. Sia g un polinomio non nullo in $F[x]$, ove F è un campo, e sia L un campo di

spezzamento di g su F. Se $\alpha \in L$ è una radice multipla di g, allora α è radice di $\gcd(g, g')$.

Ne segue che le radici di $f = x^{p^n} - x \in \mathbf{F}_p[x]$ sono distinte, e quindi abbiamo costruito un campo con p^n elementi.

Lezione 16. giovedí 3 novembre 2022 (2 ore)

[Lezione tenuta da Irene Villa]

Ripasso caratteristica nulla e positiva per anelli, domini e campi finiti.

Dato un polinomio f a coefficienti in un campo F, una radice di f in qualche estensione di F è radice multipla se e solo se è radice anche di $\gcd(f, f')$,

Ripasso. Un campo finito estensione di grado n di $\mathbf{F}_p$ è l'insieme delle radici di $x^{p^n} - x \in \mathbf{F}_p[x]$.

Per un campo finito, il gruppo moltiplicativo è un gruppo ciclico (senza dimostrazione).

Costruzione di campi finiti su $\mathbf{F}_2$: estensioni di grado 2, 3 e 4. (Polinomi irriducibili di grado 2, 3 e 4 su $\mathbf{F}_2$.)

Lezione 17. martedí 8 novembre 2022 (2 ore)

L'unicità del campo di spezzamento ci garantisce che questo campo è unico (in qualche senso).

Osservazione: se E è un campo finito di ordine p^n, allora esiste un elemento α di ordine $p^n - 1$, e vale $F_p[\alpha]$. Ma se $F_p[\alpha]$ è un campo finito di ordine p^n, non è detto che α abbia ordine $p^n - 1$.

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 $0 \leq i < n$ e α è una radice qualunque di f (con dimostrazione solo in un verso).

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

Un campo finito di ordine 9. Un polinomio monico e irriducibile di grado 3 in $\mathbf{F}_3[x]$.

Lezione 18. giovedí 10 novembre 2022 (2 ore)

Codici a rivelazione e correzione d'errore: l'esempio delle date.

Codice fiscale. ISBN-10.

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: cambiare 0 in 1 o viceversa si ottiene aggiungendo 1.

Distanza di Hamming e sue proprietà. Distanza minima $d(\mathcal{C})$ di un codice $\mathcal{C}$: il caso dei codici lineari.

Lezione 19. martedí 15 novembre 2022 (2 ore)

Un codice $\mathcal{C}$

- rivela un errore se e solo se $d(\mathcal{C}) > 1$,
- corregge un errore se e solo se $d(\mathcal{C}) > 2$.

Codice a controllo di parità. Matrice di un codice e matrice di controllo di parità: come si passa dalla seconda alla prima. Codici duali.

Lezione 20. giovedí 17 novembre 2022 (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.

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

Ciclicità del codice.

Lezione 21. lunedí 21 novembre 2022 (2 ore)

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

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.

Un cenno ai codici BCH.

Lezione 22. martedí 22 novembre 2022 (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.

Lezione 23. giovedí 24 novembre 2022 (2 ore)

[Lezione tenuta da Irene Villa]

Terzo teorema di isomorfismo per i gruppi.

Un commento su $|x\mathbf{Z}/y\mathbf{Z}| = y/x$ usando il terzo teorema: se $y \neq 0$, e $x \mid y$, allora

$$(\mathbf{Z}/y\mathbf{Z})/(x\mathbf{Z}/y\mathbf{Z}) \cong \mathbf{Z}/x\mathbf{Z}.$$

Sottogruppi dei gruppi ciclici: col terzo teorema.

Secondo e terzo teorema di isomorfismo per anelli.

Unione di due ideali I e J è un ideale se e solo se $I \subseteq J$ o $I \supseteq J$.

Lezione 24. martedí 29 novembre 2022 (2 ore)

L'unione crescente di ideali è un ideale.

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

Anelli noetheriani: caratterizzazione.

Teorema della base di Hilbert.

Lezione 25. giovedí 1 dicembre 2022 (2 ore)

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

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.

$\mathbf{Z}[x]$ 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.

Lezione 26. martedí 6 dicembre 2022 (2 ore)

Un PID è un UFD.

Codice di Hamming e piano di Fano.

Lezione 27. martedí 13 dicembre 2022 (2 ore)

[Lezione tenuta da Irene Villa]

Il contenuto di un polinomio su $\mathbf{Z}[x]$ e su $\mathbf{Q}[x]$, polinomi primitivi. Il prodotto di polinomi primitivi è primitivo. L'unicità del contenuto, a meno di unità in $\mathbf{Z}$. Un polinomio irriducibile in $\mathbf{Z}[x]$ lo è anche in $\mathbf{Q}[x]$ (il viceversa non vale) e $\mathbf{Z}[x]$ è un UFD.

Lezione 28. giovedí 15 dicembre 2022 (2 ore)

[Lezione tenuta da Irene Villa]

Massimo comun divisore in un dominio generico: definizione, unicità (a meno di unità), esempio in $\mathbf{Z}[\sqrt{-5}]$ dove non esiste.

Quanto visto nella lezione precedente risulta valido anche per il massimo comun divisore in un dominio generico (dove esiste).

Definizione di polinomio primitivo e di contenuto per polinomi in $D[x]$ e in $F[x]$, ove D è un UFD e F il suo campo dei quozienti.

Il prodotto di polinomi primitivi è primitivo, il contenuto di un polinomio in $F[x]$ è unico a meno di unità in D e il contenuto del prodotto di due polinomi è associato al prodotto del contenuto dei polinomi ($C(fg) \sim C(f)C(g)$).

Teorema: un polinomio in $D[x]$ (di grado positivo) irriducibile in $D[x]$ è anche irriducibile in $F[x]$. $D[x]$ è un UFD.

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

Email address: andrea.caranti@unitn.it

URL: https://caranti.maths.unitn.it