Review - Algebra 2.

10. Modules.

Convention: All rings have 1; all modules are unital left modules.

Definition. For a subset A of an R-module M,

$$RA := \{r_1a_1 + \dots r_ka_k \ : \ k \in \mathbb{N}, r_1, \dots, r_k \in R, a_1, \dots, a_k \in A\}$$

finite R-linear combinations

is the *submodule of M generated by A*.

Definition. An R-module M is *free* over $A \subseteq M$ if $\forall m \in M \setminus \{0\}$ $\exists! n \in \mathbb{N}$ $\exists! r_1, \dots, r_n \in R \setminus \{0\}$ $\exists! a_1, \dots, a_n \in A$: $m = r_1a_1 + \dots + r_na_n$.

unique representation

Then we call A *free generators* (a *basis*) for M.

Theorem. *For each set A there exists a free R-module $F(A)$ on A. $F(A)$ satisfies the following* **universal mapping property***: for any R-module M and any $\varphi\colon A \to M$ there exists a unique $\Phi \in \mathrm{Hom}_R(F(A), M)$ such that $\Phi|_A = \varphi$.*

11. Vector spaces.

Definition. $V^* := \mathrm{Hom}_F(V, F)$ is the *dual space* of the F-vector space V; its elements are *linear functionals*.

If $B = \{b_1, \dots, b_n\}$ is a basis of V, then $B^* := \{b_1^*, \dots, b_n^*\}$ defined by

$$b_i^*(b_j) := \delta_{ij} \text{ for } i, j \in \{1, \dots, n\}$$

is the *dual basis* of B.

Theorem. *Let V, W be finite dimensional with bases B, C, respectively. Let $\varphi \in \mathrm{Hom}_F(V, W)$, define*

$$\varphi^*\colon W^* \to V^*, \ \ f \mapsto f \circ \varphi.$$

Then $\varphi^* \in \mathrm{Hom}_F(W^*, V^*)$ and $M_{C^*}^{B^*}(\varphi^*) = M_B^C(\varphi)^T$.

Theorem. *For B a basis of V over F, we have $V = F(B)$ (direct sum) but $V^* = F^B$ (direct product).* $= \{\varphi : B \to F\}$

Theorem. *The determinant $\det\colon M_n(R) \to R$ is the unique function that is multilinear, alternating on the columns and satisfies $\det(I_n) = 1$.*

12. Modules over PIDs.

Definition. An R-module is *Noetherian* if it satisfies the *ascending chain condition (ACC)* on submodules.

no infinite strictly increasing chain

A ring R is (left) *Noetherian* if it satisfies the ACC on left ideals.

Theorem. *PIDs are Noetherian.*

Ex $\mathbb{Z}$, $F[x]$

Structure Theorem (Invariant Factor Form). *Let M be a finitely generated R-module for a PID R. Then*

$$M \cong R/(a_1) \oplus \cdots \oplus R/(a_k) \oplus R^r$$

where $k, r \geq 0$, $a_1, \ldots, a_k \in R$ are neither 0 nor a unit and $a_1 | a_2 | \ldots | a_k$.
$a_1, \ldots, a_k$ are the invariant factors *of M.*
r is the free rank *of M.*

R^r is the free R-module over r generators $(1,0 \ldots 0), \ldots (0 \ldots 0 1)$

Proof. Since R is Noetherian, M is finitely presented. Since R is a PID, this finite presentation can be diagonalized which yields the invariant factors. $\square$

Structure Theorem (Elementary Divisor Form). *Let M be a finitely generated R-module for a PID R. Then*

$$M \cong R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_n^{\alpha_n}) \oplus R^r$$

where $p_1, \ldots, p_n \in R$ are (not necessarily distinct) primes, $\alpha_1, \ldots, \alpha_n, r \in \mathbb{N}$.
$p_1^{\alpha_1}, \ldots, p_n^{\alpha_n}$ are the elementary divisors *of M.*

Proof. Decompose $R/(a)$ from the invariant factor form into its primary components $a = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ for distinct primes $p_1, \ldots, p_n \in R$ and $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$. $\square$

Application: canonical forms for $A \in M_n(F)$.

Let V be a finite dimensional vector space over a field F and $\varphi \in \mathrm{End}_F(V)$. Then V is an $F[x]$-module V_φ by

$$xv := \varphi(v) \text{ for } v \in V.$$

Theorem. *$V_A \cong V_B$ iff matrices A, B are similar.*

Rational canonical form.

$$V_\varphi \cong F[x]/(a_1(x)) \oplus \cdots \oplus F[x]/(a_k(x))$$

where $a_1(x) \mid a_2(x) \mid \ldots \mid a_k(x)$ are monic.
Note $\mathrm{Ann}_{F[x]}(V_\varphi) = (a_k(x))$.

For $a(x) = b_0 + b_1 x + \cdots + b_{d-1}x^{d-1} + x^d$, the *companion matrix* $C_{a(x)}$ of $a(x)$ is

$$C_{a(x)} := \begin{pmatrix} 0 & \cdots & \cdots & 0 & -b_0 \\ 1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -b_{d-2} \\ 0 & \cdots & 0 & 1 & -b_{d-1} \end{pmatrix}$$

The *rational canonical form* of $\varphi \in \mathrm{End}_F(V)$ is the block diagonal matrix

$$\begin{pmatrix} C_{a_1(x)} & & & 0 \\ & C_{a_2(x)} & & \\ & & \ddots & \\ 0 & & & C_{a_k(x)} \end{pmatrix}$$

for the invariant factors $a_1(x) \mid a_2(x) \mid \ldots \mid a_k(x)$ of V_φ.

Theorem. *Every $\varphi \in \mathrm{End}_F(V)$ has a unique rational canonical form which determines φ up to similarity.*

Jordan canonical form.
Assume the characteristic pol. of $A \in M_{n\times n}(F)$ splits in linear factors in F.
Then each invariant factor $a(x)$ of A splits into prime powers (elementary divisors)

$$a(x) = (x-\lambda_1)^{\alpha_1} \ldots (x-\lambda_l)^{\alpha_l},$$

and

$$V_A \cong F[x]/(x-\lambda_1)^{\alpha_1} \oplus \cdots \oplus F[x]/(x-\lambda_m)^{\alpha_m}.$$

The $\alpha \times \alpha$ *Jordan block* with eigenvalue λ is defined as

$$J_\alpha(\lambda) := \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix}.$$

A *Jordan canonical form* of $A \in M_{n\times n}(F)$ is a block diagonal matrix

$$\begin{pmatrix} J_{\alpha_1}(\lambda_1) & & & 0 \\ & J_{\alpha_2}(\lambda_2) & & \\ & & \ddots & \\ 0 & & & J_{\alpha_m}(\lambda_m) \end{pmatrix}$$

for the multiset $\{(x-\lambda_i)^{\alpha_i} \;:\; i \le m\}$ of elementary divisors of V_A.

Theorem. *If the characteristic polynomial of $A \in M_{n\times n}(F)$ splits in linear factors over F, then A has a Jordan canonical form (unique up to permutation of Jordan blocks), which determines A up to similarity.*

13. Field theory.

Theorem. *For $p(x) \in F[x]$ irreducible and $p(\alpha) = 0$,*

$$F(\alpha) \cong F[x]/(p(x))$$

Theorem. *For every $f(x) \in F[x]$ there exists a unique (up to isomorphism) minimal extension K/F such that f splits into linear factors over K (the splitting field of $F[x]$).*

Theorem. *Every field F has a (unique up to isomorphism) algebraic closure $\overline{F}$ (i.e. $\overline{F}/F$ is algebraic and every $f(x) \in F[x]$ splits over $\bar{F}$).*

14. Galois theory.

Definition. K/F algebraic is

- *separable* if $m_{\alpha,F}(x)$ is separable (has no multiple roots) for all $\alpha \in K$;
- *normal* if every irreducible $f(x) \in F[x]$ with some root in K splits in $K[x]$.

$\mathrm{Aut}\,(K/F) := \{\sigma \in \mathrm{Aut}\,(K) \ : \ \sigma|_F = \mathrm{id}_F\}$.
For $H \leq \mathrm{Aut}\,(K)$, $\mathrm{Fix}(H) := \{a \in K \ : \ \sigma(a) = a \text{ for all } \sigma \in H\}$.

Theorem. *For K/F of finite degree TFAE:*

(1) *K/F is Galois.*
(2) *K/F is normal and separable.*
(3) *K is the splitting field of some separable $f(x) \in F[x]$.*
(4) $|\mathrm{Aut}\,(K/F)| = [K : F]$.

The Fundamental Theorem of Galois Theory.
Let K/F be a finite Galois extension with $G := Gal(K/F)$. Then

(1) Fix: $\{H \leq G\} \to \{E \ : \ F \leq E \leq K\}$ *is a bijection with inverse* $\mathrm{Aut}\,(K/.)$.
(2) *For $H_1, H_2 \leq G$ with $E_1 := \mathrm{Fix}(H_1), E_2 := \mathrm{Fix}(H_2)$*
  (a) *$H_1 \leq H_2$ iff $E_1 \geq E_2$,*
  (b) *$E_1 \cap E_2 = \mathrm{Fix}(\langle H_1 \cup H_2 \rangle)$,*
  (c) *$E_1 E_2 = \mathrm{Fix}(H_1 \cap H_2)$.*
(3) *For $H \leq G$ with $E := \mathrm{Fix}(H)$*
  (a) *K/E is Galois with $\mathrm{Gal}(K/E) = H$,*
  (b) *$[K : E] = |H|$, $[E : F] = |G : H|$,*
  (c) *For $\sigma \in G$, $\mathrm{Aut}\,(K/\sigma(E)) = \sigma H \sigma^{-1}$,*
  (d) *E/F is Galois iff H is normal in G. In this case $\mathrm{Gal}(E/F) \cong G/H$.*

always Galois

Galois iff $H \trianglelefteq G$

$$\begin{array}{cc} K & 1 \\ | & | \\ E=\mathrm{Fix}(H) & H \\ | & | \\ F & G \end{array}$$

Theorem. *Every finite, separable E/F has a unique (up to isomorphism)* Galois closure K *(i.e. K/E is minimal such that K/F is Galois).*

Primitive Element Theorem. *If K/F is finite separable, then $K = F(\alpha)$ for some $\alpha \in K$.*

Finite fields.

Let p prime, $n \in \mathbb{N}$. Then

(1) There exists a (unique up to isomorphism) field F_{p^n} of order p^n (the splitting field of $x^{p^n} - x$ over F_p).
(2) $F_{p^n}^*$ is cyclic.
(3) F_{p^n}/F_p is Galois with $\mathrm{Gal}(F_{p^n}/F_p) \cong \mathbb{Z}_n$ generated by the Frobenius automorphism $a \mapsto a^p$.
(4) $F_{p^d} \leq F_{p^n}$ iff $d|n$.

Cyclotomic fields.

Let $\zeta := e^{2\pi i/n}$ be a primitive n-th root of unity. Then

(1) $\mathbb{Q}(\zeta)$ is the cyclotomic field of n-th roots of unity (the splitting field of $x^n - 1$).
(2) $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois with $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathbb{Z}_n^*$ abelian.

Galois groups of polynomials.

Let $f(x) \in F[x]$ separable of degree n.

(1) The Galois group G of $f(x)$ is the Galois group of the splitting field of $f(x)$ over F.
(2) G acts on the roots of $f(x)$ and embeds into S_n.
(3) If $f(x) \in \mathbb{Z}[x]$ and $\bar{f}(x) := f(x) \bmod p$ is separable in F_p, then the Galois group of $\bar{f}(x)$ over F_p is permutation group isomorphic to a subgroup of the Galois group of $f(x)$ over $\mathbb{Q}$.

6 problems to expect on the prelim exam.

(1) group theory
(2) group theory
(3) ring theory
(4) modules over PIDs (canonical forms)
(5) field theory
(6) Galois theory