Algebra 2 - a.a. 2018/2019 - Ilaria Damiani
Corso di Laurea Triennale in Matematica

Primo semestre: 01/10/2018-18/01/2019
Orario settimanale: martedì, giovedì, venerdì 11.00-13.00 aula L3
Ricevimento: lunedì 13.30-15.30 o su appuntamento

Programma d'esame

1. Anelli.

Riferimento bibliografico:
Schoof, R., Van Geemen, B.: Dispense di Algebra, Pavia 2001, cap. 8,9,11,12,13
http://www.mat.uniroma2.it/∼damiani/notealgebra_Schoof_vanGeemen.pdf

A) Definizioni (richiami).

B) Esempi.

C) Il campo dei quozienti di un dominio di integrità.

D) Primo, secondo e terzo teorema di isomorfismo per anelli.

E) Ideali.
Ideali principali, ideali massimali, ideali primi. Elementi primi e irriducibili.

F) Fattorizzazione in domini di integrità.
Domini euclidei.
Domini a ideali principali; euclideo implica a ideali principali.
Domini a fattorizzazione unica; a ideali principali implica a fattorizzazione unica; il teorema di Gauss.

2. A-moduli.

Riferimento bibliografico:
http://www.mat.uniroma2.it/∼damiani/mod_fg_pid.pdf

A) Che cosa significa classificare.

B) A-moduli e omomorfismi di A-moduli: definizione ed esempi.

C) Introduzione alla struttura degli A-moduli.
Quozienti. Somma diretta e prodotto diretto di A-moduli. Moduli liberi. Torsione.

D) Moduli finitamente generati su domini a ideali principali: classificazione.

E) Esempi.
$\mathbb{Z}$-moduli: la classificazione dei gruppi abeliani finitamente generati e dei gruppi abeliani finiti.
$K[x]$-moduli ed endomorfismi di spazi vettoriali.
$K[[x]]$-moduli di dimensione finita ed endomorfismi nilpotenti.

3. Gruppi.

Riferimenti bibliografici:
Artin - Algebra, cap. 2 par. 2-8 e 10, cap. 5 par. 5-8, cap. 6 par. 1,3,4,6.
Lang - Algebra (terza edizione, 1993), cap. 1, par. 2-8.

A) Generalità.
Quozienti. Primo, secondo e terzo teorema di isomorfismo per i gruppi. Prodotto diretto di gruppi. Prodotto semidiretto.

B) Azioni di gruppi.
Quoziente. Classificazione delle azioni transitive. Formula delle classi.
Il teorema di Cauchy.

C) Primo, secondo e terzo teorema di Sylow.

D) Gruppi semplici e teorema di Jordan-Hölder.

E) Gruppi risolubili.

Sottogruppi normali e quozienti, criterio di risolubilità.
Risolubilità dei p-gruppi.
$\mathcal{S}_n$ non è risolubile per $n \geq 5$.

4. Campi.

Riferimenti bibliografici:
Lang - Algebra (terza edizione, 1993), cap. 5, cap. 6 par. 1-4,6,7.

A) Definizioni e notazioni. Classi "distinte" di estensioni.

B) Estensioni algebriche.

Grado di un'estensione, polinomio minimo di un elemento, radici di polinomi irriducibili, campi algebricamente chiusi e chiusura algebrica di campi.

C) Omomorfismi e loro estensioni.

D) Automorfismi e loro restrizioni.

E) Estensioni normali e campi di spezzamento.

F) Estensioni separabili.

Il teorema dell'elemento primitivo. Estensioni normali e separabili: il gruppo di Galois.

G) Il teorema di corrispondenza di Galois.

H) Campi finiti.

I) Estensioni puramente inseparabili (cenni).

L) Risolubilità.

Estensioni ciclotomiche. Teorema di lineare indipendenza dei caratteri ed estensioni cicliche. Estensioni abeliane. Estensioni e polinomi risolubili per radicali. Estensioni risolubili.
Risolubilità per radicali dei polinomi di grado ≤ 4.
Polinomi simmetrici e funzioni razionali simmetriche: non risolubilità del generico polinomio di grado ≥ 5.

Programma d'esame - maggiori dettagli

1. Anelli.

Riferimento bibliografico:
Schoof, R., Van Geemen, B.: Dispense di Algebra, Pavia 2001, cap. 8,9,11,12,13
http://www.mat.uniroma2.it/~damiani/notealgebra_Schoof_vanGeemen.pdf

A) Definizioni (richiami).

Gruppi e gruppi abeliani; anelli, anelli commutativi, anelli unitari, anelli commutativi unitari.
Elementi invertibili e divisori dello zero; anelli privi di divisori dello zero e domini di integrità.
Anelli con divisione (corpi) e campi.
Omomorfismi di gruppi, omomorfismi di anelli, omomorfismi di anelli unitari.
Sottoanelli e sottoanelli unitari; intersezione di sottoanelli; sottoanello generato da un sottoinsieme.
Il gruppo degli elementi invertibili di un anello unitario.
Oggetti iniziali; proprietà universale dell'anello unitario $\mathbb{Z}$.

B) Esempi.

Interi, razionali, reali, complessi, quaternioni e loro sottoanelli.

L'anello delle funzioni da un insieme a un anello; l'anello delle funzioni continue/derivabili/analitiche da $\mathbb{R}$ a $\mathbb{R}$.
Gli endomorfismi di un gruppo abeliano e di uno spazio vettoriale; l'anello delle matrici $n \times n$ a coefficienti in un anello. L'anello opposto A^{op}: trasposta e duale.
Prodotto e somma diretta di anelli.
Polinomi. $A[x]$ e $A[x_i|i \in I]$ (con A anello unitario): proprietà universale e descrizione. Anelli (in particolare commutativi) finitamente generati e non finitamente generati. $A[x, x^{-1}]$ e $A[[x]]$ (anelli), $A[[x, x^{-1}]]$ (non anello).

C) Il campo dei quozienti di un dominio di integrità: proprietà universale, esistenza e unicità. Esempi.

D) I teoremi di isomorfismo.
Immagine e nucleo di un omomorfismo di anelli; gli ideali.
Proiezioni e immagini omomorfe.
Il quoziente: caratterizzazione delle proiezioni e proprietà universale (primo teorema di omomorfismo).
Primo, secondo e terzo teorema di isomorfismo.
Esempi.

E) Ideali.
Intersezione e somma di una famiglia di ideali; prodotto e intersezione di due ideali.
Ideali coprimi: il teorema cinese del resto (richiamo e generalizzazione). Ideali coprimi e interi coprimi.
L'ideale generato da un sottoinsieme; ideali finitamente generati e non finitamente generati; ideali principali.
Ideali massimali. Esistenza di ideali massimali in anelli unitari. Ideali massimali, quozienti e anelli semplici (definizione); il caso commutativo: ideali massimali e campi; il caso non commutativo: l'esempio degli endomorfismi di uno spazio vettoriale e quello delle matrici $n \times n$ a coefficienti in un corpo. Ideali massimali ed elementi irriducibili in domini di integrità.
Ideali primi. Connessione tra ideali primi e massimali, tra ideali primi e divisori dello zero. Caso commutativo unitario: esistenza; ideali primi e domini di integrità; ideali primi ed elementi primi.

F) Fattorizzazione in domini di integrità.
Legame tra l'esistenza di una fattorizzazione in primi e l'unicità della fattorizzazione in irriducibili.
<u>Domini euclidei</u> e divisione con resto. La valutazione euclidea degli invertibili. Esempi: campi, interi, polinomi in una variabile a coefficienti in un campo, interi Gauss, sottoanelli di $\mathbb{Q}$, serie di potenze formali in una variabile.
<u>Domini a ideali principali</u>. I domini euclidei sono a ideali principali; esistono domini a ideali principali che non sono euclidei (esempio). Elementi primi e irriducibili e ideali primi e massimali in un dominio a ideali principali; massimo comun divisore e identità di Bézout. Esistenza di divisori irriducibili di elementi non invertibili. Gli irriducibili nell'anello degli interi di Gauss e i numeri interi che sono somma di due quadrati.
<u>Domini a fattorizzazione unica</u>. I domini a ideali principali sono a fattorizzazione unica; esistono domini a fattorizzazione unica che non sono a ideali principali (esempi). Elementi primi, elementi irriducibili, catene crescenti di ideali principali: caratterizzazione dei domini a fattorizzazione unica. Massimo comun divisore e minimo comune multiplo. Contenuto di un polinomio e polinomi primitivi.

Lemma di Gauss: i polinomi irriducibili a coefficienti in un dominio a fattorizzazione unica. Teorema fondamentale dei domini a fattorizzazione unica (teorema di Gauss): l'anello dei polinomi a coefficienti in un dominio a fattorizzazione unica è a fattorizzazione unica. Esempi di domini a fattorizzazione unica. Esempi di domini di integrità che non sono a fattorizzazione unica. Sottoanelli e quozienti di domini a fattorizzazione unica non sono necessariamente a fattorizzazione unica.

2. A-moduli.

Riferimento bibliografico:
http://www.mat.uniroma2.it/~damiani/mod_fg_pid.pdf

A) Che cosa significa classificare.

Esempi: insiemi e cardinalità; spazi vettoriali e dimensione; gruppi ciclici e cardinalità; quozienti di anelli e ideali; endomorfismi diagonalizzabili di uno spazio vettoriale e autovalori con molteplicità; endomorfismi di uno spazio vettoriale su un campo algebricamente chiuso e matrici a blocchi di Jordan.

B) A-moduli e omomorfismi di A-moduli: definizione.

Esempi: K-modulo equivale a K-spazio vettoriale; $\mathbb{Z}$-modulo equivale a gruppo abeliano; un anello A è un A-modulo e un A^{op}-modulo; un K-spazio vettoriale V è un $End_K(V)$-modulo e il suo duale è un $End_K(V)^{op}$-modulo; per ogni $\lambda \in K$ K è un $K[x]$-modulo; $K[x]$-modulo equivale a K-spazio vettoriale con endomorfismo.

C) Introduzione alla struttura degli A-moduli.

A-sottomoduli. Intersezione e somma di A-sottomoduli. Quozienti. Somma diretta e prodotto diretto di A-moduli.

Il problema dell'esistenza di un complementare di un A-sottomodulo; il problema dell'esistenza di una base di un A-modulo.

Sistemi di generatori, insiemi liberi, basi. A-moduli finitamente generati; esempi; $\mathbb{Q}$ non è finitamente generato su $\mathbb{Z}$. A-moduli ciclici e quozienti di A. A-moduli liberi; caso commutativo: la dimensione. Esempi di A-moduli liberi e di A-moduli non liberi.

Elementi di torsione in un modulo su un dominio di integrità. Moduli di torsione e moduli privi di torsione; i moduli liberi sono privi di torsione; il quoziente di un modulo per la sua torsione è privo di torsione; caso finitamente generato: il sottomodulo di torsione ammette un complementare, che è libero.

L'annullatore di un sottoinsieme di un A-modulo. L'A-modulo generato da un elemento e il quoziente di A per il suo annullatore.

D) Moduli finitamente generati su domini a ideali principali.

Generalizzazione dell'ordine di un elemento di un gruppo: il generatore dell'annullatore di un elemento di un A-modulo; il generatore dell'annullatore di un A-modulo.

Esistenza del complementare di un sottomodulo ciclico generato da un elemento con annullatore uguale all'annullatore del modulo.

Ogni modulo finitamente generato su un dominio a ideali principali è somma diretta di moduli ciclici. Un sistema completo di invarianti: i divisori elementari; la classificazione con i divisori elementari. Un'altra classificazione e un altro sistema completo di invarianti: le potenze degli irriducibili; il sottomodulo della p-torsione.

E) Esempi.

$\mathbb{Z}$-moduli: la classificazione dei gruppi abeliani finitamente generati e dei gruppi abeliani finiti; la p-torsione di un gruppo abeliano finitamente generato; ogni gruppo abeliano finito è somma diretta delle sue p-torsioni.

$K[x]$-moduli. La classificazione degli endomorfismi di spazi vettoriali di dimensione finita e la forma canonica di Jordan; $(x-\lambda)$-torsione, autospazi e autospazi generalizzati di autovalore λ. La forma canonica razionale per endomorfismi ciclici; polinomio minimo e polinomio caratteristico.
$K[[x]]$-moduli di dimensione finita ed endomorfismi nilpotenti.

3. Gruppi.

Riferimenti bibliografici:

Artin - Algebra, cap. 2 par. 2-8 e 10, cap. 5 par. 5-8, cap. 6 par. 1,3,4,6.

Lang - Algebra (terza edizione, 1993), cap. 1, par. 2-8.

A) Generalità.

Richiami: gruppi, omomorfismi di gruppi; immagine e nucleo di un omomorfismo; sottogruppi, generatori; proiezioni, quozienti e sottogruppi normali.
Esistenza, unicità e proprietà universale del quoziente; primo, secondo e terzo teorema di isomorfismo per i gruppi.
Prodotto diretto di gruppi.
Prodotto semidiretto.

B) Azioni di gruppi.

G-insiemi, G-morfismi, G-sottoinsiemi.
La relazione di equivalenza indotta da un'azione: quoziente e G-orbite; ogni G-insieme è unione disgiunta di G-orbite.
Esempi. Azione banale. Azioni naturali: $\mathcal{S}_n$ e $GL(V)$. Azione sinistra e destra di un gruppo su se stesso. Coniugio in un gruppo. Azioni indotte su unioni disgiunte, prodotti, insieme delle parti di G-insiemi. Azioni che commutano. Spazio proiettivo e proiettività.
Lo stabilizzatore di un elemento; gli stabilizzatori di elementi G-equivalenti; stabilizzatori e morfismi. Azioni transitive e loro classificazione.
La formula delle classi e sue applicazioni: azioni e orbite di p-gruppi, il teorema di Cauchy, il centro di un p-gruppo; il coniugio sui sottogruppi di G; il normalizzatore di un sottogruppo; azione sinistra di G sulle parti di G: alcune proprietà degli stabilizzatori.

C) Teoria di Sylow.

Gruppi abeliani: p-torsione e decomposizione dei gruppi abeliani finiti in somma diretta delle p-torsioni. Gruppi non abeliani: gli elementi di p-torsione non sono sottogruppi.
p-gruppi, definizioni e proprietà; gruppi di ordine p^2; gruppi di ordine p^n: esistenza di sottogruppi di ordine p^m per ogni $m \leq n$. p-sottogruppi di un gruppo finito e sottogruppi di Sylow: definizione.
Primo teorema di Sylow: esistenza di un sottogruppo di Sylow. Il teorema di Cauchy come corollario del primo teorema di Sylow.
Secondo teorema di Sylow: legame tra i p-Sylow di un gruppo finito e quelli di un suo sottogruppo; i p-Sylow di un gruppo sono coniugati. Il normalizzatore di un p-Sylow; indice del normalizzatore e numero di p-Sylow.
Terzo teorema di Sylow: l'azione di un p-Sylow sull'insieme dei p-Sylow e ulteriori proprietà del numero di p-Sylow.

D) Gruppi semplici.

Definizione ed esempi: i gruppi semplici abeliani; il gruppo alterno $\mathcal{A}_n$ è semplice per ogni $n \geq 5$.

Serie e fattori di composizione; ogni gruppo finito ammette una serie di composizione; serie e fattori di composizione di sottogruppi normali e quozienti.
I fattori di composizione e le loro molteplicità sono un invariante: il teorema di Jordan-Hölder.
Esempi: i fattori di composizione dei gruppi abeliani finiti; i fattori di composizione dei p-gruppi; i fattori di composizione di $\mathcal{S}_n$.

E) Gruppi risolubili.
Definizioni: il commutatore di due elementi; sottogruppo derivato e sua proprietà universale; serie derivata e definizione di gruppo risolubile.
I quozienti della serie derivata; fattori di composizione di un gruppo risolubile finito; caratterizzazione dei gruppi risolubili.
Sottogruppi, sottogruppi normali e quozienti di gruppi risolubili; criterio di risolubilità. Risolubilità di prodotti diretti e semidiretti. I p-gruppi sono risolubili.
Semplicità e risolubilità: $\mathcal{S}_n$ non è risolubile per $n \geq 5$.

4. Campi.

Riferimenti bibliografici:
Lang - Algebra (terza edizione, 1993), cap. 5, cap. 6 par. 1-4,6,7.

A) Definizioni e notazioni.
Campi e omomorfismi di campi.
Caratteristica di un campo e sottocampo fondamentale.
Sottocampi e loro intersezioni. Estensioni di campi, sottoestensioni generate da un sottoinsieme, composto di sottoestensioni. Estensioni finitamente generate.
Classi "distinte" di estensioni.

B) Estensioni algebriche.
Grado di un'estensione ed estensioni finite. Le estensioni finite sono finitamente generate; le estensioni finitamente generate non sono necessariamente finite. Moltiplicatività del grado. La classe delle estensioni finite è "distinta".
Il polinomio minimo di un elemento. Elementi algebrici ed elementi trascendenti. Anello e campo generato da un elemento. Il grado dell'estensione generata da un elemento.
Definizione di estensione algebrica. Le estensioni finite sono algebriche; le estensioni algebriche finitamente generate sono finite; esistono estensioni algebriche non finite. La classe delle estensioni algebriche è "distinta".
Polinomi irriducibili ed estensioni algebriche; il campo generato da una radice di un polinomio irriducibile: esistenza e costruzione, grado, unicità a meno di isomorfismo, non unicità come sottoestensione di un'estensione data. Campi algebricamente chiusi e chiusura algebrica di campi: definizione; la chiusura algebrica di un campo contenuto in un campo algebricamente chiuso. Esempi: i campi finiti non sono algebricamente chiusi; $\mathbb{Q}$ ed $\mathbb{R}$ non sono algebricamente chiusi.

C) Omomorfismi e chiusura algebrica.
L'immagine di un elemento algebrico su un campo K è un elemento algebrico sull'immagine di K; l'immagine di un'estensione algebrica di K è un'estensione algebrica dell'immagine di K. Omomorfismi che fissano K: ogni omomorfismo di un'estensione algebrica di K in sé è un automorfismo. Estensione di omomorfismi su estensioni algebriche a valori in una chiusura algebrica: esistenza.
L'unicità della chiusura algebrica di un campo a meno di isomorfismo. Cardinalità di una chiusura algebrica. Esistenza della chiusura algebrica di un campo a meno di isomorfismi.

Caratterizzazione delle estensioni algebriche come sottoestensioni della chiusura algebrica.

D) Automorfismi.

Il gruppo degli automorfismi della chiusura algebrica di K che fissano K.
La restrizione a sottoestensioni: gli omomorfismi da un'estensione algebrica di K alla sua chiusura algebrica.
Il sottogruppo degli automorfismi che stabilizzano una sottoestensione data; il sottogruppo degli automorfismi che fissano una sottoestensione data; relazione di normalità tra questi sottogruppi.

E) Estensioni normali.

Il campo di spezzamento di un polinomio: definizione, esistenza, unicità, grado e gruppo degli automorfismi.
Il campo di spezzamento di una famiglia di polinomi.
Estensioni normali: definizione e caratterizzazione. La minima estensione normale su K di un'estensione algebrica di K. Omomorfismi e automorfismi.
La classe delle estensioni normali non è "distinta".
Esempi: le estensioni quadratiche sono normali; esempi di estensioni non normali di grado 3; altri esempi di estensioni normali e non normali e loro gruppo degli automorfismi.

F) Estensioni separabili.

Il grado di separabilità: definizione e moltiplicatività; polinomi separabili. Estensioni finite separabili ed estensioni separabili anche non finite.
La classe delle estensioni separabili è "distinta". La chiusura separabile di un campo in una sua estensione algebrica.
Esempi: in caratteristica zero ogni estensione algebrica è separabile; ogni estensione algebrica di un campo finito è separabile; campi di funzioni razionali ed esempi di estensioni non separabili.
Estensioni separabili finite/finitamente generate: il teorema dell'elemento primitivo.

G) Teoria di Galois.

Il gruppo di Galois di un'estensione algebrica normale e separabile.
Il campo fissato da un gruppo finito G di automorfismi di un campo dato: estensione algebrica finita normale e separabile con gruppo di Galois G (teorema di Artin).
Il teorema di corrispondenza di Galois.

H) Campi finiti.

Cardinalità dei campi finiti. Esistenza e unicità del campo di cardinalità p^n con p primo.
Il Frobenius e il gruppo di Galois di un'estensione finita di un campo finito.

I) Estensioni puramente inseparabili (cenni).

Definizione ed esempi. Radici p-esime.
Le estensioni puramente inseparabili sono normali.
La classe delle estensioni puramente inseparabili è "distinta".

L) Risolubilità.

<u>Estensioni ciclotomiche</u>: definizione, grado, normalità e separabilità, gruppo di Galois. Estensioni ciclotomiche su $\mathbb{Q}$.
Il polinomio $x^n - a$, il suo campo di spezzamento e il suo gruppo di Galois. Caratteristica p: il polinomio $x^p - x - a$ e il suo gruppo di Galois.
<u>Estensioni cicliche</u>. Il teorema di lineare indipendenza dei caratteri (o degli automorfismi di un campo). Caratterizzazione delle estensioni cicliche di campi che contengono abbastanza radici dell'unità.

Estensioni abeliane. Le estensioni ciclotomiche e le estensioni cicliche sono abeliane.
Estensioni e polinomi risolubili per radicali: definizione. Le estensioni ciclotomiche e le estensioni cicliche sono risolubili per radicali. La minima estensione normale di un'estensione risolubile per radicali è risolubile per radicali. La classe delle estensioni risolubili per radicali è "distinta".
Estensioni risolubili: definizione. Le estensioni abeliane sono risolubili. La classe delle esensioni risolubili è "distinta".
Risolubilità per radicali e risolubilità coincidono: un polinomio è risolubile per radicali se e solo se il gruppo di Galois del suo campo di spezzamento è risolubile.
Ogni polinomio di grado ≤ 4 è risolubile per radicali. Esistono polinomi di grado 5 che non sono risolubili per radicali.
Funzioni razionali, polinomi simmetrici e funzioni razionali simmetriche: il generico polinomio di grado ≥ 5 non è risolubile per radicali.