DIARIO DEL CORSO DI ALGEBRA

A.A. 2015/16

DOCENTE: ANDREA CARANTI

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

Lezione 1. martedí 15 settembre 2015 (2 ore)

Presentazione del corso.

Esercizio: cosa succede a moltiplicare per $2, 3, 4, \dots$ il numero

$$142857,$$

e perché?

Divisibilità fra interi. Proprietà riflessiva e transitiva.

Non vale la proprietà simmetrica. Determinazione delle coppie (a, b) tali che a divide b e b divide a. Determinazione delle coppie (x, y) di interi tali che $xy = 1$.

Divisione con resto non negativo. Il caso del dividendo negativo. Il caso del divisore negativo. Unicità di quoziente e resto.

Lezione 2. mercoledí 16 settembre 2015 (2 ore)

Ruolo di ± 1 e 0 nella divisibilità. Se a divide b e c, allora divide anche $b \pm c$.

Ancora sulla divisione con resto: dimostrazione per induzione.

Criterio di divisibilità in base all'annullarsi del resto.

Massimo comun divisore (MCD): definizione elementare. Problema: non esiste il MCD di 0 e 0.

Modalità di calcolo del MCD: l'approccio mediante la fattorizzazione fallisce con numeri "grandi".

Provare con

$$1\,000\,000\,014\,000\,000\,049 \qquad \text{e} \qquad 1\,200\,000\,049\,400\,000\,287.$$

Provare con numeri dell'ordine di grandezza di 10^{200}, tenendo presente che l'Universo ha $13.7 \cdot 10^9$ anni, che il più potente calcolatore attuale fa (approssimativamente) 33.86 petaflops, cioè $33.86 \cdot 10^{15}$ operazioni al secondo, e che la popolazione mondiale è di poco più di $7 \cdot 10^9$ abitanti.

Definizione formale del MCD fra due interi a, b. Il MCD di 0 e 0 è 0.

Sono equivalenti: d è il massimo comun divisore fra a e b, e $D(a) \cap D(b) = D(d)$. (Qui $D(c) = \{\, x \in \mathbf{Z} : x \mid c \,\}$.)

Paradosso di Russell.

Date: Trento, A. A. 2015/16.

Lezione 3. venerdí 18 settembre 2015 (2 ore)

Assioma di specificazione.

Esistenza e costruzione del MCD mediante l'algoritmo di Euclide: si comincia con il fatto che il MCD fra 0 e b è b.

"Unicità" del massimo comun divisore.

Notazione $\gcd(a, b)$ per il MCD.

L'algoritmo di Euclide su due numeri grandi all'incirca N termina in al più $2 \cdot \log_2(N)$ passi. Grafico di $y = 2^x$.

Teorema di Bézout (enunciato).

Lezione 4. lunedí 21 settembre 2015 (2 ore)

Algoritmo di Euclide esteso per esprimere il massimo comun divisore d di due numeri a, b come loro combinazione lineare $ax + by = d$, con $x, y \in \mathbf{Z}$.

Esempi dei due metodi.

Se $\gcd(a, b) = 1$, allora a e b si dicono coprimi, o primi fra loro, o relativamente primi.

a e b sono coprimi se e solo se esistono $x, y \in \mathbf{Z}$ tali che $ax + by = 1$.

Lemmi aritmetici.

Applicazione dei lemmi aritmetici: tutte le combinazioni per esprimere il massimo comun divisore come combinazione lineare.

Applicazione dei lemmi aritmetici: il minimo comune multiplo, la formula

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

e interpretazione in termini di *fattori comuni e non comuni*.

Congruenze. Basta considerare le congruenze modulo numeri non negativi. Le congruenze modulo $0, 1$.

Lezione 5. martedí 22 settembre 2015 (2 ore)

La congruenza è una relazione di equivalenza: dimostrazione

Essere congrui vuol dire avere lo stesso resto, dunque la congruenza è una relazione di equivalenza.

Classi rispetto a una relazione di equivalenza, e loro proprietà.

Relazioni di equivalenza e partizioni. Le classi formano una partizione.

Classi di congruenza (o resto) modulo un intero n. Le classi modulo 2 e 3.

Modulo n ci sono esattamente n classi resto, che sono $[0], [1], \ldots, [n-1]$. Notazione $\mathbf{Z}/n\mathbf{Z}$. Si può calcolare con le classi resto.

Lemma: n divide a se e solo se $a \equiv 0 \pmod{n}$ se e solo se $[a] = [0]$ in $\mathbf{Z}/n\mathbf{Z}$.

La prova del nove, ovvero criterio di divisibilità per 9.

Lezione 6. mercoledí 23 settembre 2015 (2 ore)

Criteri di divisibilità per 11, 3 e 7.

Esercizio proposto: trovare i numeri interi positivi il cui prodotto delle cifre faccia un numero della forma $111\ldots1$.

Le operazioni su $\mathbf{Z}/n\mathbf{Z}$ sono ben definite.

Definizione di anello.

Lezione 7. venerdí 25 settembre 2015 (2 ore)

$\mathbf{Z}$ e $\mathbf{Z}/n\mathbf{Z}$ sono anelli commutativi con unità. Quest'ultimo eredita dal primo le proprietà di anello.

Definizione di operazione (binaria), operazione associativa, semigruppo, elemento neutro, monoide e elemento simmetrico.

Elemento neutro e elemento simmetrico, se esistono, sono unici.

Notazione neutra, additiva e moltiplicativa per un monoide.

Lemma sugli inversi.

Gruppi. L'insieme degli elementi invertibili di un monoide è un gruppo.

Gli elementi invertibili in $\mathbf{Z}/n\mathbf{Z}$ sono le classi a tali che $\gcd(a, b) = 1$.

Lezione 8. lunedí 28 settembre 2015 (2 ore)

Calcolo degli inversi in $\mathbf{Z}/n\mathbf{Z}$ mediante l'algoritmo di Euclide esteso.

0-divisori. 0-divisori in $\mathbf{Z}/n\mathbf{Z}$.

Dunque $[a] \in \mathbf{Z}/n\mathbf{Z}$ è invertibile se e solo se $\gcd(a, n) = 1$, e l'inverso si trova mediante l'algoritmo di Euclide esteso. Se invece $\gcd(a, n) > 1$, allora $[a]$ è un divisore dello zero.

$\mathbf{Z}/n\mathbf{Z}$ è un campo se n è primo.

L'unico anello con unità in cui $0 = 1$ è l'anello $\{ 0 \}$.

L'unico 0-divisore in un anello è 0 se e solo se vale la legge di annullamento del prodotto.

Domini: un dominio è un anello in cui l'unico divisore dello zero è 0, ovvero in cui vale la legge di annullamento del prodotto.

In un anello finito (commutativo, con unità) gli elementi sono o invertibili o divisori dello zero.

Lemma dei cassetti (solo enunciato).

Lezione 9. mercoledí 30 settembre 2015 (2 ore)

In un anello commutativo si può semplificare per i non divisori dello zero.

Un dominio finito è un campo.

Lemma dei cassetti: relazione e partizione indotta da una funzione.

Il gruppo $U(\mathbf{Z}/n\mathbf{Z})$ delle classi invertibili modulo n. Funzione di Eulero. Valore della funzione di Eulero su piccoli numeri, e sui numeri primi.

La funzione di Eulero è moltiplicativa nel senso della teoria dei numeri (solo enunciato). Il caso in cui $n = pq$ è il prodotto di due numeri primi distinti: cenno al principio di inclusione/esclusione.

Lezione 10. venerdí 2 ottobre 2015 (2 ore)

Se n è il prodotto di due numeri primi distinti, calcolare $\varphi(n)$ equivale a fattorizzare n.

Valore della funzione di Eulero per la potenze di un primo.

La funzione $f : \mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ che manda $x \mapsto ([x]_m, [x]_n)$, e i sistemi di due congruenze

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

Esempi. Il sistema ha soluzione se e solo se $\gcd(m, n) \mid a - b$. Come trovare una soluzione.

Un sistema di congruenze. Come trovare tutte le soluzioni: se il sistema

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

ha una soluzione x_0, allora le soluzioni sono tutti e soli gli x tali che

$$x \equiv x_0 \pmod{\operatorname{lcm}(m, n)}.$$

Primo teorema di isomorfismo fra insiemi.

Lezione 11. lunedí 5 ottobre 2015 (2 ore)

Applicazione del primo teorema di isomorfismo fra insiemi: prima forma del Teorema Cinese dei resti: la biiezione $\mathbf{Z}/mn\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ data da $[x]_{mn} \mapsto ([x]_m, [x]_n)$.

Corollario: la funzione di Eulero è moltiplicativa nel senso della teoria dei numeri.

Logaritmo. Tavole dei logaritmi. Morfismi di semigruppi e di gruppi. Isomorfismi. Un morfismo di gruppi conserva l'elemento neutro e l'inverso. Un morfismo di anelli non conserva necessariamente l'unità.

Prodotto diretto di gruppi e di anelli.

Lezione 12. martedí 6 ottobre 2015 (2 ore)

La biiezione di cui sopra è un isomorfismo.

Seconda forma del Teorema Cinese dei Resti: la funzione $\mathbf{Z}/mn\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ data da $[x]_{mn} \mapsto ([x]_m, [x]_n)$ è un isomorfismo.

Di nuovo: la formula per la funzione di Eulero in termini di una fattorizzazione.

Il gioco dei 9 numeri come esempio di isomorfismo.

Sottoanelli: attenzione anche qui all'unità.

Sottogruppi: sottogruppi di $\mathbf{Z}$. Principio di induzione e principio del minimo intero.

Lezione 13. mercoledí 7 ottobre 2015 (2 ore)

Sottoanelli di $\mathbf{Z}$. Ideali. Ideali di $\mathbf{Z}$.

L'immagine di un morfismo è un sottoanello.

Prima forma del primo Teorema di isomorfismo di anelli, in termini di relazioni compatibili con le operazioni. Descrizione di queste relazioni in termini di congruenze modulo un ideale.

Lezione 14. venerdí 9 ottobre 2015 (2 ore)

(Lezione tenuta da Simone Ugolini)

Potenze e multipli, regole delle potenze. Sottogruppi ciclici, caratterizzazione dei sottogruppi.

Periodo (o ordine) di un elemento in un gruppo. Eguaglianza di due potenze.

Calcolo del periodo di ogni elemento di $U(\mathbf{Z}/7\mathbf{Z}), U(\mathbf{Z}/10\mathbf{Z}), U(\mathbf{Z}/15\mathbf{Z})$. Se l'ordine $|a|$ di un elemento di un gruppo è finito, allora

$$|a^k| = \frac{|a|}{\gcd(|a|, k)}$$

per ogni intero k.

Lezione 15. lunedí 12 ottobre 2015 (2 ore)

Una congruenza modulo un ideale è una relazione compatibile con le operazioni.

Seconda forma del primo Teorema di isomorfismo di anelli.

Periodo di $[10]$ in $U(\mathbf{Z}/p\mathbf{Z})$, con p un primo che non divide 10 (dunque $p \neq 2, 5$), e sviluppo decimale periodico di $1/p$. Cenno al caso $1/n$, con $\gcd(10, n) = 1$. Cenno al caso generale (antiperiodo).

In un gruppo finito, il periodo di un elemento divide l'ordine del gruppo. (Dimostrazione nel solo caso commutativo.)

Le traslazioni destre e sinistre sono funzioni biiettive.

Teorema di Eulero-Fermat.

Piccolo teorema di Fermat.

Lezione 16. martedí 13 ottobre 2015 (2 ore)

Introduzione alla crittografia. Cifrario di Cesare.

RSA, chiave pubblica e chiave privata (segreta).

Problema: mostrare che un numero è primo. Numeri di Carmichael.

Lezione 17. mercoledí 14 ottobre 2015 (2 ore)

Criteri probabilistici e deterministici di primalità.

Scrittura di un intero in base arbitraria: l'albergo di Hilbert, e cenni all'aritmetica cardinale.

Come si calcolano le potenze.

Lezione 18. giovedí 16 ottobre 2015 (3 ore)

Prima provetta intermedia.

Lezione 19. lunedí 19 ottobre 2015 (2 ore)

Esempi di RSA.

Polinomi: definizione formale. Grado. Grado della somma e del prodotto.

Lezione 20. martedí 20 ottobre 2015 (2 ore)

Estensioni. Estensioni semplici.

Valutazione di un polinomio in un elemento, e proprietà universale dei polinomi.

Struttura di una estensione semplice $A[\alpha]$.

Divisibilità in un anello dei polinomi $F[x]$, ove F è un campo. Divisione con resto, MCD, razionalizzazione.

Lezione 21. mercoledí 21 ottobre 2015 (2 ore)

Aritmetica nei domini: divisibilità, elementi invertibili ed associati, ideali principali. Unicità del MCD: il caso dei polinomi.

Radici di un polinomio e regola di Ruffini.

L'anello dei polinomi a coefficienti in un campo è ad ideali principali: un ideale non nullo è generato da un suo elemento di grado minimo. Polinomi monici.

Se A è un dominio, e $a, b \in A$, sono equivalenti:

- $a \mid b$ e $b \mid a$,
- $b = a\varepsilon$, con ε una unità,
- $(a) = (b)$.

Struttura delle estensioni semplici: elementi trascendenti ed algebrici, polinomio minimo. Il polinomio minimo di $\sqrt{2}$ su $\mathbf{Q}$.

Lezione 22. venerdí 23 ottobre 2015 (2 ore)

Ancora sulla struttura delle estensioni semplici: se F è un campo, e $0 \neq g \in F[x]$, gli elementi di $F[x]/(g)$ si scrivono in modo unico come $r + (g)$, ove r è un possibile resto della divisione per g.

MCD nei domini: unicità a meno di unità.

Estensioni di $\mathbf{Z}$ del tipo $\mathbf{Z}[\alpha]$, ove $\alpha \notin \mathbf{Q}$, e α è radice di un polinomio $x^2 + b_1 x + b_0 \in \mathbf{Z}[x]$.

Elementi primi e irriducibili. Un primo è sempre irriducibile.

2 è irriducibile in $\mathbf{Z}[\sqrt{-5}]$.

Lezione 23. lunedí 26 ottobre 2015 (2 ore)

Equivalenze della definizione di irriducibile. 2 non è primo in $\mathbf{Z}[\sqrt{-5}]$.

In $\mathbf{Z}[\sqrt{-5}]$ non esiste in generale il MCD.

Norme: esempi, in particolare la norma sugli anelli di polinomi. Una unità ha norma 1, ma non vale in generale il viceversa. Norme speciali.

In un dominio dotato di norma speciale, ogni elemento si scrive come prodotto di irriducibili.

Fattorizzazione unica. In generale la scrittura non è unica, vedi

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$$

in $\mathbf{Z}[\sqrt{-5}]$.

Lezione 24. martedí 27 ottobre 2015 (2 ore)

Se la scrittura è unica, allora gli irriducibili sono primi.

Se gli irriducibili sono primi, allora la scrittura è unica a meno dell'ordine e di elementi associati.

Domini euclidei. In un dominio euclideo la norma è speciale, e gli irriducibili sono primi.

Gli interi di Gauss sono un dominio euclideo.

Numeri primi come somma di due quadrati, e fattorizzazione in $\mathbf{Z}[i]$.

Lezione 25. mercoledí 28 ottobre 2015 (2 ore)

Un polinomio di grado n a coefficienti in un campo F ha al più n radici distinte in F. (Ma se F non è un campo non è più vero.)

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 $p \equiv 1 \pmod{4}$.

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.

Lezione 26. venerdí 30 ottobre 2015 (2 ore)

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

I primi in $\mathbf{Z}[i]$.

Terne pitagoriche, terne pitagoriche primitive.

Lezione 27. lunedí 2 novembre 2015 (2 ore)

Terne pitagoriche: classificazione. Fattorizzazione in potenze di primi in un UFD.

Radici quadrate modulo un primo congruo a 3 modulo 4. Testa o croce per telefono (inizio).

Lezione 28. martedí 3 novembre 2015 (2 ore)

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

Metodo alternativo, col prodotto di due primi, congrui rispettivamente a 1 e a 3 modulo 4.

Grado di una estensione, grado e struttura di una estensione semplice.

Se $g \in F[x]$ è primo (irriducibile), allora $F[x]/(g)$ è un campo.

Lezione 29. mercoledí 4 novembre 2015 (2 ore)

Se $g \in F[x]$ è primo (irriducibile), allora $F[x]/(g)$ è un campo, altrimenti $F[x]/(g)$ non è neanche un dominio.

Se B è un dominio, estensione del campo F, e $\alpha \in B$ è algebrico su F, allora $F[\alpha]$ è un campo, e il polinomio minimo di α su F è irriducibile.

Un esempio di polinomio minimo non irriducibile.

L'anello commutativo B sia estensione del campo F, e $f \in F[x]$ sia un polinomio monico, che abbia $\alpha \in B$ come radice. Se f è irriducibile in $F[x]$, allora f è il polinomio minimo di α su f.

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

Lezione 30. venerdí 6 novembre 2015 (3 ore)

Seconda provetta.

Lezione 31. lunedí 9 novembre 2015 (2 ore)

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

Estensioni algebriche. Un'estensione di grado finito è algebrica.

Lezione 32. martedí 10 novembre 2015 (2 ore)

Formula dei gradi. Se E/F è una estensione di grado finito n, allora ogni elemento di E è algebrico su F, di grado un divisiore di n.

Campo dei quozienti di un dominio.

Cenni al Lemma di Gauss e alle due conseguenze:

(1) Se A è un UFD, e $f \in A[x]$ è un polinomio non costante, ed irriducibile, allora f è irriducibile anche in $Q(A)[x]$.
(2) Se A è un UFD, allora $A[x]$ è un UFD.

Lezione 33. mercoledí 11 novembre 2015 (2 ore)

I numeri algebrici formano un campo, di grado infinito sui razionali.

Lemma di Eisenstein. Polinomio minimo di una radice primitiva p-sima dell'unità.

Lezione 34. venerdí 13 novembre 2015 (2 ore)

Sostituzione di indeterminate ed isomorfismo.

Il teorema della radice razionale: applicazione alle terne pitagoriche.

I numeri algebrici sono numerabili.

Lezione 35. lunedí 16 novembre 2015 (2 ore)

Esistenza di una radice di un polinomio irriducibile: due dimostrazioni. Matrice compagna.

Lezione 36. martedí 17 novembre 2015 (2 ore)

Campo di spezzamento di un polinomio.

Caratteristica di un anello con unità, sottoanello primo.

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

Un campo finito E ha ordine p^n, ove p è la sua caratteristica, e $|E : \mathbf{F}_p| = n$.

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

Lezione 37. mercoledí 18 novembre 2015 (2 ore)

Criterio della derivata per radici multiple. Le radici di $x^{p^n} - x$ sono distinte, e formano un campo.

Un campo finito è estensione semplice del campo primo (cioè del campo $\mathbf{F}_p$, se il campo ha caratteristica p).

Costruzione di campi di ordine 4 e 9.

Lezione 38. venerdí 20 novembre 2015 (2 ore)

Costruzione di campi di ordine $9, 8, 16$. Polinomi minimi degli elementi. Morfismo di Frobenius.

Lezione 39. lunedí 23 novembre 2015 (2 ore)

$\mathrm{GF}(p^n) \subseteq \mathrm{GF}(p^m)$ se e solo se $m \mid n$.

Codici a rivelazione e correzione d'errore. Codici a ripetizione 2 e 3 volte. Codice a controllo di parità. Codici lineari (binari). Matrici C e H di un codice lineare.

Lezione 40. martedí 24 novembre 2015 (2 ore)

Codifica di un codice lineare. Uso delle matrici C e H. Distanza di Hamming. Caratterizzazione dei codici che rivelano un errore mediante distanza e matrice H. Caratterizzazione dei codici che correggono un errore mediante la distanza.

Lezione 41. mercoledí 25 novembre 2015 (2 ore)

(Lezione tenuta da Simone Ugolini)

Definizione delle classi laterali destre e sinistre rispetto a un sottogruppo di in gruppo. Definizione di sottogruppi normale. Teorema di Lagrange. Indice di un sottogruppo in un gruppo. Monoide delle mappe affini su $\mathbf{Z}/n\mathbf{Z}$. Il gruppo diedrale D_3. Verifica della non commutatività di D_3. Il sottogruppo generato da una rotazione è normale in D_3. Il sottogruppo generato da una riflessione non è normale in D_3. Cenno al fatto che un sottogruppo di indice due in un gruppo qualunque è normale.

Lezione 42. venerdí 27 novembre 2015 (3 ore)

Terza provetta.

Lezione 43. lunedí 30 novembre 2015 (2 ore)

Caratterizzazione dei codici che correggono un errore mediante la matrice H.

Il codice di Hamming di lunghezza 7 basato sul polinomio $x^3 + x + 1 \in \mathbf{F}_2[x]$. Codifica e decodifica. Ciclicità.

Lezione 44. martedí 1 dicembre 2015 (2 ore)

Il codice di Hamming di lunghezza 7 basato sul polinomio $x^3 + x^2 + 1 \in \mathbf{F}_2[x]$. Codifica e decodifica. Legame on l'altro codice. Ciclicità.

Codici di Hamming in generale. Il codice di Hamming di lunghezza 3 è il codice a ripetizione.

Il codice di Hamming di lunghezza 15 basato sul polinomio $x^4 + x + 1$.

Lezione 45. mercoledí 2 dicembre 2015 (2 ore)

(Lezione tenuta da Simone Ugolini)

Caratterizzazioni equivalenti dei sottogruppi normali.

Se R è una relazione di equivalenza su un gruppo G compatibile con l'operazione di gruppo, allora $[1]$ è un sottogruppo normale di G. Viceversa, se N è un sottogruppo normale di un gruppo G, allora la relazione definita da aRb se e solo se $a^{-1}b \in N$ è un relazione di equivalenza su G compatibile con l'operazione.

Definizione del gruppo quoziente G/N e verifica della buona definizione dell'operazione $(aN)(bN) = (ab)N$. Verifica degli assiomi di gruppo per G/N. La proiezione canonica $\pi : G \to G/N$ è un morfismo suriettivo.

Primo teorema di isomorfismo fra gruppi con dimostrazione.

Lezione 46. venerdí 4 dicembre 2015 (2 ore)

Teorema di struttura dei gruppi ciclici.

Secondo teorema di isomorfismo per gruppi. Applicazione alla formula per massimo comun divisore e minimo comune multiplo.

Secondo teorema di isomorfismo per anelli (solo enunciato).

Lezione 47. mercoledí 9 dicembre 2015 (2 ore)

Immagini dirette e inverse.

Terzo teorema di isomorfismo (teorema di corrispondenza) per gruppi. Applicazione: sottogruppi dei gruppi ciclici.

Lezione 48. venerdí 11 dicembre 2015 (2 ore)

Terzo teorema di isomorfismo (teorema di corrispondenza) per anelli. (Solo enunciato.)

Lemma di Gauss e questioni collegate.

Lezione 49. martedí 15 dicembre 2015 (2 ore)

Due applicazioni del codice di Hamming:

- sette domande, una menzogna, e
- cappelli rossi, cappelli blu.

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/