Modern Algebra II Notes

Pramana

Fall 2023

Field extensions, roots of polynomials, splitting fields, simple extensions, linear transformations, matrices, characteristic roots, canonical forms, determinants. Textbook: [DF03].

Professor: Paul Apisa.

Contents

1. Modules

September 7, 2023

1.1. Linear group actions

Definition 1.1

Let G be a group and S be a set. A **group action** $G \curvearrowright S$ is a map from $(g, s) \in G \times S$ to $g \cdot s \in S$ such that

1. $\mathrm{id}_G \cdot s = s$,
2. $g \cdot (h \cdot s) = (gh) \cdot s$.

There is a bijection

$$\left\{\begin{matrix}\text{actions} \\ G \curvearrowright S\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{homomorphisms} \\ \rho\colon G \to \mathrm{Sym}(S)\end{matrix}\right\}.$$

Definition 1.2

If V is a vector space, a group action $G \curvearrowright V$ is **linear** if each $g \in G$ acts *linearly* on V, i.e.

$$g \cdot (av + bw) = a(g \cdot v) + b(g \cdot w).$$

In this case,

$$\left\{\begin{matrix}\text{linear actions} \\ G \curvearrowright V\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{homomorphisms} \\ \rho\colon G \to \mathrm{GL}(V)\end{matrix}\right\},$$

since we can represent bijections $V \to V$ by matrices over V.

1.2. Modules

Definition (R-module)

Definition 1.3

A ring R **acts on an abelian group** M if for all $s, s_1, s_2 \in M$ and $r, r_1, r_2 \in R$,

1. $1_R \cdot s = s$,
2. $r_1 \cdot (r_2 \cdot s) = (r_1 r_2) \cdot s$,
3. $(r_1 + r_2) \cdot s = r_1 \cdot s + r_2 \cdot s$ and $r \cdot (s_1 + s_2) = r \cdot s_1 + r \cdot s_2$.

Definition 1.4

An abelian group M with an R-action is called a **(left) R-module**.

We now cover some examples of R-modules.

Proposition 1.1

If M is an R-module, and $S \subseteq R$ is a subring, then M can also be viewed as an S-module.

Proposition 1.2

If M is an abelian group, then $\mathrm{Hom}_{\mathbf{Ab-Gp}}(M, M)$, the set of group homomorphisms from M to itself, is naturally a ring, where for all $\phi, \psi \in \mathrm{Hom}_{\mathbf{Ab-Gp}}(M, M)$,

- $\phi + \psi$ is defined by $(\phi + \psi)(m) = \phi(m) + \psi(m)$,
- $\phi\psi$ is defined by $\phi\psi = \phi \circ \psi$.

Analogous to the correspondence for group actions and linear group actions, we have one for R-module structures that come about from ring actions on an abelian group.

Proposition 1.3

If M is an abelian group, then

$$\left\{\begin{array}{c}\text{left } R\text{-module} \\ \text{structures on } M\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{ring homomorphisms} \\ \rho\colon G \to \mathrm{Hom}_{\mathbf{Ab-Gp}}(M, M)\end{array}\right\}.$$

Exercise: check this is a ring homomorphism

Proof. ($\longleftarrow$) Given an R-module structure on M, i.e. an R-action on M, we define the ring homomorphism $\rho(r)(m) \coloneqq r \cdot m$.

($\longrightarrow$) Given a ring homomorphism $\rho\colon R \to \mathrm{Hom}_{\mathbf{Ab-Gp}}(M, M)$, define $r \cdot m \coloneqq \rho(r)(m)$. □

Definition 1.5

A **homomorphism (isomorphism) of R-modules** M_1 and M_2 is a group homomorphism (isomorphism) $f\colon M_1 \to M_2$ where for all $r \in R, m \in M$, $r \cdot f(m) = f(r \cdot m)$.

Let M is an R-module. The **endomorphism ring** is the set of R-module homomorphisms from a module to itself. We denote it $\mathrm{End}_R(M) \coloneqq \mathrm{Hom}_{\mathbf{R-Mod}}(M, M)$.

Proposition 1.4 (Endomorphism ring is a subring)

The endomorphism ring is a subring of $\mathrm{Hom}_{\mathbf{Ab-Gp}}(M, M)$.

Example 1.5 – If $M = \mathbb{R}^n$ is an $\mathbb{R}$-module, then

$$\mathrm{End}_{\mathbb{R}}(M) \cong \mathrm{Mat}_{n\times n}(\mathbb{R}).$$

1.2.1. Module examples

September 12, 2023

Definition 1.6

Given a field k and a finite group G, $k[G]$ is the **group algebra** of G, containing linear sums of elements of G, i.e.

$$k[G] \coloneqq \left\{\sum_{g\in G} c_g g : c_g \in k\right\}.$$

Example 1.6 – Let $\mathbb{Z}/3 = \{1, r, r^2\}$. Then

$$\mathbb{R}[\mathbb{Z}/3] = \{a + br + cr^2\} \cong \mathbb{R}[x]/(x^3 - 1).$$

Proposition 1.7

We have the correspondence

$$\{k[G]\text{-modules}\} \longleftrightarrow \{k\text{-vector spaces with a linear action of } G\}.$$

1.2.2. Algebras

Definition (k-algebras)

Definition 1.7

The center of a ring R is defined as

$$Z(R) \coloneqq \{r \in R : sr = rs, \forall s \in R\}.$$

Definition 1.8

R is a k-algebra if $Z(R)$ contains an isomorphic copy of k.

Example 1.8 (k-algebra examples) –

1. If $R = k$, then $Z(R) = k$.
2. If $R = k[x]$, then k is contained in R as constant functions.
3. $R = k[G]$ is an algebra because $Z(R) \supseteq k \cdot 1_G$.

Lemma 1.9 (Modules over k-algebras are k-vector spaces)

Let R be a k-algebra. If V is an R-module, then V is a k-vector space and there is a ring homomorphism $\rho\colon R \to \mathrm{End}_k(V)$ that, if V is finite-dimensional, associates elements of R with a matrix with entries in k.

Proof. Since k is a subring of R, V is a k-module, i.e. a k-vector space. Note that for $r \in R$, $c \in k$ and $v, v_1, v_2 \in V$, then $r \cdot (v_1 + v_2) = rv_1 + rv_2$, and $r(c \cdot v) = (rc) \cdot v$ So $\rho(r)\colon V \to V\colon v \mapsto r \cdot v$ determines a linear map from V to itself, i.e. an element of $\mathrm{End}_k(V)$. □

Lemma 1.10 (Homomorphisms (isomorphisms) between k-algebras)

Let R be a k-algebra. Let V_1 and V_2 be R-modules, which determine homomorphisms $\rho_i\colon R \to \mathrm{End}_k(V_i)$.

$$\mathrm{Hom}(V_1, V_2) \cong \{A\colon V_1 \to V_2 \mid A \text{ is linear}, A\rho_1(r) = \rho_2(r)A, \forall r\},$$
$$\mathrm{Isom}(V_1, V_2) \cong \{A\colon V_1 \to V_2 \mid A \text{ is linear, } \textit{invertible}, A\rho_1(r) = \rho_2(r)A, \forall r\}.$$

Another way of saying the second statement is that V_1 and V_2 are isomorphic if and only if the homomorphisms they correspond to are similar.

Example 1.11 ($\mathbb{R}[x]$-module) – Let $R = \mathbb{R}[x]$. Let $M = \mathbb{R}^2$, and let x be a matrix. We use this to let polynomials $p(x) \in \mathbb{R}[x]$ act on $\mathbb{R}^2$. Then

$$\mathrm{End}_{\mathbb{R}[x]}(M) = \{A \in \mathrm{Mat}_{2\times 2}(\mathbb{R}) : Ax = xA\}.$$

For concreteness, suppose that $x = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be an arbitrary matrix with real entries. Then if $A \in \mathrm{End}_{\mathbb{R}[x]}(M)$,

$$Ax = \begin{bmatrix} a & a+b \\ c & c+d \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ c & d \end{bmatrix} = xA,$$

which implies $c = 0$ and $a = d$, so A is of the form

$$A = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix}.$$

1.2.3. Parallels in linear algebra

Definition 1.9

Given a module M, a subgroup $M' \leq M$ is a **submodule** if it is closed under the R-action.

For example, a $\mathbb{Z}$-module's submodules are just subgroups. A $k[x]$-module's submodules are subspaces that are x-invariant.

Definition 1.10

Let S be some subset of an R-module M. The **span** of S is defined as the set of finite linear combinations in R of elements of S, i.e.

$$\mathrm{span}(S) = \mathrm{span}_R(S) \coloneqq \left\{ \sum_{\substack{i \\ \text{finite}}} r_i \cdot s_i \mid r_i \in R \right\}.$$

A module is **finitely generated** if it has a finite spanning set.

Example 1.12 (Module that is infinitely generated) – Let $R = \mathbb{C}$, and let $M = \mathbb{C}[x]$. Then $M = \mathrm{span}_{\mathbb{C}} \{1, x, x^2, \ldots\}$

1.3. Module constructions

We will introduce different ways to construct modules from other modules.

1.3.1. Quotients

September 14, 2023

Definition 1.11

Let N be a submodule of M. Then the **quotient module** is the abelian group quotient M/N where we define multiplication by elements of R as $r \cdot (m + N) \coloneqq rm + N$.

Given a module homomorphism $f\colon M_1 \to M_2$, we define the **kernel** of f as

$$\ker f \coloneqq \{m \in M_1 \mid f(m) = 0\},$$

and the **image** of f as

$$\operatorname{im} f \coloneqq \{f(m) \mid m \in M_1\}.$$

Lemma 1.13 (First module isomorphism theorem)

1. f is an isomorphism if and only if $\ker f = \{0\}$ and $\operatorname{im} f = M_2$.
2. $\operatorname{im} f \cong M_1/\ker f$.

1.3.2. Direct sums

Definition 1.12

Let $M_1, \dots, M_n$ be modules. The **direct sum** of these modules is

$$\bigoplus_{i=1}^{n} M_i \coloneqq \{(m_1, \dots, m_n) \mid m_i \in M_i\} = M_1 \times \cdots \times M_n.$$

For $r \in R$, we have $r \cdot (m_1, \dots, m_n) \coloneqq (rm_1, \dots, rm_n)$.

The reason for using $\oplus$ instead of $\times$ as we do for groups is because it is the classical notation used for vector spaces.

Lemma 1.14 (Condition for module sum to be direct sum)

Let M be a module with submodules A, B. Suppose that $A \cap B = \{0\}$ and $A + B \coloneqq \{a + b \mid a \in A, b \in B\} = M$. Then $f\colon A \oplus B \to M\colon (a, b) \mapsto a + b$ is an isomorphism.

Proof. $\operatorname{im} f = A + B = M$, so f is a surjection. If $(a, b) \in \ker f$, then $a + b = 0$, i.e. $a = -b \in A \cap B$. So, $a = b = 0$ and f is injective. □

1.3.3. Free modules

Note that R can be viewed as an R-module.

Definition (Free modules)

Definition 1.13

A module M is **free** if it has a linearly independent spanning set.

The prototypical example of a free module we give is the **free module of rank** n defined as $R^n \coloneqq \underbrace{R \oplus \cdots \oplus R}_{n \text{ times}} = \{(r_1, \dots, r_n) \mid r_i \in R\}$ (compare this with the vector space k^n, where k is a field).

Let $[S, R]$ denote the set of all functions from S to R where all but finitely many points are sent to 0. Then $f + r \in [S, R]$, and $rf \in [S, R]$. Then we have $R^n = [\{1, \dots, n\}, R]$.

Lemma 1.15
If M is a free module with a linearly independent spanning set S, then $M \cong [S, R]$.

Proof. Consider

$$\begin{aligned} \Phi \colon [S,R] &\to M \\ f &\mapsto \sum_{s\in S} f(s)\cdot s. \end{aligned}$$

This is clearly an R-module homomorphism. $\operatorname{im}\Phi = \operatorname{span} S = M$. $f \in \ker\Phi$ implies $\sum_{s\in S} f(s)\cdot s = 0$. By linear independence, $f(s) = 0$ for all $s \in S$, i.e. $f \equiv 0$. □

1.4. Tensor products

1.4.1. Bilinear maps

Definition 1.14
Let A, B, C be R-modules. A function $f \colon A \oplus B \to C$ is a **bilinear map** if

1. $f(r\cdot a, b) = rf(a,b)$
2. $f(a, r\cdot b) = rf(a,b)$
3. $f(a_1 + a_2, b) = f(a_1,b) + f(a_2,b)$
4. $f(a, b_1 + b_2) = f(a,b_1) + f(a,b_2)$

A prototypical example would be the dot product of two vectors, with $A = B = \mathbb{R}^n$, $C = \mathbb{R}$.

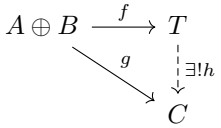
Example 1.16 – We showed in the class worksheet that all bilinear maps $f \colon R^2 \oplus R^2 \to R$ are given by

$$f((r_1,r_2),(r_3,r_4)) = \begin{bmatrix} r_1 & r_2 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} r_3 \\ r_4 \end{bmatrix}.$$

September 19, 2023

Let R be a *commutative* ring. We introduce this new construction, which will lead to the tensor product. This will turn out to be the defining property, or as mathematicians like to call it, the *universal property* of the tensor product. The nice thing about constructing this universal property is that after the universality is proven, we won't have to worry about the details for the proof. We will be using *commutative diagrams* for many of these proofs.

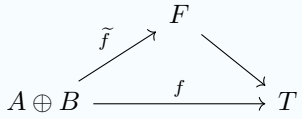
Lemma 1.17 (Universal property of the tensor product)
Let A, B, and C be R-modules. Given an R-module T and a bilinear map $f \colon A \oplus B \to T$ such that for all $g \colon A \oplus B \to C$, there is a *unique* homomorphism $h \colon T \to C$ such that $g = h \circ f$, i.e. the following diagram commutes



Proof. Let F be the free module with basis $A \oplus B$, i.e.

$$F = \left\{ \sum_{\substack{(a,b)\in A\oplus B \\ \text{finite}}} r_{(a,b)}(a,b) \mid r_{(a,b)} \in R \right\}.$$

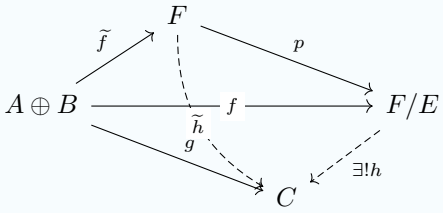
Consider $\widetilde{f}\colon A \oplus B \to F\colon (a,b) \mapsto 1\cdot(a,b)$. We want to show that the following diagram commutes



Let E be the submodule of F generated by

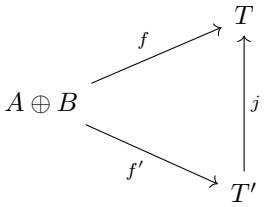
$$\begin{aligned}(x_1 + x_2, y) - (x_1, y) - (x_2, y)\\ (r \cdot x, y) - r \cdot (x, y)\\ (x, y_1 + y_2) - (x, y_1) - (x, y_2)\\ (x, r \cdot y) - r \cdot (x, y).\end{aligned}$$

Let $T = F/E$, $p\colon F \to F/E$ be the projection of F into F/E, and let $f = p \circ \widetilde{f}$. Note that f is bilinear. Suppose that $g\colon A \oplus B \to C$ is bilinear. If $\widetilde{h}\colon F \to C$ is a homomorphism such that $g = \widetilde{h} \circ \widetilde{f}$, then $\widetilde{h}$ sends (a,b) to $g(a,b)$. By bilinearity, all elements of E are in the kernel of $\widetilde{h}$ so $\widetilde{h}$ descends to a homomorphism $h\colon F/E \to C$.



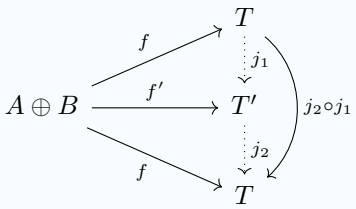
□

Lemma 1.18 (T is unique up to isomorphism)
Suppose that there also exists a bilinear map $f'\colon A \oplus B \to T'$ satisfies the commutative diagram in Lemma 1.17. Then there exists an isomorphism $j\colon T' \to T$ such that $f = j \circ f'$, i.e. the following diagram commutes:



Proof. Use the following diagram with the universal property twice on the outer

triangle to show that $j_2 \circ j_1 = j_1 \circ j_2 = \mathrm{id}$.



□

We have shown that this module T exists and is well-defined, so we give it a name.

Definition 1.15

T is called the **tensor product**, denoted $A \otimes B$. Given $(a, b) \in A \otimes B$, $a \otimes b = f(a, b)$.

Since f is bilinear, the same bilinearity properties apply to the tensors $a \otimes b$.

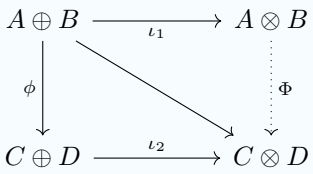
Note that if $\{a_1, \ldots, a_n\}$ is a spanning set of A and $\{b_1, \ldots, b_n\}$ is a spanning set of B, then $\{a_i \otimes b_j\}_{(i,j)}$ is a spanning set of $A \otimes B$. This is because if $a = \sum_i r_i a_i$ and $b = \sum_j r_j b_j$, then

$$\begin{aligned} a \otimes b &= \left\{ \sum_i r_i a_i \right\} \otimes \left\{ \sum_j r_j b_j \right\} \\ &= \sum_{i,j} r_i r_j (a_i \otimes b_j). \end{aligned}$$

Lemma 1.19 (Induced tensor product homomorphism)

If $\phi \colon A \oplus B \to C \oplus D$ is a homomorphism, then there is an induced homomorphism $\Phi \colon A \otimes B \to C \otimes D$.

Proof (sketch). Consider the following diagram:



First we must show that the diagonal is bilinear. Then, Φ exists by the universal property. □

Lemma 1.20 (Tensored modules commute)

$A \otimes B \cong B \otimes A$.

Proof. With the isomorphism $\phi \colon A \oplus B \to B \oplus A \colon (a, b) \mapsto (b, a)$, we use the previous lemma to find the isomorphism $\Phi \colon A \otimes B \to B \otimes A$. □

Lemma 1.21
$R \otimes A \cong A$.

Proof. Let $g\colon R \oplus A \to A\colon (r, a) \mapsto r \cdot a$ be a bilinear map. By the universal property, the following diagram commutes

$$\begin{array}{ccc} R \oplus A & \xrightarrow{f} & R \otimes A \\ & \searrow^{g} & \downarrow{\scriptstyle h} \\ & & A \end{array}$$

We will prove h is an isomorphism. $\operatorname{im}(f) = \operatorname{im}(h) = A$ since the diagram commutes.

$$\begin{aligned} \ker(h) &= \left\{ \sum_i r_i \otimes a_i \mid \sum_i r_i a_i = 0 \right\} \\ &= \left\{ \sum_i r_i (1 \otimes a_i) \mid \sum_i r_i a_i = 0 \right\} \\ &= \left\{ \sum_i 1 \otimes r_i a_i \mid \sum_i r_i a_i = 0 \right\} \\ &= \left\{ 1 \otimes \left(\sum_i \otimes r_i a_i \right) \mid \sum_i r_i a_i = 0 \right\} \\ &= \{1 \otimes 0\} \\ &= \{0\}. \end{aligned}$$

□

Lemma 1.22
$(A \oplus B) \otimes C \cong (A \otimes C) \oplus (B \otimes C)$.

Remark 1.23. This means that the set of R-modules forms a *commutative semiring* using $\oplus$ for addition and $\otimes$ for multiplication.

Theorem 1.24 (Rank of free module is well-defined)
For a commutative ring R, if $R^n \cong R^m$, then $n = m$.

Proof. Let $\mathfrak{p}$ be a maximal ideal of R, so $R/\mathfrak{p} = k$ is a field. Then

$$\begin{aligned} k^n &\cong (R/\mathfrak{p})^n \\ &\cong \underbrace{(R \otimes R/\mathfrak{p}) \oplus \cdots \oplus (R \otimes R/\mathfrak{p})}_{n \text{ times}} \\ &\cong R^n \otimes R/\mathfrak{p} \\ &\cong R^m \otimes R/\mathfrak{p} \\ &\cong \underbrace{(R \otimes R/\mathfrak{p}) \oplus \cdots \oplus (R \otimes R/\mathfrak{p})}_{m \text{ times}} \\ &\cong (R/\mathfrak{p})^m \\ &\cong k^m. \end{aligned}$$

So $k^n \cong k^m$ as R-modules. But since the R-action factors through $k = R/\mathfrak{p}$ action, $k^n \cong k^m$ as k-modules, i.e. vector spaces. So $n = m$. □

This last lemma is mostly useful for the worksheet in class today.

Lemma 1.25
If A is an abelian group, $A \otimes \mathbb{Z}/n \cong A/nA$, where $nA \coloneqq \{n \cdot a \mid a \in A\}$.

September 21, 2023

Proposition 1.26
For R-modules A, B, C,

$$\operatorname{Hom}(A \oplus B, C) \cong \operatorname{Hom}(A, C) \oplus \operatorname{Hom}(B, C),$$

$$\operatorname{Hom}(A, B \oplus C) \cong \operatorname{Hom}(A, B) \oplus \operatorname{Hom}(A, C).$$

By induction, for the sets of R-modules $\{A_i\}$, $\{B_j\}$.

$$\operatorname{Hom}\left(\bigoplus_i A_i, \bigoplus_j B_j\right) \cong \bigoplus_{i,j} \operatorname{Hom}(A_i, B_j).$$

Proposition 1.27 (Vector space decomposition with $W^\perp$)
Let $k \subseteq \mathbb{R}$ and let V be k-vector spaces. Consider $\langle \cdot, \cdot \rangle : V \times V \to k$, a symmetric ($\langle v, w \rangle = \langle w, v \rangle$) bilinear map so that $\langle v, v \rangle > 0$ if $v \neq 0$. Let $W \subseteq V$ be a subspace. Let

$$W^\perp \coloneqq \{v \in V \mid \forall w \in W, \langle v, w \rangle = 0\}.$$

Then $V \cong W \oplus W^\perp$.

1.5. Simplicity and Schur's lemma

Our goal for this section is to classify all group homomorphisms $G \to \mathrm{GL}_n(\mathbb{R})$ (i.e. *representations*) up to change of basis. We showed a correspondence between

$$\left\{\begin{array}{c}\mathbb{R}[G]\text{-module structure} \\ \text{on } \mathbb{R}^n\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{ring homomorphisms} \\ \varphi\colon \mathbb{R}[G] \to \mathrm{Mat}_{n\times n}(\mathbb{R})\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{group homomorphisms} \\ \rho\colon G \to \mathrm{GL}_n(\mathbb{R})\end{array}\right\}$$

Moreover, we have the correspondence

$$\left\{\begin{array}{c}\mathbb{R}[G]\text{-module structure on } \mathbb{R}^n \\ \textit{up to isomorphism}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{ring homom. } \varphi, \text{ where} \\ \varphi, A\varphi A^{-1} \text{ define the} \\ \text{same structure, } A \in \mathrm{GL}_n(\mathbb{R})\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{group homom. } \rho \\ \text{where } \rho \text{ and } A\rho A^{-1} \text{ define} \\ \text{isom. modules, } \forall A \in \mathrm{GL}_n(\mathbb{R})\end{array}\right\}$$

The takeaway from these correspondences is that if R is a k-algebra, then $M_1 \cong M_2$ if and only if the R-actions agree up to a *change of basis*.

Lemma 1.28 (Module decomposition with $W^\perp$)
Let $k \subseteq \mathbb{R}$. Let V be a finite dimensional $k[G]$-module. If W is a submodule of V, then there is a submodule U of V such that $V \cong W \oplus U$ as modules.

Proof. Let $\langle v, w\rangle \coloneqq v \cdot w$. Let $(v, w) \coloneqq \sum_{g\in G} \langle gv, gw\rangle$. This is a symmetric bilinear map so that $(v, v) > 0$ if $v \neq 0$. So as *vector spaces*, $V \cong W \oplus W^\perp$.

We want to show that $W^\perp$ is a G-invariant (or equivalently, $W^\perp$ is a submodule). Let $w \in W^\perp$, $h \in G$, $v \in W$.

$$\begin{aligned}(h \cdot w, v) &= \sum_{g\in G} \langle ghw, gv\rangle \\ &= \sum_{g\in G} \big\langle (gh) \cdot w, (gh)h^{-1} \cdot v\big\rangle \\ &= \sum_{\gamma\in G} \big\langle \gamma \cdot w, \gamma h^{-1} \cdot v\big\rangle && (\gamma = gh) \\ &= (w, \underbrace{h^{-1} \cdot v}_{\in W}) \\ &= 0.\end{aligned}$$

So $h \cdot w \in W^\perp$. □

The proof holds even if $k \subseteq \mathbb{C}$ (use the *Hermitian product* instead of the dot product).

In the homework we encountered simple modules:

Definition 1.16
A non-zero R-module M is simple is its only submodules are 0 and itself.

Corollary 1.29
If $k \subseteq \mathbb{C}$, then any $k[G]$-module is isomorphic to the direct sum of simple modules.

Proof. Induct on $\dim V$. If $\dim V = 1$, V is automatically simple. For the inductive step, if V is simple, we are done. Otherwise, it contains a submodule A, and hence, we can write $V = A \oplus B$ by Lemma 1.28, where $\dim A, \dim B < \dim V$. By induction, we can decompose A and B. □

Definition 1.17
A division algebra over k is a ring whose center contains k, and so every $0 \neq d \in D$ is invertible.

Lemma 1.30 (Schur's lemma)
Let S and T be simple non-isomorphic $k[G]$-modules. Then

1. $\mathrm{Hom}_{k[G]}(S,T) = 0$,
2. $\mathrm{End}_{k[G]}(S) = \mathrm{Hom}_{k[G]}(S,S)$ is a division algebra over k.

Proof. Let $f\colon S \to T$ be a homomorphism. $\ker f$ is a submodule of S, so $\ker f = S$ (then f is zero) or $\ker f = 0$ (then f is injective). In the second case, $\mathrm{im}\, f \neq 0$, so $\mathrm{im}\, f = T$, so f is surjective (hence an isomorphism). So if $f\colon S \to S$ is non-zero, then it is invertible. □

Note that if $f\colon C \to C$ for some $c \in k$, the f is central since all homomorphisms are k-linear maps.

Corollary 1.31 (Finite dimensional algebras over $\mathbb{R}$ and $\mathbb{C}$)
The only finite dimensional division algebras over $\mathbb{R}$ are $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{H}$. The only finite dimensional division algebra over $\mathbb{C}$ is $\mathbb{C}$.

Lemma 1.32
Let R be a k-algebra, and let V be a finite dimensional R-module. Then *as k-vector spaces*, $V \cong \mathrm{Hom}_R(R,V)$.

Proof. Given $v \in V$, consider $\phi_v\colon R \to V\colon r \mapsto r \cdot v$. Then let

$$\begin{aligned}\Phi\colon V &\to \mathrm{Hom}_R(R,V)\\ : v &\mapsto \phi_v.\end{aligned}$$

This is a k-linear map. $\ker \Phi = \{v \mid \phi_v \equiv 0\}$ Since $\phi_v(1) = v$, $v = 0$, and $\ker \Phi = \{0\}$. Suppose $\phi\colon R \to V$ is an R-module homomorphism.

$$\phi(r) = \phi(r \cdot 1) = r \cdot \phi(1).$$

So $\phi = \phi_{\phi(1)}$, so $\mathrm{im}(\Phi) = \mathrm{Hom}_R(R,V)$. □

Theorem 1.33 (Calculations from Schur's lemma)
Let $k[G] = \bigoplus_i S_i^{n_i}$ (which we can do by Corollary 1.29), where S_i is simple, and $S_i \ncong S_j$ if $i \neq j$. Let $e_i := \dim \mathrm{End}_{k[G]}(S_i)$. Then the following hold

1. For all simple modules S, $S \cong S_i$ for some i,
2. $n_i e_i = \dim S_i$,
3. $|G| = \sum_i \frac{(\dim S_i)^2}{e_i}$.

Proof. (1) Let $R = k[G]$. Let S be a simple module.

$$\begin{aligned} S &\cong \mathrm{Hom}_R(R, S) \\ &\cong \mathrm{Hom}_R\left(\bigoplus_i S_i^{n_i}, S\right) \\ &\cong \bigoplus_R \mathrm{Hom}_R(S_i, S)^{n_i}. \end{aligned}$$

By Lemma 1.30, $S \cong S_i$ for some i.

(2) We have

$$\dim S_i = \dim \bigoplus_j \mathrm{Hom}_R(S_j, S_i)^{n_j} = \dim \mathrm{Hom}_R(S_j, S_i)^{n_i} = e_i n_i.$$

(3)

$$\begin{aligned} |G| &= \dim k[G] \\ &= \dim \mathrm{Hom}_R(k[G], k[G]) \\ &= \dim \mathrm{Hom}_R\left(\bigoplus_i S_i^{n_i}, \bigoplus_i S_i^{n_i}\right) \\ &= \dim\left(\bigoplus_{i,j} \mathrm{Hom}_R(S_i, S_j)^{n_i n_j}\right) \\ &= \dim\left(\bigoplus_i \mathrm{Hom}_R(S_i, S_i)^{n_i^2}\right) \\ &= \sum_i n_i^2 e_i \\ &= \sum_i \frac{(n_i e_i)^2}{e_i} \\ &= \sum_i \frac{(\dim S_i)^2}{e_i}. \end{aligned}$$

□

This theorem will be very useful for decomposing $k[G]$-modules. (1) tells us that we can decompose $k[G]$-modules decomposes in to a direct sum of its simple modules, (2) gives us a way to find the dimensions of the endomorphism algebras, and (3) lets us verify that we have found *all* simple modules for a $k[G]$-module.

Corollary 1.34

The only simple $\mathbb{C}[G]$-modules when $G \cong \mathbb{Z}/n$ are 1-dimensional.

Proof. Consider $\rho_k \colon \mathbb{Z}/n \to \mathrm{GL}_1(\mathbb{C}) \cong \mathbb{C}^\times \colon 1 \mapsto \zeta_n^k$, where $\zeta_n = \exp\left(\frac{2\pi}{n}\right)$. This gives n distinct $\mathbb{C}[G]$-modules. $n = |G| = 1^2 + \cdots + 1^2 = \dim(S_1 \oplus \cdots \oplus S_n)$, where S_k is simple module corresponding to ρ_k. □

Corollary 1.35

Every element of finite order in $\mathrm{GL}_n(\mathbb{C})$ is diagonalizable.

Proof. Suppose $A \in \mathrm{GL}_n(\mathbb{C})$ has finite order m. Then $\rho\colon \mathbb{Z}/m \to \mathrm{GL}_n(\mathbb{C})$ by $k \mapsto A^k$ is a group homomorphism, so we have a corresponding $\mathbb{C}[\mathbb{Z}/m]$-module structure on $\mathbb{C}^n$, where x acts on $v \in \mathbb{C}^n$ by $x \cdot v = Av$. By the previous example, all $\mathbb{C}[\mathbb{Z}/m]$-modules are 1-dimensional, so we can decompose $\mathbb{C}^n$ into a direct sum of 1-dimensional modules S_i, $\mathbb{C}^n \cong \bigoplus_{i=1}^n S_i$. To find out how $x \in \mathbb{Z}/m$ acts on $\bigoplus_{i=1}^n S_i$, we know that

$$x \cdot (s_1, \ldots, s_n) = (\rho_1(x) \cdot s_1, \ldots, \rho_n(x) \cdot s_n),$$

where $\rho_i\colon \mathbb{Z}/m \to \mathbb{C}^\times$ is the homomorphism by which x acts on each S_i. Recall that A is diagonalizable if there exists invertible matrix M and diagonal matrix D such that

$$D = M^{-1}AM.$$

Since the action $(\rho_1, \ldots, \rho_n)$ and ρ define isomorphic modules, we can find a matrix M such that

$$\begin{bmatrix} \rho_1(x) & & \\ & \ddots & \\ & & \rho_n(x) \end{bmatrix} = M^{-1}AM,$$

where the LHS is the matrix corresponding to how $(\rho_1, \ldots, \rho_n)$ acts on $\bigoplus_{i=1}^n S_i$. □

Since $\mathrm{tr}(A^{-1}BA) = \mathrm{tr}(B)$ for all matrices A, B, we have the following corollary.

Corollary 1.36 (Equality between traces of isomorphic modules)
If ρ_1 and ρ_2 determine isomorphic $\mathbb{R}[G]$-modules, then $\mathrm{tr}(\rho_1(g)) = \mathrm{tr}(\rho_2(g))$.

September 26, 2023

Example 1.37 (Dihedral group modules) – Let $G = \langle r, t \mid r^2 = t^n = (tr)^2 = 1 \rangle$ be the dihedral group of order $2n$. The simple $\mathbb{C}[G]$-modules are the following:

1. $\langle r \rangle \trianglelefteq G$ and $G/\langle r \rangle \cong \mathbb{Z}/2$, so we have two 1-dimensional modules:

$$\begin{aligned} \rho_{\mathrm{triv}}&\colon G \to \mathbb{C}^\times \\ &\colon g \mapsto 1, \\ \rho_{\mathrm{sgn}}&\colon G \to \mathbb{C}^\times \\ &\colon r^a t^b \mapsto (-1)^b. \end{aligned}$$

2. Consider the 2-dimensional $\mathbb{C}[G]$ modules for $1 \le k \le \frac{n-1}{2}$:

$$\begin{aligned} \rho_k&\colon G \to \mathrm{GL}_2(\mathbb{R}) \\ r &\mapsto \mathrm{rot}_{\frac{2\pi k}{n}} = \begin{bmatrix} \cos\left(\frac{2\pi k}{n}\right) & -\sin\left(\frac{2\pi k}{n}\right) \\ \sin\left(\frac{2\pi k}{n}\right) & \cos\left(\frac{2\pi k}{n}\right) \end{bmatrix} \\ t &\mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \end{aligned}$$

   Since $\mathrm{tr}(\rho_k(r)) = 2\cos\left(\frac{2\pi k}{n}\right)$, these modules are not isomorphic.

Let's compare $|G|$ to $\sum_i (\dim S_i)^2$. We have

$$(1)^2 + (1)^2 + \left(\frac{n-1}{2}\right) \cdot 2^2 = 2 + 2n - 2 = 2n.$$

Since this sum is $|G|$, we have found all the simple modules.

Example 1.38 (HW3 Problem 4.a) – Let $G = \mathbb{Z}/n$. Find all simple $\mathbb{R}[G]$-modules.
Simple $\mathbb{R}[G]$-modules correspond to group homomorphisms $\rho\colon G \to \mathrm{GL}_m(\mathbb{R})$, where $m \in \mathbb{N}$.

- For $m = 1$, $\rho_{\mathrm{triv}}\colon c \mapsto 1$ for all $c \in \mathbb{Z}/n$. If n is even then we have the map $\rho_{\mathrm{sgn}}\colon c \mapsto (-1)^c$. Since $n_i e_i = \dim S_i = 1$, the endomorphism algebras have dimension 1.
- For $m = 2$, we have the modules defined on the generator $1 \in \mathbb{Z}/n$

  $$\rho_k\colon 1 \mapsto \mathrm{rot}_{\frac{2\pi k}{n}},$$

  where rot_θ is a rotation matrix in $\mathrm{GL}_2(\mathbb{R})$ by θ. If n is odd, we let $1 \le k \le \frac{n-1}{2}$, if n is even, we let $1 \le k \le \frac{n-2}{2}$.
  Since $\mathrm{tr}(\rho_k(1)) = 2\cos\left(\frac{2\pi k}{n}\right)$ are not equal for any two k, none of these modules are isomorphic.
  $\mathrm{rot}_{\frac{2\pi}{2n}}$ is not a scalar multiple of the other rotation matrices, and

  $$\mathrm{rot}_{\frac{2\pi}{2n}}\mathrm{rot}_{\frac{2\pi k}{n}} = \mathrm{rot}_{\frac{2\pi k}{n}}\mathrm{rot}_{\frac{2\pi}{2n}},$$

  so the dimension of the endomorphism algebra is at least 2. Since $n_i e_i = \dim S_i = 2$ for the two-dimensional simple modules S_i, $e_i = 2$.

At this point, we stop, since by looking at the sum,

submodule dimension	n odd	n even
1	ρ_{triv}	$\rho_{\mathrm{triv}}, \rho_{\mathrm{sgn}}$
2	$\{\rho_k\}_{1\le k\le \frac{n-1}{2}}$	$\{\rho_k\}_{1\le k\le \frac{n-2}{2}}$
comparison with $\lvert\mathbb{Z}/n\rvert = n$	$1^2 + \frac{n-1}{2}\left(\frac{2^2}{2}\right) = n$	$1^2 + 1^2 + \frac{n-2}{2}\left(\frac{2^2}{2}\right) = n$

Thus, we have found all simple $\mathbb{R}[\mathbb{Z}/n]$-modules.

For computing 1-dimensional representations (i.e. 1-dimensional (simple) $k[G]$-modules) we have a trick. Notice that $\rho\colon G \to \mathrm{GL}_1(k) = k^\times$ is a map from the group into an abelian group. Therefore, it must factor through the abelianization of G, $G/[G,G]$. The number of representations precisely corresponds with the order of $G/[G,G]$.

September 26, 2023

The following generalizes the last step in the proof of Corollary 1.35.

Corollary 1.39

Suppose V and $V_1, \dots, V_n$ are $\mathbb{R}[G]$ modules determined by ρ and $\rho_1, \dots, \rho_n$. Then if $V \cong V_1 \oplus \cdots \oplus V_n$, then up to change of basis,

$\rho_1(g)$ are block matrices.

$$\rho(g) = \begin{bmatrix} \boxed{\rho_1(g)} & & \\ & \ddots & \\ & & \boxed{\rho_n(g)} \end{bmatrix}$$

The simplest case of a decomposition of a $k[G]$ module is with $k = \mathbb{C}$.

Theorem 1.40

$\mathbb{C}[G] \cong S_1^{\dim S_1} \oplus \cdots \oplus S_n^{\dim S_n}$, where each simple $\mathbb{C}[G]$ module corresponds to a unique S_i.

We proved the following theorem on the homework, which is a generalization of Corollary 1.29.

Theorem 1.41 (Maschke's theorem)
Let k be a field. Let V be a finite-dimensional k-vector space. Suppose that V is a $k[G]$-module where G is a finite group, and $|G|$ is invertible in k. Then V is a direct sum of simple $k[G]$-modules.

1.6. Extending linear algebra to R^n

If R is a commutative ring, we've seen that R^n is "sometimes like a vector space." For example, $\mathrm{Hom}_R(R^n, R^n) \cong \mathrm{Mat}_{n\times n}(R)$. The goal of this section will be to define a "determinant" on homomorphisms between free R-modules.

1.6.1. Multilinear maps

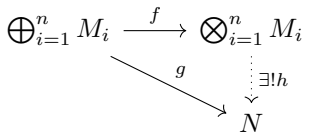
Definition 1.18
Let (M_i) be R-modules and let N be an R-module. A map $f\colon M_1 \oplus \cdots \oplus M_n \to N$ is **multilinear** if it is linear in each entry, i.e.

$$f(m_1, \ldots, r\cdot m_i + m_i', \ldots, m_n) = r\cdot f(m_1, \ldots, m_i, \ldots, m_n) + f(m_1, \ldots, m_i', \ldots, m_n).$$

$V^{\oplus n} = \underbrace{V \oplus \cdots \oplus V}_{n \text{ times}}$

The determinant $\det\colon V^{\oplus n} \to k$ is multilinear. Moreover, the determinant is *alternating*, i.e. $\det(v_1, \ldots, v_n) = 0$ if $v_i = v_j$ for some $i \neq j$.

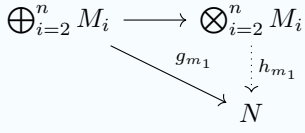
Theorem 1.42 (Universal property of tensor product for multilinear maps)
For any multilinear map $g\colon \bigoplus_{i=1}^n M_i \to N$, there exists a homomorphism $h\colon \bigotimes_{i=1}^n M_i \to N$ such that the following diagram commutes:



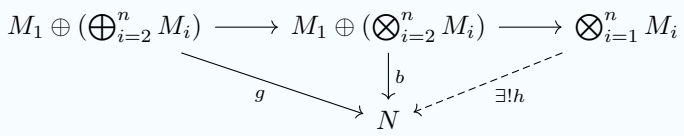
Proof. We prove this by induction on n. $n = 2$ is just the case with the regular tensor product. For each $m_1 \in M_1$, there exists a multilinear map

$$\begin{aligned} g_{m_1}\colon &\bigoplus_{i=2}^{n} M_i \to N \\ &: (m_2, \ldots, m_n) \mapsto g(m_1, \ldots, m_n). \end{aligned}$$

We can think of this as the map corresponding to the diagram



We then can add M_1 to get the diagram:



If we construct the bilinear map $b\colon (m_1, m_2 \otimes \cdots \otimes m_n) \mapsto h_{m_1}(m_2 \otimes \cdots \otimes m_n) = f(m_1, \ldots, m_n)$, by the universal property, we find the map h. □

September 28, 2023

Suppose $R^n \cong M$ with span $e_1, \ldots, e_n$. Then $M \otimes M$ is free of rank n^2 with basis $\{e_i \otimes e_j\}_{i,j}$. Then $M^{\otimes k} := \underbrace{M \otimes \cdots \otimes M}_{k \text{ times}}$ is free of rank n^k with basis $\{e_{i_1} \otimes \cdots e_{i_n}\}$.

By Theorem 1.42, there is a bijection from the set of multilinear maps $M^{\oplus n} \to N$ and $\mathrm{Hom}_R(M^{\otimes k}, N)$.

1.6.2. Exterior products

Tensor products were what every bilinear map filtered through. Exterior products will be what every *alternating* bilinear map will filter through.

Definition 1.19

A multilinear map $f\colon M^{\oplus k} \to N$ is **alternating** if $f(m_1, \ldots, m_k) = 0$ for $m_i = m_j$, $i \neq j$.

For notation, given $\sigma \in \mathrm{Sym}(k)$ and $v = (m_1, \ldots, m_n)$, we let $v^\sigma := (m_{\sigma(1)}, \ldots, m_{\sigma(n)})$. Recall that the **sign homomorphism** $\mathrm{sgn}\colon \mathrm{Sym}(k) \to \{\pm 1\}$ such that $\mathrm{sgn}(\sigma) = (-1)^\ell$, where ℓ is the number of transpositions in σ.

Lemma 1.43

Let $v \in M^{\oplus n}$, let $\sigma \in \mathrm{Sym}(k)$ and $f\colon M^{\oplus n} \to N$ and alternating, then $f(v^\sigma) = \mathrm{sgn}(\sigma) f(v)$.

Proof. We can work out the case where $\sigma = (12)$:

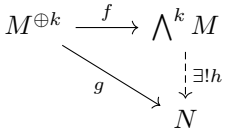
$$\begin{aligned} 0 &= f(v_1 + v_2, v_1 + v_2, \ldots, v_k) \\ &= f(v_1, v_1 + v_2, \ldots, v_k) + f(v_2, v_1 + v_2, \ldots, v_k) \\ &= f(v_1, v_1, \ldots) + f(v_1, v_2, \ldots) + f(v_2, v_1, \ldots) + f(v_2, v_2, \ldots) \\ &= f(v_1, v_2, \ldots) + f(v_2, v_1, \ldots). \end{aligned}$$

Since $\sigma \in \mathrm{Sym}(k)$ is a product of transpositions, we can generalize this further. □

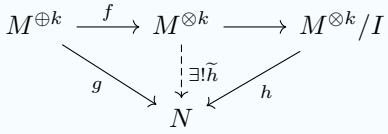
Definition 1.20

The **kth exterior product** $\bigwedge^k M$ is the quotient of $M^{\otimes n}$ by the submodule I generated by the subset of $\{m_1 \otimes \cdots \otimes m_k\}$ where $m_i = m_j$ for some $i \neq j$.

Theorem 1.44 (Universal product of exterior product)
Consider $f\colon M^{\oplus k} \to M^{\otimes k} \to M^{\otimes k}/I$ by $(m_1, \dots, m_n) \mapsto m_1 \otimes \cdots \otimes m_n \mapsto m_1 \otimes \cdots \otimes m_n + I$. This is an alternating map. Moreover, if $g\colon M^{\oplus k} \to N$ is an alternating bilinear map, then $\exists! h\colon \bigwedge^k M \to N$, a module homomorphism, such that $g = h \circ f$, i.e. the following diagram commutes:



Proof.



Since g is alternating, any element of the form $m_1 \otimes \cdots \otimes m_n$, where $m_i = m_j$ for some $i \neq j$ is in the kernel of h. So $\ker \widetilde{h} \supseteq I$. □

Denote $f(m_1, \dots, m_k) =: m_1 \wedge \cdots \wedge m_k$. The $\wedge$ symbol stands for *wedge*.

Remark 1.45. $e_1 \otimes e_2 \neq e_2 \otimes e_1$ sometimes, but $e_1 \wedge e_2 = -e_2 \wedge e_1$ always.

Once again, let $R^n \cong M = \operatorname{span}_R(e_1, \dots, e_n)$. As with $M^{\otimes k}$, $\bigwedge^k M$ is spanned by $\{e_{i_1} \wedge \cdots \wedge e_{i_n}\}$, where $1 \leq i_1 < \cdots < i_k \leq n$. Let this set be B.

Theorem 1.46 (Rank of exterior product)
$\bigwedge^k M$ is a free module of rank $\binom{n}{k}$ with basis B.

Proof. Let

$$\begin{aligned} \varphi\colon M^{\oplus k} &\to M^{\otimes k} \\ : (m_1, \dots, m_k) &\mapsto \sum_{\sigma \in \operatorname{Sym}(k)} \operatorname{sgn}(\sigma) m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(k)}. \end{aligned}$$

φ is multilinear, since it is a sum of multilinear maps (by using $f\colon M^{\oplus k} \to M^{\otimes k}$ to define elements of $M^{\otimes k}$).

We claim φ is alternating. Let $v = (m_1, \dots, m_k)$ such that $m_1 = m_2$. Let $\{\tau_i\}$ be a collection of permutations so that $\sigma \in \operatorname{Sym}(k)$ is either $\sigma = \tau_i$ or $\sigma = \tau_1(12)$.

$$\begin{aligned} \phi(v) &= \sum_{i=1}^{n!/2} \operatorname{sgn}(\tau_i) f(v_i^\tau) + \operatorname{sgn}(\tau_i(12)) f(v^{\tau_i(12)}) \\ &= \sum_{i=1}^{n!/2} \operatorname{sgn}(\tau_i) f(v_i^\tau) - \operatorname{sgn}(\tau_i) f(v^{\tau_i}) \\ &= 0. \end{aligned}$$

By the universal property, we have

$$\begin{aligned} h\colon \bigwedge^k &\to M^{\otimes k} \\ : m_1 \wedge \cdots \wedge m_k &\mapsto \sum_{\sigma \in \mathrm{Sym}(k)} \mathrm{sgn}(\sigma) m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(k)}. \end{aligned}$$

Now we show that B is a linearly independent set. Since $B' \coloneqq \{e_{i_1} \otimes e_{i_k}\}$ is linearly independent in $M^{\otimes k}$, if B were not linearly independent, then there would be a linear relation

$$\sum_{1 \le i_1 < \cdots < i_k \le n} \mathrm{const} \cdot e_{i_1} \wedge \cdots \wedge e_{i_k}$$

that was sent under φ to a nontrivial linear relation between B', a contradiction. □

Definition 1.21

Let $A\colon M \to M$ be an R-module homomorphism. $\bigwedge^k A$ is the module homomorphism such that the following diagram commutes:

$$\begin{array}{ccc} M^{\oplus k} & \xrightarrow{f} & \bigwedge^k M \\ {\scriptstyle A^{\oplus k}}\downarrow & \searrow & \downarrow{\scriptstyle \bigwedge^k A} \\ M^{\oplus k} & \xrightarrow[f]{} & \bigwedge^k M \end{array}$$

Where $f\colon M^{\oplus k} \to \bigwedge^k M$ is the map $(m_1, \ldots, m_k) \mapsto m_1 \wedge \cdots \wedge m_k$.

If $M \cong R^n$, then $\bigwedge^k M$ is free of rank 1. If $M = \mathrm{span}_R(e_1, \ldots, e_n)$, then $\bigwedge^n M = \mathrm{span}_R(e_1 \wedge \cdots \wedge e_n)$. If $A \in \mathrm{Mat}_{n\times n}(R) \cong \mathrm{Hom}_R(R^n, R^n)$, so $\bigwedge^n A\colon \bigwedge^n M \to \bigwedge^n M$. Any R-module endomorphism f is given by $f(x) = r \cdot x$ for some $r \in R$. So $\bigwedge^n A$ is multiplication by $r \in R$. The value is defined to be the **determinant of the R-module homomorphism A**, $\det A \coloneqq r$.

1.6.3. Properties of determinants

October 3, 2023

Lemma 1.47

Let $M \cong R^n$ with basis $e_1, \ldots, e_n$. Let $A\colon M \to M$ be an R-module homomorphism. Let $A(e_1) = \sum_{i=1}^n a_{i,j} e_j$, where $a_{i,j} \in R$.

Then

$$\det A = \sum_{\sigma \in \mathrm{Sym}(n)} \mathrm{sgn}(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}.$$

Remark 1.48. This is a very inefficient way of calculating the determinant, needing on the order of $n! \cdot n$ calculations.

Proof.

$$\begin{aligned}(\bigwedge^n A)(e_1 \wedge \cdots \wedge e_n) &= A(e_1) \wedge \cdots \wedge A(e_n) \\ &= (a_{1,1}e_1 + c \cdots + a_{1,n}e_n) \wedge (a_{2,1}e_1 + c \cdots + a_{2,n}e_n) \wedge \cdots \\ &= \sum_{f\colon \{1,\ldots,n\}\to\{1,\ldots,n\}} (a_{1,f(1)} \cdots a_{n,f(n)}) e_{f(1)} \wedge \cdots \wedge e_{f(n)}\end{aligned}$$

f must be a bijection for the wedge to be nonzero

$$\begin{aligned}&= \sum_{\sigma\in \mathrm{Sym}(n)} (a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}) e_{\sigma(1)} \wedge \cdots \wedge e_{\sigma(n)} \\ &= \left[\sum_{\sigma\in\mathrm{Sym}(n)} \mathrm{sgn}(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}\right] e_1 \wedge \cdots \wedge e_n \\ &= \det A.\end{aligned}$$

□

Lemma 1.49

Let $M \cong R^n$. Let $A, B\colon M \to M$ be an R-module homomorphism Then $\det AB = \det A \det B$.

Proof. Let $(e_1, \ldots, e_n)$ be a basis.

$$\begin{aligned}(\bigwedge^n AB)(e_1 \wedge \cdots e_n) &= A(B(e_1)) \wedge \cdots A(B(e_n)) \\ &= (\bigwedge^n A)(B(e_1) \wedge \cdots \wedge B(e_n)) \\ &= \det A(Be_1 \wedge \cdots Be_n) \\ &= \det A \cdot (\bigwedge^n B)(e_1 \wedge \cdots \wedge e_n) \\ &= \det A \det Be_1 \wedge \cdots \wedge e_n.\end{aligned}$$

□

1.6.4. Principal ideal domains

Definition 1.22

R is a **principal ideal domain (PID)** if the following hold:

1. if $x, y \in R - \{0\}$, then $xy \neq 0$ (i.e. a PID is an *integral domain*)
2. if $I \subseteq R$ is an ideal, then there is $x \in R$ such that $I = (x)$, the ideal generated by x.

Example 1.50 – $\mathbb{Z}$ and $k[x]$ are PIDs. So is $R_{(p)}$, where R is a PID and p is prime.

Let R be a PID.

Definition 1.23

Given $x, y \in R$, we let $(x, y) \coloneqq \{r_1 x + r_2 y \mid r_1 r_2 \in R\} = (e)$. The element e is called the **greatest common divisor** of x and y.

If e is invertible, then x and y are called **coprime**.

Lemma 1.51
If $(e) = (f)$, $e = cf$, where c is invertible.

Proof. Since e is in the ideal generated by f and vice versa, $e = c_1 f = c_1(c_2 e)$, so $(1 - c_1 c_2)e = 0$. Either e is zero, in which case c can be 1, or e is not zero, so $1 = c_1 c_2$, so $c = c_1$ is invertible. □

Lemma 1.52
If $x, y \in R$ and $(e) = (x, y)$, then there are coprime elements a and b so that $ax + by = e$.

Proof. Since $(x, y) = (e)$, there exist $a, b \in R$ s.t. $ax + by = e$. Let $f \in R$ be any common factor of a and b. Suppose $a = fa'$ and $b = fb'$ for $a', b' \in R$. Then $e = ax + by = f(a'x + b'y)$. Then $(e) \subseteq (a'x + b'y) \subseteq (x, y) = (e)$. Then $(e) = (a'x + b'y)$ so by the previous lemma, f is invertible. □

1.6.5. Smith normal form

Definition 1.24
Let $M \cong R^n$. Let $v_1, \ldots, v_n \in M$. A **quasi-elementary operation** on $(v_1, \ldots, v_n)$ is

$$(v_1, \ldots, v_i, \ldots, v_j \ldots, v_n) \to (v_1, \ldots, av_i + bv_j, \ldots, cv_i + dv_j \ldots, v_n)$$

where $a, b, d, c \in R$ and $ad - bc$ is invertible.

We can represent q.e. operations as

$$A \to \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & a & & b & & \\ & & & \ddots & & & \\ & & c & & d & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix} A.$$

Note that q.e. operations are invertible, since $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. The inverse of this matrix is similar to the case of the 2×2 matrix. The operation also has the same determinant as its transpose.

Example 1.53 (Comparison with elementary operations in linear algebra) – The elementary operations we know in linear algebra can be turned into quasi-elementary operations.

1. $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ swaps v_i and v_j
2. $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ sends $v_i \to v_i + v_j$
3. $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$ sends $v_i \to av_i$, where a is invertible.

Definition 1.25

A **quasi-elementary row (column) operation** on $A \in \mathrm{Mat}_{n\times n}(R)$ is given by multiplication on the left (right) by an invertible matrix.

Proposition 1.54

Let $A \in \mathrm{Mat}_{n\times n}(R)$. Then there are $S, D, T \in \mathrm{Mat}_{n\times n}(R)$ such that $A = SDT$, where S, T are invertible matrices and D is a diagonal matrix.

Proof. It suffices to show that A can be diagonalized with quasi-elementary row/column operations. Induct on n. The $n = 1$ base case is clear. Suppose $n > 1$ and $A \neq 0$.

By swapping rows and columns, suppose $a_{1,1} \neq 0$ (where $a_{i,j}$ entry of A in row i and column j).

Claim 1.1. If $a_{1,1} \mid a_{i,1}$ and $a_{1,1} \mid a_{1,i}$ for all i, then A is diagonalizable using quasi-elementary row/column operations.

Proof. Subtract the appropriate multiple row 1 (resp. col 1) from all subsequent rows (resp. cols) to make $a_{1,i} = a_{i,1} = 0$ for all $i > 1$. After this, our matrix has the form

$$\left[\begin{array}{c|ccc} a_{1,1} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right]$$

We can then apply induction to $A' \in \mathrm{Mat}_{n-1\times n-1}(R)$. ■

If $a_{1,1} \neq 0$, then using quasi-elementary row/column operations we can diagonalize A.

Since R is a PID, it is a unique factorization domain (UFD). So if $r \in R - \{0\}$, then

$$r = up_1^{e_1} \cdots p_n^{e_n},$$

where u invertible and p_i prime. Define $\delta(r) = e_1 + \cdots + e_n$. Induct on $\delta(a_{1,1})$. If $\delta(a_{1,1}) = 0$, then $a_{1,1}$ is invertible, so $a_{1,1} \mid a_{i,1}$ and $a_{1,1} \mid a_{1,i}$. By the previous lemma, we are done.

If $a_{1,1} \mid a_{i,1}$ and $a_{1,1} \mid a_{1,i}$ for all $i > 1$, we are done by the last lemma. For concreteness, suppose that $a_{1,1} \nmid a_{2,1}$. Let $(a_{1,1}, a_{2,1}) = (e)$. This implies $\delta(e) < \delta(a_{1,1})$. There are elements $a, b \in R$ s.t. $aa_{1,1} + ba_{1,2} = e$, and so a, b are coprime, i.e. $(a, b) = (1)$. There are elements $c, d \in R$ s.t. $ad - bc = 1$ by the definition of GCD. Let v_1 and v_2 be the first and second row of the matrix respectively. Use q.e. operations

$$(v_1, \ldots, v_n) \to (av_1 + bv_2, cv_1 + dv_2, v_3, \ldots, v_n).$$

So after this operation, our matrix has e in the 1st row and 1st column. But $\delta(e) < \delta(a_{1,1})$, so the new matrix can be diagonalized by q.e. row/column operations by induction. □

October 5, 2023 We proved the following in the worksheet in class yesterday:

Theorem 1.55 (Smith normal form)
We can write $A \in \mathrm{Mat}_{n\times n}(R)$ as $A = SDT$, where

$$D = \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{bmatrix},$$

and $d_i \mid d_{i+1}$ for all i.

This is called the **Smith normal form (SNF)**. The set $(d_1, \dots, d_n)$ are called the **invariant factors**. We will show that A uniquely determines its invariant factors up to multiplying each by an invertible element.

We introduce *multi-index notation* to make writing elements in exterior products easier. Let $(e_1, \dots, e_n)$ be a basis for $M \cong R^n$. Let $I = 1 \le i_1 < \cdots < e_k \le n$. Then $e_I \coloneqq e_{i_1} \wedge \cdots \wedge e_{i_k}$.

1.6.6. Minors

Lemma 1.56
For any matrix $A \in \mathrm{Mat}_{n\times n}(R)$, $\det A = \det A^T$.

Proof. By Theorem 1.55, we can write $A = S_1 \cdots S_n$, where S_i is either q.e. or diagonal. For q.e. and diagonal matrices the claim holds. Since

$$\det A = \det S_1 \cdots \det S_n = \det S_n^T \cdots \det S_1^T = \det(S_n^T \cdots S_1^T) = \det A^T. \qquad \square$$

Definition 1.26
Let $A \in \mathrm{Mat}_{n\times n}(R)$. Let $I, J \subseteq \{1, \dots, n\}$ with $|I| = |J| = k$. The **minor** $A_{I,J}$ is the determinant of the submatrix of A using only columns with indices in I and rows with indices in J.

Lemma 1.57
Let $A \in \mathrm{Mat}_{n\times n}(R)$ and $M \cong R^n$. Let $I \subseteq \{1, \dots, n\}$ with $|I| = k$. Then

$$\left(\bigwedge^k A\right)(e_I) = \sum_{\substack{J \subseteq \{1,\dots,n\} \\ |J| = k}} A_{I,J} \cdot e_J.$$

Proof (sketch). Choose $I = \{1, \dots, k\}$ for example. Let

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{bmatrix}.$$

We will need to show

$$\left(\bigwedge^k A\right)(e_1 \wedge \cdots \wedge e_k) = (a_{1,1}e_1 + c \ldots a_{n,1}e_n) \wedge \cdots \wedge (a_{1,k}e_1 + \cdots + a_{n,k}e_n)$$
$$= (A_{I,I})e_1 \wedge \cdots \wedge e_k + \text{other terms.}$$ □

Definition 1.27

The kth fitting ideal $I_k(A)$ of a matrix $A \in \mathrm{Mat}_{n\times n}(R)$, is the ideal generated by $A_{I,J}$ for all $I, J \subseteq \{1, \ldots, n\}$ such that $|I| = |J| = k$.

Example 1.58 –

1. For $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$,
   - $I_1(A) = (1, 2, 3, 4) = (1) = \mathbb{Z}$
   - $I_2(A) = (\det A) = (-2) = 2\mathbb{Z}$.
2. For $A = \mathrm{diag}(1, 2, 4)$ (i.e. a diagonal matrix with entries 1, 2, 4),
   - $I_1(A) = \mathbb{Z}$
   - $I_2(A) = (2, 8, 4) = (2)$
   - $I_3(A) = (8)$

These to not show up in linear algebra because there are no interesting ideals in a field k.

Lemma 1.59

If S is invertible and $A \in \mathrm{Mat}_{n\times n}(R)$, and k is a positive integer, then

$$I_k(SA) = I_k(A) = I_k(AS).$$

Proof. Since any invertible matrix is a product of q.e. matrices, we can assume without loss of generality, that S is q.e. In particular, S^T is q.e. too. It suffices to show that if S is q.e., then $I_k(SA) \subseteq I_k(A)$.

If this holds, then $I_k(A) = I_k(S^{-1}SA) \subseteq I_k(SA) \subseteq I_k(A)$, i.e. these ideals are the same. Moreover, the $k \times k$ submatrices of A and A^T have the same determinant, so $I_k(A^T) = I_k(A)$. Thus, $I_k(AS) = I_k(S^T A^T) = I_k(A^T) = I_k(A)$. So all we have to do is prove the containment in the first part.

Let $I \subseteq \{1, \ldots, n\}$ such that $|I| = k$. By applying the previous lemma twice,

$$\sum_{\substack{J\subseteq\{1,\ldots,n\} \\ |J|=k}} (SA)_{I,J} \cdot e_J = \left(\bigwedge^k SA\right)(e_I) = \left(\bigwedge^k S\right)\left(\bigwedge^k A\right)(e_I)$$
$$= \left(\bigwedge^k S\right) \sum_{\substack{J\subseteq\{1,\ldots,n\} \\ |J|=k}} A_{I,J}e_J$$
$$= \sum_{\substack{J,L\subseteq\{1,\ldots,n\} \\ |L|=|J|=k}} A_{I,J}S_{I,L}e_L.$$

Hence,

$$(SA)_{I,J} = \sum_{\substack{J,L\subseteq\{1,\dots,n\}\\ |J|=|L|=k}} \overbrace{A_{I,J}}^{\in I_k(A)} \overbrace{S_{I,L}}^{\in R} \in I_k(A). \qquad \square$$

Theorem 1.60 (Unqiueness of Smith normal form)
The invariant factors $d_i \mid d_{i+1}$ from Theorem 1.55 are unique for all i up to multiplication by an invertible element.

Proof. We need to show that A uniquely determines d_i. By the previous lemma, if $A = SDT$, then for all k, $I_k(A) = I_k(D)$. Then

$$I_1(D) = (d_1), \quad I_2(D) = (d_1d_2), \quad I_3(D) = (d_1d_2d_3), \quad \dots$$

So given A, let $e_k \in R$ such that $I_k(A) = (e_k)$. Then $e_{k-1} \mid e_k$ for all k and let d_k be the element such that $e_k = d_k e_{k-1}$. $\square$

1.7. Classification of modules over a PID

Theorem 1.61
Let R be a commutative ring. Every submodule of a finitely generated free R-module is free if and only if R is a PID.

Proof. ($\implies$) Every submodule of R is free, so if $0 \neq x \in R$, then $R \cdot x$ is a free submodule. So $r \cdot x \neq 0$ if $r \neq 0$ since this would be a nontrivial linear relation. So R has no zero divisors.

Since R is an integral domain, we show on the homework that any free submodule has rank ≤ 1. So for $I \subseteq R$, I is free by assumption, and $I \cong R$. Hence, it is principal.

($\impliedby$) We want to show that every submodule of R^n is free. We induct on n.

For the base case $n = 1$: $R^1 = R$, this follows from the definition of PID.

For the inductive step, let $M \subseteq R^n$ be a submodule. Let

$$\begin{aligned} \pi\colon R^n &\to R^{n-1} \\ \colon (x_1, \dots, x_n) &\mapsto (x_2, \dots, x_n). \end{aligned}$$

So $\pi(M) \subseteq R^{n-1}$. So $\pi(M)$ has a basis $\overline{e_1} \dots, \overline{e_m}$. Let $e_1, \dots, e_m$ be elements of M so that $\pi(e_i) = \overline{e_i}$. Note that $\ker \pi = R \oplus 0 \cdots \oplus 0$. So $\ker \pi \cap M \subseteq R \oplus 0 \oplus \cdots \oplus 0$. If $\ker \pi \cap M = \{0\}$, then $\pi\colon M \to \pi(M)$ is an isomorphism. By the induction hypothesis, this shows M is free. Otherwise, $\ker \pi \cap M$ is generated by a nonzero element e_{m+1}. We claim that this element can be added to form a basis for M.

Claim 1.2. $M = \operatorname{span}(e_1, \dots, e_{m+1})$.

Proof. Let $m \in M$. Let $\pi(m) = \sum_{i=1}^{m} r_i \overline{e_i}$ for $r_i \in R$. Then

$$m - r_1 e_1 - \cdots - r_m e_m \in \ker \pi \cap M.$$

So for some $r_{m+1 \in R}$,

$$m - r_1 e_1 - \cdots - r_m e_m = r_{m+1} e_{m+1}.$$ ■

Claim 1.3. $(e_1, \ldots, e_{m+1})$ are linearly independent.

Proof. Suppose $r_1 e_1 + \cdots + r_{m+1} e_{m+1} = 0$ for some $r_1, \ldots, r_{m+1} \in R$. Then

$$\pi(r_1 e_1 + \cdots + r_{m+1} e_{m+1}) = r_1 \overline{e_1} + \cdots + r_m \overline{e_m}.$$

Since $(\overline{e_1}, \ldots, \overline{e_m})$ are linearly independent, $r_i = 1$ for $1 \leq i \leq m$. So $r_{m+1} \cdot e_{m+1} = 0$. But $e_{m+1} = (r, 0, \ldots, 0)$. Since R is a PID, $r_{m+1} e_{m+1} = 0$ if and only if $r_{m+1} r = 0$, so $r_{m+1} = 0$. ■

□

October 10, 2023

Our goal is to classify all finitely generated modules over a PID R. Suppose M is a finitely generated R-module with generating set $S \coloneqq \{v_1, \ldots, v_n\}$. Hence, we have a map

$$\begin{aligned} \phi_S \colon R^n &\to M \\ : (r_1, \ldots, r_n) &\mapsto r_1 v_1 + \cdots + r_n v_n. \end{aligned}$$

This is a module homomorphism, so $\ker \phi_S$ is a submodule, hence, by Theorem 1.61, a free module of rank $k \leq n$.

Lemma 1.62
The invariant factors of S do not depend on the choice of a basis for $\ker \phi_S$.

Proof. Suppose that $\{w_1, \ldots, w_k\}$ and $\{w_1', \ldots, w_k'\}$ are two bases for $\ker \phi_S$. Equivalently, there are isomorphisms $\psi \colon R^k \to \ker \phi_S$ and $\psi' \colon R^k \to \ker \phi_S$ where $w_i = \psi(e_i)$ and $w_i' = \psi'(e_i)$. Hence,

$$\psi^{-1} \circ \psi' \colon R^k \to R^k$$

is an invertible linear map with matrix representation T. If ψ and ψ' are represented by the matrices A and A' respectively,

$$A' = AT.$$

The invariant factors are determined by the fitting ideals. Since T is invertible, by Lemma 1.59, $I_k(A') = I_k(AT) = I_k(A)$ for all k. □

Lemma 1.63 (Fitting's lemma)
Suppose $S = \{v_1, \ldots, v_n\}$ is a generating set of M. Let $S' = S \cup \{v_{n+1}\}$, where $v_{n+1} \in M$. Then the invariant factors of S and S' are the same. Moreover, the invariant factors of M are independent of S.

Proof. Let A be a matrix whose rows form a basis for $\ker \phi_S$. Write

$$v_{n+1} = \sum_{i=1}^{n} r_i v_i, \quad \mathbf{r} \coloneqq (r_1, \dots, r_n).$$

A basis for $\phi_{S'}$ can be written as the rows of the matrix

$$A' \coloneqq \left[\begin{array}{c|c} A & \mathbf{0} \\ \hline \mathbf{r} & 1 \end{array}\right].$$

We can perform q.e. column operations to turn this into $\begin{bmatrix} A & 0 \\ 0 & 1 \end{bmatrix}$. So there is an invertible matrix T' so that $A'T' = \begin{bmatrix} A & 0 \\ 0 & 1 \end{bmatrix}$. By Theorem 1.55, there are invertible matrices P and T so that

$$PA'T'T = \begin{bmatrix} d_1 & & & \\ & \ddots & & \\ & & d_n & \\ & & & 1 \end{bmatrix},$$

where $d_1, \dots, d_n$ are the invariant factors of A.

For the second claim, we suppose $\{v_1, \dots, v_n\}$ and $\{v'_1, \dots, v'_m\}$ are two generating sets. Note that invariant factors of $\{v_1, \dots, v_n\}$ and $\{v_1, \dots, v_n, v'_1\}$ are the same. Repeating this procedure, $\{v_1, \dots, v_n\}$ and $\{v_1, \dots, v_n, v'_1, \dots, v'_n\}$ have the same invariant factors. We can do this procedure in the opposite direction to get $\{v'_1, \dots, v'_n\}$ and $\{v_1, \dots, v_n, v'_1, \dots, v'_n\}$ have the same invariant factors. Hence, $\{v_1, \dots, v_n\}$ and $\{v'_1, \dots, v'_n\}$ have the same invariant factors. □

Theorem 1.64 (Classification of finitely generated modules over PIDs)
If M is a finitely generated R-module, where R is a PID, then there is a unique list of non-invertible elements $d_1 \mid d_2 \mid \cdots \mid d_n$ so that

$$M \cong \bigoplus_i R/(d_i).$$

Proof. Let $(d_1, \dots, d_n)$ be the invariant factors of the module M (this is well-defined because of the previous two lemmas). Let B be any generating set of size m for M. Let

$$A \colon R^k \to R^m$$

be a linear injection whose image is $\ker \phi_B$. There are invertible matrices S and T such that

$$A = SDT,$$

where

$$D = \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & d_1 & & \\ & & & & \ddots & \\ & & & & & d_n \end{bmatrix}$$

Let K be the row span of D. Note that

$$S^{-1} \colon R^m \to R^m,$$

which sends $\ker \phi_B$ to K. Therefore

$$M \cong R^m / \ker \phi_B \cong R^m / K \cong \bigoplus_i R/(d_i). \qquad \square$$

Example 1.65 (Classification of finitely generated abelian groups) – For every finitely generated abelian group A, there is $r \in \mathbb{Z}$ called the *rank* and integers $2 \le d_1 \mid \cdots \mid d_n$ that are nonzero, the *invariant factors*, so that

$$A \cong \mathbb{Z}^r \bigoplus_i \mathbb{Z}/d_i\mathbb{Z}.$$

1.7.1. Applications to linear algebra

October 12, 2023

Letting x act on $\mathbb{C}^n$ makes it a $\mathbb{C}[x]$-module. Let the matrix representation of x be $M \in \mathrm{Mat}_{n\times n}(\mathbb{C})$. Also, if $A_1, A_2 \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ make the $\mathbb{C}$-vector spaces V_1 and V_2 into $\mathbb{C}[x]$-modules, then $V_1 \cong V_2$ if and only if A_1 is similar to A_2, i.e. the matrices are the same up to change of basis.

Let A_i be $n_i \times n_i$ matrices with complex entries and let V_i be the associated $\mathbb{C}[x]$-module for $1 \le i \le n$. Moreover, let $A \in M_{n\times n}(\mathbb{C})$ and let V be its associated $\mathbb{C}[x]$-module. Then if there is a module isomorphism $V \cong V_1 \oplus \cdots \oplus V_n$, then there exists $B \in \mathrm{GL}_n(\mathbb{C})$ such that

$$BAB^{-1} = \begin{bmatrix} \boxed{A_1} & & \\ & \ddots & \\ & & \boxed{A_n} \end{bmatrix}.$$

1.7.2. Elementary divisor form

Another way to decompose modules is with the Chinese remainder theorem for rings.

Theorem 1.66 (Chinese remainder theorem)
Let R be a unique factorization domain. Let $d \in R$ so that $d = up_1^{e_1} \cdots p_n^{e_n}$ where p_i are primes such that $p_i \neq p_j$ if $i \neq j$ and u is invertible. Then $R/(d) \cong \bigoplus_{i=1}^n R/(p_i^{e_i})$.

Hence, we can first decompose M into its invariant factors $M \cong \bigoplus_i R/(d_i)$, and then further decompose each $R/(d_i)$ into the form given by the Chinese remainder theorem. Combining these, we may write $M \cong \bigoplus_j R/(p_j^{e_j})$ for some primes p_j and power e_j. The list (with multiplicity) of $p_j^{e_j}$ is called the elementary divisors.

Example 1.67 (Algorithm to go from invariant factor form to elementary divisor form and vice-versa) – Let $G = \mathbb{Z}/2 \oplus \mathbb{Z}/6 \oplus \mathbb{Z}/24$, written in invariant factor form. Then by factorizing,

$$G = \mathbb{Z}/2 \oplus (\mathbb{Z}/2 \oplus \mathbb{Z}/3) \oplus (\mathbb{Z}/8 \oplus \mathbb{Z}/3).$$

Hence, the elementary divisors are $(2, 2, 8, 3, 3)$.

Let G be written in elementary divisor form: $\mathbb{Z}/2 \oplus \mathbb{Z}/4 \oplus \mathbb{Z}/8 \oplus \mathbb{Z}/5 \oplus \mathbb{Z}/9$. Then by writing

$$\begin{array}{ccc} 2 & 2^2 & 2^3 \\ 1 & 1 & 5^1 \\ 1 & 1 & 9^1 \end{array}$$

and multiplying the columns, we can turn it into elementary divisor form:

$$G = \mathbb{Z}/2 \oplus \mathbb{Z}/4 \oplus \mathbb{Z}/360.$$

We have a correspondence from invariant factors to elementary divisors by the procedures in the previous example.

1.7.3. Rational canonical form

The invariant factor and elementary divisor decomposition of modules works just as well for $\mathbb{C}[x]$-modules, which we explore in this section. First we define the natural way to represent multiplication by x in a $\mathbb{C}[x]$ module quotiented by a polynomial.

Definition 1.28

Let $p(x) = a_n x^n + \cdots + a_1 x + a_0$ where $a_n \neq 0$ and consider $\mathbb{C}[x]/(p(x))$. Then we have an (ordered) basis $(1, x, \ldots, x^{n-1})$. The matrix

$$A_p := \begin{bmatrix} 0 & 0 & \cdots & \cdots & \cdots & -a_0/a_n \\ 1 & 0 & \cdots & \cdots & \cdots & -a_1/a_n \\ 0 & 1 & \cdots & \cdots & \cdots & -a_2/a_n \\ 0 & 0 & \ddots & & & \vdots \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & \cdots & 1 & -a_{n-1}/a_n \end{bmatrix},$$

called the companion matrix, represents multiplication in $\mathbb{C}[x]/(p(x))$ by x.

Suppose $A \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ and let the indeterminate x act on the vector space $V \cong \mathbb{C}^n$ by multiplication by A, thereby turning it into a $\mathbb{C}[x]$-module. Then there are polynomials (the invariant factors) $d_1(x) \mid \cdots \mid d_n(x)$ such that

$$V \cong \mathbb{C}[x]/(d_1) \oplus \cdots \oplus \mathbb{C}[x]/(d_n(x)).$$

Hence, there is $B \in \mathrm{GL}_n(\mathbb{C})$ such that

$$BAB^{-1} = \begin{bmatrix} \boxed{A_{d_1}} & & \\ & \ddots & \\ & & \boxed{A_{d_n}} \end{bmatrix}.$$

Since invariant factors are unique, this matrix, called the *invariant factor* rational canonical form is unique. This generalizes to a field k. Two matrices are similar if and only if they have the same invariant factor rational canonical form.

Moreover, in a $k[x]$-module, there is a (unique) collection of primes $p_j(x) \in k[x]$ and $e_j \in \mathbb{N} \cup \{0\}$ so that

$$V \cong \bigoplus_j k[x]/(p_j^{e_j}).$$

There are the elementary divisors so that there exists $C \in \mathrm{GL}_n(k)$ such that

$$CAC^{-1} = \begin{bmatrix} A_{p_1^{e_1}} & & \\ & \ddots & \\ & & A_{p_n^{e_n}} \end{bmatrix}.$$

This is the *elementary divisor* rational canonical form. When people refer to rational canonical form, they are usually referring to the invariant factor rational canonical form, and many of the following results are related to the invariant factors.

1.7.4. Characteristic and minimal polynomial

Let x act on $V \cong k^n$ by $A \in \mathrm{Mat}_{n\times n}(k)$, turning it into a $k[x]$-module.

Definition 1.29

Let $\chi_A(x) \coloneqq \det(xI - A)$ be the characteristic polynomial.

Example 1.68 – Let $A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$.

$$\chi_A = \det\left(\begin{bmatrix} x & \\ & x \end{bmatrix} - A\right) = (x-2)(x-1) - 1.$$

Lemma 1.69

$\chi_A(x) = d_1(x) \cdots d_n(x)$.

Proof. We need the following claims:

Claim 1.4. $\chi_{BAB^{-1}} = \chi_A$ for any $B \in \mathrm{GL}_n(k)$.

Proof.

$$\begin{aligned} \chi_{BAB^{-1}} &= \det(xI - BAB^{-1}) \\ &= \det(B(xI)B^{-1} - BAB^{-1}) \\ &= \det(B(xI - A)B^{-1}) \\ &= \det(B)\det(xI - A)\det(B^{-1}) \\ &= \chi_A. \end{aligned}$$

■

We bring A into rational canonical form by conjugating it with some matrix in $\mathrm{GL}_n(k)$:

$$A = BAB^{-1} = \begin{bmatrix} A_1 & & \\ & \ddots & \\ & & A_n \end{bmatrix}.$$

Claim 1.5. $\chi_A = \chi_{A_1} \cdots \chi_{A_k}$.

Proof.

$$\begin{aligned}
\chi_A &= \det(xI - A) \\
&= \det(xI - BAB^{-1}) \\
&= \det\begin{bmatrix} \boxed{xI - A_1} & & \\ & \ddots & \\ & & \boxed{xI - A_k} \end{bmatrix} \\
&= \det(xI - A_1) \cdots \det(xI - A_k) \\
&= \chi_{A_1} \cdots \chi_{A_k}.
\end{aligned}$$

■

By letting

$$A = \begin{bmatrix} 0 & 0 & \cdots & -a_0 \\ 1 & 0 & \cdots & -a_1 \\ & \ddots & \ddots & \vdots \\ & & 1 & -a_{n-1} \end{bmatrix}$$

I claim that $\chi_A(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. We prove this by inducting on n. The base case is trivial.

$$\begin{aligned}
\chi_A &= \det\left(\begin{bmatrix} x & & \\ & \ddots & \\ & & x \end{bmatrix} - A\right) \\
&= \det\left(\begin{bmatrix} x & 0 & \cdots & a_0 \\ -1 & x & \cdots & a_1 \\ & \ddots & \ddots & \vdots \\ & & -1 & x + a_{n-1} \end{bmatrix}\right) \\
&= x \det\left(\begin{bmatrix} x & 0 & \cdots & a_1 \\ -1 & x & \cdots & a_2 \\ & \ddots & \ddots & \vdots \\ & & -1 & x + a_{n-1} \end{bmatrix}\right) + (-1)^{n-1} a_0 \det\left(\begin{bmatrix} -1 & x & & \\ & \ddots & \ddots & \\ & & \ddots & x \\ & & & -1 \end{bmatrix}\right) \\
&= x(x^{n-1} a_{n-1} x^{n-2} + \cdots + a_1) + (-1)^{n-1} a_0 (-1)^{n-1} \\
&= x^n + a_{n-1}x^{n-1} + \cdots + a_0.
\end{aligned}$$

□

Definition 1.30

The **minimal polynomial** $m_A(x)$ is the lowest degree monic polynomial so that $m_A(A) = 0$. Recall if $p(x) = x^n + \cdots + a_0 x^0$ then $p(A) \coloneqq A^n + \cdots + a_0 I$.

October 17, 2023

Let $\mathrm{ev}_A \colon k[x] \to \mathrm{Mat}_{n\times n}(k) \colon p(x) \mapsto p(A)$ be the *evaluation map*, a ring homomorphism. Since $k[x]$ is a principal ideal domain, $\ker(\mathrm{ev}_A) = (m_A)$. Hence, any polynomial that evaluates on A to 0 is a multiple of m_A.

Example 1.70 (Comparing characteristic is not necessarily minimal polynomial) – If $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, then $\chi_A = (x-1)^2 = m_A$.

On the other hand, if $A = \operatorname{diag}(1,1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, then $\chi_A = (x-1)^2$, but $m_A = x - 1$.

Theorem 1.71 (The minimal polynomial is the last invariant factor)
$m_A = d_m$, so $d_m = m_A \mid d_1 \cdot \cdots \cdot d_m = \chi_A$, so $\chi_A(A) = 0$. Moreover, any root of χ_A is a root of m_A since $d_i \mid d_m$ for all i.

Proof. For the first part we prove the following claim:

Claim 1.6. If $B \in \mathrm{GL}_n(k)$, then $m_{BAB^{-1}} \mid m_A$.

Proof. Since

$$m_A = m_{B^{-1}(BAB^{-1})B} \mid m_{BAB^{-1}} \mid m_A,$$

it is sufficient to show that $m_A = m_{BAB^{-1}}$.

It suffices then to show that $m_A(BAB^{-1}) = 0$. Let $m_A = \sum_i a_i x^i$.

$$\begin{aligned} m_A(BAB^{-1}) &= \sum_i a_i (BAB^{-1})^i \\ &= \sum_i a_i B A^i B^{-1} \\ &= B \left(\sum_i a_i A^i \right) B^{-1} \\ &= B m_A(A) B^{-1} = 0. \end{aligned}$$

■

Suppose that A is a block diagonal matrix with blocks $A_1, \ldots, A_m$. Given $p(x) \in k[x]$,

$$p(A) = \begin{bmatrix} \boxed{p(A_1)} & & \\ & \ddots & \\ & & \boxed{p(A_m)} \end{bmatrix}.$$

So $m_A = \operatorname{lcm}(m_{A_1}, \ldots, m_{A_m})$.

By rational canonical form, there exists $B \in \mathrm{GL}_n(k)$ such that

$$BAB^{-1} = \begin{bmatrix} \boxed{A_{d_1}} & & \\ & \ddots & \\ & & \boxed{A_{d_m}} \end{bmatrix}.$$

So $m_A = \operatorname{lcm}(m_{A_{d_1}}, \ldots, m_{A_{d_m}})$. It suffices to show that $m_{A_{d_i}} = d_i$. A_{d_i} is given by the action of x by left multiplication on $k[x]/(d_i)$. Hence, for $p \in k[x]$, $p(A_{d_i})$ is given by left multiplication by $p(x)$ on $k[x]/(d_i)$. But $p(x) = 0$ in $k[x]/(d_i) \iff d_i \mid p$. Then $d_i = m_{A_{d_i}}$. □

Example 1.72 (HW6 Problem 2) – Find all similarity classes of matrices in $\mathrm{Mat}_{6\times 6}(\mathbb{C})$ such that their minimal polynomial is $m_A = (x+2)^2(x-1) = x^3+3x^2-4$.

m_A is the last invariant factor. We need to come up with all lists of invariant factors whose product is a degree 6 polynomial (since the matrix is 6×6).

1. $\{(x+2),(x+2),(x+2),(x+2)^2(x-1)\} = \{(x+2),(x+2),(x+2),x^3+3x^2-4\}$:

$$\begin{bmatrix} -2 & & & & & \\ & -2 & & & & \\ & & -2 & & & \\ & & & 0 & 0 & -4 \\ & & & 1 & 0 & 0 \\ & & & 0 & 1 & 3 \end{bmatrix}$$

2. $\{(x-1),(x-1),(x-1),(x+2)^2(x-1)\} = \{(x-1),(x-1),(x-1),x^3+3x^2-4\}$:

$$\begin{bmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 0 & 0 & -4 \\ & & & 1 & 0 & 0 \\ & & & 0 & 1 & 3 \end{bmatrix}$$

3. $\{(x+2),(x+2)^2,(x+2)^2(x-1)\} = \{(x+2),x^2+4x+4,x^3+3x^2-4\}$:

$$\begin{bmatrix} -2 & & & & & \\ & 0 & -4 & & & \\ & 1 & -4 & & & \\ & & & 0 & 0 & -4 \\ & & & 1 & 0 & 0 \\ & & & 0 & 1 & 3 \end{bmatrix}$$

4. $\{(x+2),(x+2)(x-1),(x+2)^2(x-1)\} = \{(x+2),x^2+x-2,x^3+3x^2-4\}$:

$$\begin{bmatrix} -2 & & & & & \\ & 0 & 2 & & & \\ & 1 & -1 & & & \\ & & & 0 & 0 & -4 \\ & & & 1 & 0 & 0 \\ & & & 0 & 1 & 3 \end{bmatrix}$$

5. $\{(x-1),(x-1)(x+2),(x+2)^2(x-1)\} = \{x-1,x^2+x-2,x^3+3x^2-4\}$:

$$\begin{bmatrix} 1 & & & & & \\ & 0 & 2 & & & \\ & 1 & -1 & & & \\ & & & 0 & 0 & -4 \\ & & & 1 & 0 & 0 \\ & & & 0 & 1 & 3 \end{bmatrix}$$

6. $\{(x+2)^2(x-1),(x+2)^2(x-1)\} = \{x^3+3x^2-4,x^3+3x^2-4\}$:

$$\begin{bmatrix} 0 & 0 & -4 & & & \\ 1 & 0 & 0 & & & \\ 0 & 1 & 3 & & & \\ & & & 0 & 0 & -4 \\ & & & 1 & 0 & 0 \\ & & & 0 & 1 & 3 \end{bmatrix}$$

This shows the six similarity classes.

Corollary 1.73
Let k be a subfield of the field L. Let $A \in \mathrm{Mat}_{n\times n}(k)$ and A_k (resp. A_L) be the action of A on k^n (resp. L^n), then $m_{A_k} = m_{A_L}$.

Proof. There exists $B \in \mathrm{GL}_n(k)$ such that

$$BAB^{-1} = \begin{bmatrix} \boxed{A_{d_1}} & & \\ & \ddots & \\ & & \boxed{A_{d_m}} \end{bmatrix}.$$

This expression still makes sense in $\mathrm{Mat}_{n\times n}(L)$. The invariant factors are *unique*, so the invariant factors for $A_L : L \to L$ are still $d_1 \mid \cdots \mid d_m$, but $d_m = m_{A_L} = m_{A_k}$. □

Example 1.74 – We know $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ as subfields. Let

$$A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}.$$

Notice that A is well-defined with entries in $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, so we may define maps $A_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{Q}$, $A_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}$, $A_{\mathbb{C}} : \mathbb{C} \to \mathbb{C}$ by multiplication by this matrix. The minimal polynomials $m_{A_{\mathbb{Q}}}$, $m_{A_{\mathbb{R}}}$, $m_{A_{\mathbb{Q}}}$ are all equal.

1.8. Jordan canonical form

Lemma 1.75 (Jordan blocks)
Let $\lambda \in k$. Let $p(x) = (x-\lambda)^e$ for some $e > 0$. Then there exists $B \in \mathrm{GL}_e(k)$ such that

$$BA_pB^{-1} = \begin{bmatrix} \lambda & & & \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & \lambda \end{bmatrix}.$$

These are called **Jordan blocks**.

Proof. Let $C \coloneqq A_p - \lambda I$, so $m_{A_p} = (x-\lambda)^e$, so $m_C = x^e$. So there exists $B \in \mathrm{GL}_e(k)$ such that

$$BCB^{-1} = A_{x^e} = \begin{bmatrix} 0 & & & 0 \\ 1 & \ddots & & \vdots \\ & \ddots & \ddots & \vdots \\ & & 1 & 0 \end{bmatrix}.$$

Hence

$$BA_pB^{-1} = B(C+\lambda I)B^{-1} = BCB^{-1} + \lambda I = \begin{bmatrix} 0 & & & 0 \\ 1 & \ddots & & \vdots \\ & \ddots & \ddots & \vdots \\ & & 1 & 0 \end{bmatrix} + \begin{bmatrix} \lambda & & & 0 \\ & \ddots & & \vdots \\ & & \ddots & \vdots \\ & & & \lambda \end{bmatrix}. \quad \square$$

Definition 1.31

A **Jordan matrix** is a block diagonal matrix with Jordan blocks on the diagonal.

Theorem 1.76 (Jordan canonical form)

Suppose $\chi_A(x) = (x-\lambda_1)\cdots(x-\lambda_n)$, where $\lambda_i \in k$. Then there exists B such that BAB^{-1} is a Jordan matrix. The Jordan blocks are unique up to permutation.

Proof. Note that $d_1 \cdots d_m = \chi_A = (x-\lambda_1)\cdots(x-\lambda_n)$. The elementary divisors of $V \cong k^n$ w/ the associated $k[x]$-module structure are $(x-\lambda_i)^{e_j}$. There is $B \in \mathrm{GL}_n(k)$ so that

$$BAB^{-1} = \begin{bmatrix} A_{(x-\lambda_1)^{e_1}} & & \\ & A_{(x-\lambda_2)^{e_2}} & \\ & & \ddots \end{bmatrix}.$$

By the lemma, each $A_{(x-\lambda_i)^{e_j}}$ is conjugate to a Jordan block. □

Remark 1.77. The Jordan canonical form is very useful, but it relies on the fact that all the roots of the characteristic polynomial belong to the field we work over. This always holds if $k = \mathbb{C}$. However, matrices such as the 2×2 rotation matrices rot_θ, $\theta \in (0, 2\pi) \setminus \{\pi\}$ cannot be conjugated to Jordan canonical form in $\mathrm{GL}_2(\mathbb{R})$, but can be in $\mathrm{GL}_2(\mathbb{C})$.

2. Fields

October 26, 2023

Recall that field is a commutative ring where $0 \neq 1$, and all nonzero elements have multiplicative inverses.

Definition 2.1

The **characteristic** of a field k, denoted $\operatorname{char}(k)$ is the smallest $n \in \mathbb{N}$ such that $n \cdot 1 = 0$. If no such n exists, we let $\operatorname{char}(k) = 0$.

Lemma 2.1

$\operatorname{char}(k)$ is either 0 or prime.

Proof. Suppose not. Let $\operatorname{char}(k) = ab$, where $a, b \in \mathbb{Z}_{>1}$. So $a, b \neq 0$. But $a \cdot b = a \cdot b \cdot 1 = 0$, a contradiction, since k has no zero divisors. □

Definition 2.2

The **prime subfield** of k is the smallest field in k containing 1.

From Lemma 2.1, the prime subfield is one of two fields:

$$\begin{cases} \mathbb{F}_p \coloneqq \mathbb{Z}/p\mathbb{Z} & \text{if } \operatorname{char}(k) = p > 0, \\ \mathbb{Q} & \text{if } \operatorname{char}(k) = 0. \end{cases}$$

Consider a subfield k of a field F. We may consider F as a k-vector space with elements of F as vectors and elements of k as scalars.

Lemma 2.2

Any finite field has prime power order.

Proof. A finite field k has characteristic $p > 0$ (if $p = 0$, then it would have a prime subfield $\mathbb{Q}$, hence infinite). So k is a $\mathbb{F}_p$-vector space. Moreover, since our field has finitely many elements, it is a finite-dimensional $\mathbb{F}_p$-vector space, and $k \cong \mathbb{F}_p^d$ for some $d \in \mathbb{N}$. □

Definition 2.3

If k is a subfield of L, then L is a k-vector space, called an **extension of k** of **degree** $[L : k] \coloneqq \dim_k(L)$.

Example 2.3 –

- $\mathbb{R} \subseteq \mathbb{C}$ is a subfield. Since $\mathbb{C} \cong \mathbb{R}^2$ as a vector space, $\mathbb{C}$ is an extension of $\mathbb{R}$ of degree $[\mathbb{C} : \mathbb{R}] = 2$.
- $\mathbb{Q} \subseteq \mathbb{R}$ is a subfield. $\mathbb{R}$ is an extension of $\mathbb{Q}$ of degree $[\mathbb{R} : \mathbb{Q}] = \infty$.
- $\mathbb{Q}$ is a subfield of $\mathbb{Q}(\sqrt{2}) \coloneqq \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ (called $\mathbb{Q}$ *adjoined* $\sqrt{2}$) of degree $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Lemma 2.4 (Degrees of extensions multiply)
Let $L_1 \subseteq L_2 \subseteq L_3$ be subfields. Then $[L_3 : L_1] = [L_3 : L_2][L_2 : L_1]$.

Proof. Let $[L_3 : L_2] = m$ and $[L_2 : L_1] = n$. Let $(v_1, \dots, v_n)$ be a basis of L_2 as an L_1-vector space, and $(w_1, \dots, w_m)$ be a basis of L_3 as an L_2-vector space.

Claim 2.1. $\mathcal{B} = (v_i w_j)_{ij}$ is a basis for L_3 as an L_1-vector space.

> **Proof.** Let $v \in L_3$. Then
>
> $$v = \sum_{i=1}^{m} \underbrace{a_i}_{\in L_2} w_i = \sum_{i=1}^{m} \left(\sum_{i=1}^{n} \underbrace{b_{ij}}_{\in L_1} v_j \right) w_i. \qquad \blacksquare$$

Suppose that $\sum_{i,j} a_{ij} v_i w_i = 0$. Then

$$\sum_{j=1}^{m} \underbrace{\left(\sum_{i=1}^{n} a_{ij} v_i \right)}_{\in L_2} w_j.$$

Since $w_1, \dots, w_m$ is a basis, it follows that $\sum_{i=1}^{n} a_{ij} v_i = 0$ for all j. Since $(v_1, \dots, v_n)$ is a basis, $a_{ij} = 0$ for all i and j. $\square$

2.1. Creating new fields

Suppose that $p(x) \in k[x]$ is prime. So the ideal $(p) \subseteq k[x]$ is prime, hence maximal. So $k[x]/(p)$ is a field. As a k-vector space, $L \coloneqq k[x]/(p)$ has a basis $\{1, x, \dots, x^{d-1}\}$, where $d = \deg p$. Therefore, $[k[x]/(p) : k] = \deg p$. Notice that $x \in L$, so $p(x) = 0$. The field L is formed by adjoining a root of p to k.

Example 2.5 (Constructing the complex numbers from the reals) – We want to add a number i satisfying $i^2 = -1$.

$$\mathbb{C} = \mathbb{R}[i]/(i^2 = -1) = \mathbb{R}[i]/(i^2 + 1),$$

where i is a variable in a polynomial ring here.
Similarly, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[x]/(x^2 - 2)$.

2.1.1. Finite fields

Definition 2.4
The **Euler ϕ function** is

$$\phi(n) \coloneqq \#\left\{m \in \{1, \dots, n-1\} \mid \gcd(m, n) = 1\right\}.$$

Equivalently, it is the number of $g \in \mathbb{Z}/n$ such that $\langle g \rangle = \mathbb{Z}/n$ (g generates $\mathbb{Z}/n$).

Lemma 2.6 (Combinatorial ϕ identity)
$\sum_{d|n} \phi(d) = n$.

Proof. By our second interpretation of the ϕ function, we note the subgroups of $\mathbb{Z}/n$ are $\mathbb{Z}/d$ for $d \mid n$. Each element of $\mathbb{Z}/n$ generates some subgroup. There are $\phi(d)$ elements that generate $\mathbb{Z}/d$. □

Lemma 2.7

Let H be a finite group of order n. For each $d \mid n$, suppose that $x^d = \mathrm{id}$ has at most d solutions. Then H is a cyclic group of order n.

Proof. If $x \in H$ has order d, then $\langle x \rangle$ is isomorphic to $\mathbb{Z}/d$, so there are exactly d solutions to $x^d = \mathrm{id}$ and all of them belong to $\langle x \rangle$. So there are exactly $\phi(d)$ elements of H of order d.

Suppose no element in H has order n. Then

$$n = |H| = \sum_{d \mid n} \#\{g \in H \mid \mathrm{ord}(g) = d\} \leq \sum_{\substack{d \mid n \\ d < n}} \phi(d) = n - \phi(n) < n.$$

This is a contradiction. □

Definition 2.5

Given a field k, $k^\times := k - \{0\}$ as a group under multiplication.

Proposition 2.8

If k is a finite field, then $k^\times$ is cyclic.

Proof. Any polynomial $p \in k[x]$ of degree d has at most d roots, so $x^d - 1 = 0$ has at most d solutions. □

Lemma 2.9

Let $k = \mathbb{F}_p$ where p is an odd prime. Then -1 has a square root $\iff 4 \mid p - 1$.

Proof. ($\implies$) Suppose $x^2 = -1$ for some $x \in \mathbb{F}_p$. Then $x^4 = 1$, so $4 = \mathrm{ord}(x)$ divides $|\mathbb{F}_p^\times| = p - 1$.

($\impliedby$) Let $\langle g \rangle = \mathbb{F}_p^\times$. Note -1 is the only element of order 2 in $\mathbb{F}_p^\times$. So $g^{\frac{p-1}{2}} = -1$. Hence, $\left(g^{\frac{p-1}{4}}\right)^2 = -1$. □

So $x^2 + 1$ is prime in $\mathbb{F}_p[x] \iff 4 \mid p - 3$ ($p = 3, 7, 11, \ldots$ work). So if $4 \mid p - 3$ then $\mathbb{F}_p[i]/(i^2 = -1)$ is a field.

2.2. Minimal polynomials

October 31, 2023

Definition 2.6

Let L be a field containing k. An element $\alpha \in L$ is called **algebraic (over k)** if there exists a monic polynomial $p \in k[x]$ such that $p(\alpha) = 0$. The smallest degree such polynomial is the **minimal polynomial**, m_α.

Example 2.10 (Examples of minimal polynomials) –

1. The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$,
2. The minimal polynomial of $\sqrt{2}$ over $\mathbb{R}$ is $x - \sqrt{2}$,
3. The minimal polynomial of $\zeta_3 = \exp\left(\frac{2\pi i}{3}\right)$ over $\mathbb{Q}$ is $x^2 + x + 1$ (by observing ζ_3 is a root of $x^3 - 1 = (x^2 + x + 1)(x - 1)$).

Lemma 2.11

Let α be algebraic. Let the *evaluation map* be the homomorphism $\mathrm{ev}_\alpha \colon k[x] \to L \colon p(x) \mapsto p(\alpha)$. Then $\ker \mathrm{ev}_\alpha = (m_\alpha)$.

Proof. We know $\ker(\mathrm{ev}_\alpha)$ is an ideal in a PID. Any nonzero ideal in $k[x]$ is generated by the smallest degree monic polynomial it contains. □

Lemma 2.12 (The minimal polynomial is irreducible)

$m_\alpha \in k[x]$ is irreducible (prime).

Proof. Suppose not, i.e. $m_\alpha(x) = f(x)g(x)$, where $f, g \in k[x]$ are monic polynomials such that $\deg f, \deg g < \deg m_\alpha$. We have

$$0 = m_\alpha(\alpha) = f(\alpha)g(\alpha),$$

so either $f(\alpha) = 0$ or $g(\alpha) = 0$, a contradiction, since we assumed that m_α had minimal degree. □

Definition 2.7

If $\alpha_1, \ldots, \alpha_n \in L$, then $k(\alpha_1, \ldots, \alpha_n)$ is the smallest subfield of L containing $\alpha_1, \ldots, \alpha_n$.

Lemma 2.13

$k(\alpha) = \mathrm{im}(\mathrm{ev}_\alpha) \cong k[x]/(m_\alpha)$.

Proof. $\mathrm{im}(\mathrm{ev}_\alpha) \coloneqq \{p(\alpha) \in L \mid p(x) \in k[x]\} \subseteq k(\alpha)$. Moreover, $\mathrm{im}(\mathrm{ev}_\alpha) \cong k[x]/\ker(\mathrm{ev}_\alpha) = k[x]/(m_\alpha)$. By the previous lemma, this is maximal. So $\mathrm{im}(\mathrm{ev}_\alpha)$ is a field. Thus $k(\alpha) \subseteq \mathrm{im}(\mathrm{ev}_\alpha)$. □

2.3. Splitting fields

Definition 2.8

Let $p(x) \in k[x]$. The **splitting field of** p is the smallest degree extension of k containing all roots of p.

Example 2.14 (Examples of splitting fields) –

1. Let $p(x) = x^2 - 2 \in \mathbb{Q}[x]$. The splitting field of p is $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$.
2. $\mathbb{R}$ contains both roots of $x^2 - 2$. It is *not* a splitting field of p because its degree over $\mathbb{Q}$ is larger than 2 (it is infinite).

Lemma 2.15

Let $p(x) \in k[x]$ such that $d = \deg p$. Then there exists a splitting field of p (over k) of degree $\leq d!$.

Proof. Induct on d. For the base case, $p(x) = x - \alpha$ for $\alpha \in k$. The splitting field is k. Suppose $d > 1$. We write $p(x) = q(x)r(x)$, $q, r \in k[x]$ and q is irreducible. Let $L = k[x]/(q(x))$. In this extension, there is now a root α of q. So $p(x) = (x - \alpha)h(x)$ in $L[x]$. By the induction hypothesis, there is a field F extending L with all the roots of h inside it, and $[F : L] \leq (d-1)!$ by assumption. Moreover, $[L : k] = \deg q \leq d$. Hence,

$$[F : k] = [F : L][L : k] \leq (d-1)!d = d!. \qquad \square$$

Example 2.16 – Suppose we want to find the degree of the splitting field of $x^3 - 2$ over $\mathbb{Q}$. The roots of $x^3 - 2$ are $\left\{\sqrt[3]{2}, \sqrt[3]{2} \cdot \zeta_3, \sqrt[3]{2} \cdot \zeta_3^2\right\}$, where $\zeta_3 = \exp\left(\frac{2\pi i}{3}\right)$. Let $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2} \cdot \zeta_3, \sqrt[3]{2} \cdot \zeta_3^2) \subseteq \mathbb{C}$. Note that

$$L \supseteq \mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(m_{\sqrt[3]{2}}) \cong \mathbb{Q}[x]/(x^3 - 2).$$

Hence,

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg(x^3 - 2) = 3.$$

Moreover,

$$L \supseteq \mathbb{Q}(\zeta_3) \cong \mathbb{Q}[x]/(m_{\zeta_3}) = \mathbb{Q}[x]/(x^2 + x + 1).$$

Hence,

$$[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = \deg(x^2 + x + 1) = 2.$$

Both of these degree divide $[L : \mathbb{Q}]$, so $[L : \mathbb{Q}] \geq 6$. By Lemma 2.15, $[L : \mathbb{Q}] \leq 3! = 6$. This means $[L : \mathbb{Q}] = 6$.

Definition 2.9

Let F_1 and F_2 be extensions of k. Then F_1 and F_2 are **isomorphic extensions** if there exists a field isomorphism $\tau \colon F_1 \to F_2$ such that $\tau(a) = a$ for all $a \in k$.

Given a field isomorphism $\sigma \colon F_1 \to F_2$, let $\sigma \colon F_1[x] \to F_2[x]$ be defined by $p(x) = \sum_{n \geq 0} a_n x^n$ is sent to $p^\sigma(x) = \sum_{n \geq 0} \sigma(a_n) x^n$.

Example 2.17 – Consider $\sigma \colon \mathbb{C} \to \mathbb{C} \colon z \mapsto \overline{z}$. If $p(x) = (1 + i) + (7i)x$, then $p^\sigma(x) = (1 - i) + (-7i)x$.

Lemma 2.18

Splitting fields are unique up to isomorphism of extensions.

We will prove this from a more general result:

Lemma 2.19

Given a field isomorphism $\sigma\colon k_1 \to k_2$ and a polynomial $p \in k_1[x]$, let L_1 is a splitting field of p and L_2 be a splitting field of p^σ, then there exists a field isomorphism $\tau\colon L_1 \to L_2$ such that $\tau(a) = \sigma(a)$ for all $a \in k_1 \subseteq L_1$.

$$\begin{array}{ccc} L_1 & \xrightarrow[\cong]{\tau} & L_2 \\ \uparrow & & \uparrow \\ k_1 & \xrightarrow[\cong]{\sigma} & k_2 \end{array}$$

Proof. Induct on $d := \deg p$. Base case: if $p(x) = x - \alpha$, then $p^\sigma(x) = x - \sigma(\alpha)$, $\sigma(\alpha) \in k_2$. It follows that $L_1 = k_1$ and $L_2 = k_2$, so we have $L_1 \cong L_2$ by σ.

Suppose that $d > 1$. Write $p(x) = q(x)r(x)$, where q is irreducible. Let α_1 be a root of q in L_1. Let α_2 be a root of q^σ in L_2.

Claim 2.2. $k_1(\alpha_1) \cong k_2(\alpha_2)$.

> **Proof.** $k_1(\alpha_1) \cong k_1[x]/(q_1(x))$, where the isomorphism is given by $f(x) \xrightarrow{\mathrm{ev}_{\alpha_1}} f(\alpha_1)$, and $k_2(\alpha_2) \cong k_2[x]/(q_2(x))$, where the isomorphism is given by $f(x) \xrightarrow{\mathrm{ev}_{\alpha_2}} f(\alpha_2)$. We have an isomorphism $k_1[x]/(q_1(x)) \xrightarrow{\sim} k_2[x]/(q_2(x))$ sending q_1 to q_1^σ. ■

So there exists a field isomorphism $\tau_1\colon k_1(\alpha_1) \to k_2(\alpha_2)$, whose restriction to k_1 is σ_1. By the induction hypothesis, since L_1 is a splitting field of a polynomial with coefficients in $k_1(\alpha_1)$, and L_2 is a splitting field of a polynomial with coefficients in $k_2(\alpha_2)$, we can find an isomorphism $\tau\colon L_1 \to L_2$, whose restriction to $k_1(\alpha_1)$ is τ_1. □

2.4. Separability

November 2, 2023

Definition 2.10

For a field k and $f \in k[x]$ with $\deg f > 0$, f is **separable** if f does not have roots in its splitting field that have multiplicity > 1.

In other words, we should be able to write $f(x) = a\prod_i (x - z_i)$ for $a \in k$, where z_i are all distinct.

We want a method to show that f is separable. Suppose L is a splitting field for f. Then $f(x) = a\prod_i (x - z_i)$. Consider the **formal derivative**:

$$\begin{aligned} D\colon k[x] &\to k[x], \\ : \sum_{i=1}^{n} a_i x^i &\mapsto \sum_{i=1}^{n} i a_i x^{i-1}. \end{aligned}$$

We may also write $D(f) = f'$. We can verify that it satisfies Leibniz's rule $D(fg) = fD(g) + D(f)g$. It follows that

$$D(f(x)) = a\sum_{i=1}^{n}\left(\prod_{j\neq i}(x - z_j)\right).$$

Lemma 2.20
f is separable $\iff \gcd(f, f') = 1$.

Proof. If we have a repeated root $z_j = z_{j'}$, then $(x - z_j) \mid D(f) \implies (x - z_j) \mid f$! So $\gcd(f, D(F))$ in $L[x]$ has degree > 0. Conversely, if $\gcd(f, D(f))$ has degree ≥ 1, then it has a root z_j, hence $(x - z_j) \mid a\sum_{i=1}^{n} \left(\prod_{j \neq i}(x - z_j)\right)$. So $(x - z_j) \mid \prod_{k \neq j}(x - z_k)$. Hence, there exists $k \neq j$ such that $z_k = z_j$. □

We do not need to specify that L is a splitting field because $\gcd(f, D(f))$ can be calculated by Euclid's algorithm, we know that $\gcd(f, D(f)) = 1$ in $k[x]$.

Example 2.21 (Discriminant) – If $\mathrm{char}(k) \neq 2$, then $f(x) = x^2 + ax + b \implies f'(x) = 2x + a$. $\gcd(x^2 + ax + b, 2x + a) = \gcd(b - \frac{a^2}{4}, x + \frac{a}{2})$.

$$\gcd(b - \frac{a^2}{4}, x + \frac{a}{2}) = \begin{cases} 1 & \text{if } b - \frac{a^2}{4} \neq 0, \\ x + \frac{a}{2} & \text{if } b - \frac{a^2}{4} = 0. \end{cases}$$

Example 2.22 – If $f(x) = (g(x))^2 h(x)$, $\deg g \geq 1$. Then f is not separable.

Example 2.23 – Let $k = \mathbb{F}_3(t)$, the field of rational function with coefficients in $\mathbb{F}_3$. Let $f(x) = x^3 - t \in k[x]$. $f'(x) = 3x^2 = 0$. Therefore, $\gcd(f, f') = f$. Hence, f is not separable, but also *irreducible*.

Theorem 2.24
If $f \in k[x]$ is irreducible and non-separable, then

1. $f' = 0$,
2. f can be written as $g(x^p)$, where $p = \mathrm{char}(k)$.

Proof (sketch). (1) Suppose $f' \neq 0$ for contradiction. $\gcd(f, f')$ is a factor of both and has degree $< \deg f$ and ≥ 1, which contradicts the fact that f is irreducible (alternatively, f irreducible $\implies \gcd(f, f') \neq 0 \implies f \mid f'$, so $f' = 0$).
(2) Look at

$$f(x) = \prod_{i=0}^{d} a_i x^i, \quad f'(x) = \sum_{i=1}^{d} i a_i x^{i-1}.$$ □

Lemma 2.25
If $\mathrm{char}(k) = 0$, then any irreducible polynomial is separable.

On the other hand, some fields with positive characteristic also have irreducible polynomial separable.

Theorem 2.26
If k is a finite field, then any irreducible polynomial over k is separable.

Lemma 2.27
There is a unique finite field of order p^n up to isomorphism.

Proof. If L is a finite field of order p^n, then $(L \setminus \{0\}, \times)$ is a group of order $p^n - 1$. By Lagrange's theorem, for any $x \in L \setminus \{0\}$, we have $x^{p^n-1} = 1$, so for any $x \in L$, $x^{p^n} - x = x(x^{p^n-1} - 1) = 0$. So all the roots are distinct and p^n roots are exactly the p^n elements in L. So L is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. We have uniqueness because splitting fields are unique.

Let p be a prime and $n \geq 1$ be an integer. Consider the splitting field L of $x^{p^n} - x$ over $\mathbb{F}_p$. Let $L' \subseteq L$ be the set of roots $x^{p^n} - x$ in L. Then $|L'| = p^n$ because $x^{p^n} - x$ is separable. Now we show that L' is a subfield, which implies $L = L'$. If $a^{p^n} - a = 0$, $b^{p^n} - b = 0$, then $(a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b$, $(ab)^{p^n} = a^{p^n} b^{p^n} = ab$, $(a^{-1})^{p^n} = \left(a^{p^n}\right)^{-1} = a^{-1}$, so L' is a subfield. □

We will let $\mathbb{F}_{p^n}$ denote the finite field of p^n elements. Let $k = \mathbb{F}_{p^n}$, $f \in k[x]$ be an irreducible polynomial over k. Let L be the splitting field of f. Then $L = \mathbb{F}_{p^m}$ for some $m \geq n$. For any $\alpha \in L$, $h(\alpha) = 0$, where $h(x) = x^{p^m} - x$. Let f be irreducible. Pick a root β of f in L. f is the minimal polynomial of β over k. $h(\beta) = 0$, so $f \mid h$. h is separable, so f is separable.

Corollary 2.28 ($x^{p^n} - x$ contains all irreducible polynomials in $\mathbb{F}_p$)
Let p be a prime and fix an integer $n > 0$. Suppose that $f(x) \in \mathbb{F}_p[x]$ is irreducible. Then f has degree $d \mid n$ if and only if $f \mid x^{p^n} - x$. In particular, $x^{p^n} - x$ is a product of *all* irreducible polynomials in $\mathbb{F}_p[x]$ whose degree divide n.

Proof. ($\implies$) Suppose that $\deg f = d \mid n$. $F \coloneqq \mathbb{F}_p[x]/(f)$ is a degree d extension of $\mathbb{F}_p$, so it has order p^d. If α is a root of f in F, then $\alpha^{p^d} - \alpha = 0$, so

$$\alpha^{p^{2d}} = (\alpha^{p^d})^{p^d} = \alpha^{p^d} = \alpha.$$

Iterating this argument, we have $\alpha^{p^n} = \alpha$, so α is the root of $x^{p^n} - x$. So f, which is the minimal polynomial of α over $\mathbb{F}_p$ divides $x^{p^n} - x$.

($\impliedby$) Suppose that f divides $x^{p^n} - x$. Let F be the splitting field of $x^{p^n} - x$, and let α be a root of f in F. Then $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg f$ and $[F : \mathbb{F}_p] = n$, so $\deg f \mid n$.

For the last claim, notice that $x^{p^n} - x$ is separable, so it is a product of the irreducibles dividing it. □

2.5. Algebraic elements

November 7, 2023

We define

$$k[\alpha_1, \ldots, \alpha_n] \coloneqq \{p(\alpha_1, \ldots, \alpha_n) \mid p \in k[x_1, \ldots, x_n]\}.$$

By the isomorphism $k(\alpha) \cong k[x]/(m_\alpha)$, we have $k[\alpha] = k(\alpha)$. We will extend this claim to

$$k[\alpha_1, \ldots, \alpha_n] = k(\alpha_1, \ldots, \alpha_n).$$

Let $\alpha \in L$, let $T_\alpha \colon L \to L \colon x \mapsto \alpha x$ be a multiplication map. This is a k-linear map by viewing L as a field over k.

Example 2.29 – Let $L = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, $k = \mathbb{Q}$, $\alpha = 1 + \sqrt{2}$. L has a $\mathbb{Q}$-basis $\mathcal{B} = \{1, \sqrt{2}\}$. Then

$$T_\alpha(1) = 1 \cdot 1 + 1 \cdot \sqrt{2}$$
$$T_\alpha(\sqrt{2}) = 2 \cdot 1 + 1 \cdot \sqrt{2},$$

so

$$[T_\alpha]_{\mathcal{B}}^{\mathcal{B}} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} =: A.$$

Note that

$$\chi_A(x) = \det \begin{bmatrix} x-1 & -2 \\ -1 & x-1 \end{bmatrix} = (x-1)^2 - 2 = x^2 - 2x - 1.$$

The roots are $1 \pm \sqrt{2}$.

Proposition 2.30 (Minimal polynomial of T_α is minimal polynomial of α)
$m_{T_\alpha} = m_\alpha$. Moreover, χ_{T_α} is a power of m_α.

Proof. The map

$$T \colon L \to \mathrm{End}_k(L)$$
$$: \beta \mapsto T_\beta$$

is an injective ring homomorphism. Since T is a ring homomorphism, if $p \in k[x]$, then $p(T_\beta) = T_{p(\beta)}$. Then $m_\alpha(T_\alpha) = T_{m_\alpha(\alpha)} = T_0 = 0$, so $m_{T_\alpha} \mid m_\alpha$. $0 = m_{T_\alpha}(T_\alpha) = T_{m_{T_\alpha}(\alpha)}$, so $m_{T_\alpha}(\alpha) = 0$ since T is injective, so $m_\alpha \mid m_{T_\alpha}$, hence they are equal.

The top invariant factor for a matrix A *is* its minimal polynomial. All other invariant factors are divisors of it. Since m_α is irreducible, all other invariant factors are m_α. Therefore, χ_{T_α} is a power of m_α. □

Example 2.31 – Find a monic polynomial in $\mathbb{Q}[x]$ with $\alpha = 1 + 3\sqrt[3]{2}$ as a root.
Let $L = \mathbb{Q}(\sqrt[3]{2})$, $k = \mathbb{Q}$, with basis $\mathcal{B} = \{1, \sqrt[3]{2}, \sqrt[3]{4}\}$. Then $T_\alpha \colon \mathbb{Q}^3 \to \mathbb{Q}^3$ has

$$T_\alpha(1) = 1 \cdot 1 + 3\sqrt[3]{2}$$
$$T_\alpha(\sqrt[3]{2}) = 1 \cdot \sqrt[3]{2} + 3 \cdot \sqrt[3]{4}$$
$$T_\alpha(1) = 6 \cdot 1 + 1 \cdot \sqrt[3]{4}.$$

Hence,

$$[T_\alpha]_{\mathcal{B}}^{\mathcal{B}} = \begin{bmatrix} 1 & 0 & 6 \\ 3 & 1 & 0 \\ 0 & 3 & 1 \end{bmatrix} =: A.$$

Then a tedious calculation yields

$$\chi_A = x^3 - 3x^2 + 3x - 55.$$

Definition 2.11
L is algebraic over k if every element of L is algebraic over k.

Remark 2.32. If L is a finite extension of k, it is algebraic. $\alpha \in L$ is algebraic $\iff$ $k(\alpha)$ is a finite extension.

Lemma 2.33
If $\alpha, \beta \in L$ and are algebraic, then $k(\alpha, \beta)$ is algebraic of degree $\leq \deg m_\alpha \cdot \deg m_\beta$.

Proof. $k(\alpha) \subseteq k(\alpha, \beta)$. $[k(\alpha) : k] = \deg m_\alpha$, so $k(\alpha, \beta) = (k(\alpha))(\beta) \cong (k(\alpha))[x]/(n_\beta)$, where n_β is the minimal polynomial of β with coefficients in $k(\alpha)$. Then

$$[k(\alpha, \beta) : k(\alpha)] = \deg n_\beta \leq \deg m_\beta,$$

which implies

$$[k(\alpha, \beta) : k] = [k(\alpha, \beta) : k(\alpha)] \cdot [k(\alpha) : k] \leq \deg m_\alpha \cdot \deg m_\beta. \qquad \square$$

Corollary 2.34
If $\alpha, \beta \in L$ are algebraic, then so are $\alpha + \beta$ and $\alpha\beta$. So $\{x \in L \mid x \text{ algebraic over } k\}$ is a field. Moreover, $k(\alpha, \beta) = k[\alpha, \beta]$. By induction, if $\alpha_1, \ldots, \alpha_n$, then $k(\alpha_1, \ldots, \alpha_n) = k[\alpha_1, \ldots, \alpha_n]$.

Example 2.35 (The corollary does not hold for non-algebraic elements) – For $\pi \in \mathbb{R}$, $\mathbb{Q}[\pi] \neq \mathbb{Q}(\pi)$, since $\frac{1}{\pi}$ is only in $\mathbb{Q}(\pi)$.

2.6. Algebraic closures

Definition 2.12
A field L is an algebraic closure of k if it is an algebraic extension such that any non-constant polynomial in $k[x]$ has a root in L. In other words, L is the splitting field of any irreducible polynomial in $k[x]$.

Lemma 2.36
Every field has an algebraic closure. This algebraic closure is unique up to isomorphism.

Proof. Let $C := \{L \mid L \text{ is an algebraic extension of } k\}$. If $s_i \in C$ for all i, and $s_1 \subseteq s_2 \subseteq \cdots$, then $\bigcup_i s_i$ is an algebraic extension of k. By Zorn's lemma, we have a maximal element of C, call it L, i.e. there is no $L' \supseteq L$ such that L' is an algebraic extension.

Let $p(x) \in k[x]$ be non-constant. Suppose for contradiction that it has no roots in L. Let $q(x)$ be a prime divisor of p in $L[x]$ (note that $\deg q \geq 2$ because we assumed that p did not have a root in L), so $L[x]/(q)$ is an algebraic extension of L, and hence, an algebraic extension of k (since the algebraic extension of an algebraic extension is an algebraic extension).

We will not prove the second part, it is in the notes. $\square$

Lemma 2.37
If L is the algebraic closure of k, then every non-constant polynomial in $L[x]$ has a root in L.

Proof. Suppose that $p \in L[x]$ has no roots in L. Let $\alpha_1, \dots, \alpha_d$ be the coefficients of p (these are algebraic over k by definition). Then $F \coloneqq k(\alpha_1, \dots, \alpha_d)$ is a finite extension of k. Let q be a prime factor in $F[x]$ of p with no roots in L. So $F[x]/(q)$ is a finite extension of F (and hence k) that contains a root α of q. So α is a root of an element in $k[x]$, which implies $\alpha \in L$. This is a contradiction because we assumed L did not have the roots of p. □

2.7. Cyclotomic fields

November 9, 2023

Some of the "nicest" fields we study are the *cyclotomic fields*, which are of the form $\mathbb{Q}(\zeta_m)$, where ζ_m is a special root of unity called a *primitive* root of unity.

A motivating application for this section is if $A \in \mathrm{GL}_n(\mathbb{Z})$ such that A has finite order, i.e. $A^k = I$, what are the possible values of k? It turns out, if $n = 2$, k belongs to the set $\{1, 2, 3, 4, 6\}$. This does not hold if we replace $\mathbb{Z}$ with $\mathbb{R}$, because we can pick any rotation in $\mathrm{GL}_n(\mathbb{R})$.

Definition 2.13

An n**th root of unity** ζ is a solution of $\zeta^n = 1$. ζ is **primitive** if n is the smallest possible integer such that $\zeta^n = 1$ (the root is *imprimitive* otherwise).

Example 2.38 (Roots of unity in $\mathbb{C}$) – i is a 4th primitive root of unity, since $n = 4$ is the smallest n such that $i^n = 1$. i is a 8th imprimitive root of unity. In $\mathbb{C}$, $\zeta_n \coloneqq \exp\left(\frac{2\pi i}{n}\right)$ is a primitive nth root of unity. ζ_n^k a primitive nth root of unity if and only if $\gcd(k, n) = 1$.

Definition 2.14

The n**th cyclotomic polynomial** is

$$\Phi_n(x) \coloneqq \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} (x - \zeta_n^k) \in \mathbb{C}[x].$$

Lemma 2.39 (Gauss' Lemma)

Let $f, g \in \mathbb{Z}[x]$ be monic polynomials. Suppose that $f = gh$, where $h \in \mathbb{C}[x]$. Then $h \in \mathbb{Z}[x]$.

Moreover, if $f \in \mathbb{Z}[x]$ is monic, and $f = gh$, where $g, h \in \mathbb{Q}[x]$ are monic, then $g, h \in \mathbb{Z}[x]$.

Proof. The polynomial division algorithm says that since $h = \frac{f(x)}{g(x)}$, where $f, g \in \mathbb{Q}[x]$, then $h \in \mathbb{Q}[x]$. Let d be the smallest possible integer such that $dh(x) \in \mathbb{Z}[x]$. Suppose $d \neq 1$. Then let p be a prime divisor of d.

If $r(x) \in \mathbb{Z}[x]$, let $\overline{r}(x) \in \mathbb{F}_p[x]$ where $\overline{r}$ is formed by taking r's coefficients mod p. We have

$$df(x) = g(x) \cdot (dh(x)).$$

Modding the coefficients, we have $\overline{df}(x) = 0$, $\overline{g}(x) \neq 0$. So $\overline{dh}(x) = 0$, so p divides all coefficients of $dh(x)$. So $\left(\frac{d}{p}\right) h(x) \in \mathbb{Z}[x]$. □

We have

$$x^n - 1 = \prod_{1 \le k \le n} (x - \zeta_n^k) = \prod_{d \mid n} \Phi_d(x).$$

This allows us to show that the cyclotomic polynomials have integer coefficients.

Corollary 2.40
$\Phi_n(x) \in \mathbb{Z}[x]$ for all n.

Proof. We induct on n. For the base case, $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$. For the inductive step, we have

$$x^n - 1 = \left(\prod_{\substack{d \mid n \\ d < n}} \Phi_d(x) \right) \Phi_n(x).$$

So $\Phi_n(x) \in \mathbb{Z}[x]$ by Lemma 2.39. □

Proposition 2.41
$\Phi_n(x)$ is irreducible for all n.

Proof. Suppose not, i.e. $\Phi_n(x) = f(x)g(x)$ and f, g are monic in $\mathbb{Q}[x]$. By Lemma 2.39, we may assume that $f, g \in \mathbb{Z}[x]$. Suppose f is irreducible.

Claim 2.3. If ζ is a root of f, then ζ^p is a root of p for all primes $p \nmid n$.

> **Proof.** Suppose not. So ζ^p (since $p \nmid n$) is still a primitive nth root of unity, so ζ^p is a root of Φ_n. So ζ^p is a root of g, so ζ is a root of $g(x^p)$. Since f is irreducible, it is the minimal polynomial of ζ, so $f(x) \mid g(x^p)$. Using the bar notation from before, $\overline{f}(x) \mid \overline{g}(x^p) = (\overline{g}(x))^p \in \mathbb{F}_p[x]$, so any root of f is a root of g. Since $\overline{\Phi_n} = \overline{f}\,\overline{g}$, it is not separable. So $\overline{x^n - 1}$ is not separable in $\mathbb{F}_p[x]$. Therefore, $p \mid n$, a contradiction. ■

Claim 2.4. Let a be an integer such that $\gcd(a, n) = 1$. Then if ζ is a root of f, ζ^a is a root of f.

> **Proof.** Let $a = p_1 \cdots p_n$, where p_i are prime. Since ζ is a root of f, ζ^{p_1} is root of f, so $(\zeta^{p_1})^{p_2}$ is a root of f, and so on until we get that $\zeta^a = \zeta^{p_1 \cdots p_n}$ is a root of f. ■

Since f has a root ζ that is a primitive nth root of unity and all primitive nth root of unity can be written as ζ^a where $\gcd(a, b) = 1$. f contains all root of Φ_n and hence Φ_n is irreducible. □

Proposition 2.42
Φ_n is the minimal polynomial of ζ_n.

As a result, we have $\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[x]/(\Phi_n)$. It follows that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n = \phi(n)$. When doing computations, it's useful to have the bound $\phi(n) \ge \sqrt{n/2}$.

2.7.1. Application: Cyclic group actions on $\mathbb{Q}$-vector spaces

Recall if G is a finite group that acts linearly on $\mathbb{Q}^n$, then $\mathbb{Q}^n$ is a $\mathbb{Q}[G]$-module. Moreover, $\mathbb{Q}^n$ decomposes into a direct sum of simple $\mathbb{Q}[G]$-modules. Finally, every simple $\mathbb{Q}[G]$-module is a summand in this decomposition. Let's look specifically at the case where $G = \mathbb{Z}/n$.

$$\mathbb{Q}[\mathbb{Z}/n] \cong \mathbb{Q}[x]/(x^n - 1) \cong \mathbb{Q}[x]/\left(\prod_{d|n} \Phi_d\right) \cong \bigoplus_{d|n} \mathbb{Q}[x]/(\Phi_d) \cong \bigoplus_{d|n} \mathbb{Q}(\zeta_d).$$

So if $A \in \mathrm{Mat}_{m\times n}(\mathbb{Q})$ such that $A^n = I$, then as a $\mathbb{Q}[\mathbb{Z}/n]$-module, $\mathbb{Q}^n$ decomposes into a direct sum of modules, each isomorphic to $\mathbb{Q}(\zeta_d)$ for $d \mid n$ such that A acts by multiplication by ζ_d.

Given a positive integer d, the **dth cyclotomic matrix** is the companion matrix of $\Phi_d(x) = x^{\phi(d)} + a_{\phi(d)-1}x^{\phi(d)-1} + \cdots + a_0$:

$$A_d \coloneqq \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ \vdots & 1 & \ddots & & \vdots \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \cdots & 1 & -a_{\phi(d)-1} \end{bmatrix}.$$

Proposition 2.43 (Conjugacy classes of finite order matrices in $\mathrm{GL}_m(\mathbb{Q})$)
If $A \in \mathrm{GL}_m(\mathbb{Q})$ such that $A^n = I$, then there exists some increasing sequence $d_1 \leq \cdots \leq d_k$ of divisors of n such that, up to change of basis (i.e. up to conjugacy), A looks like a block diagonal of cyclotomic matrices:

$$\begin{bmatrix} \boxed{A_{d_1}} & & \\ & \ddots & \\ & & \boxed{A_{d_m}} \end{bmatrix}.$$

Example 2.44 (Final review) – What is the smallest positive integer n so that there exists $A \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$ so that $A^{2023} = I$, but $A^k \neq I$ for $k \in \{1, 7, 17, 119, 289\}$ (the proper divisors of 2023)?

If $A \in \mathrm{Mat}_{n\times n}(\mathbb{Q})$, then we wouldn't have an issue. So let's do some wishful thinking. Notice that $\mathbb{Q}[\mathbb{Z}/2023] \cong \mathbb{Q}[x]/(x^{2023}-1) \cong \mathbb{Q} \oplus \mathbb{Q}(\zeta_7) \oplus \mathbb{Q}(\zeta_{17}) \oplus \mathbb{Q}(\zeta_{119}) \oplus \mathbb{Q}(\zeta_{289}) \oplus \mathbb{Q}(\zeta_{2023})$, where A acts on $\mathbb{Q}(\zeta_d)$ by multiplication by ζ_d.

The rational canonical form of the action on $\mathbb{Q}(\zeta_m)$ is a $\phi(m)\times\phi(m)$ matrix of order m with 1's on the subdiagonal and whose entries in the final column are the negatives of the coefficients of $\Phi_m(x)$, which are *integers*.

Any $m \times m$ matrix in $\mathbb{Q}$ which has an order dividing 2023 is conjugate in $\mathrm{GL}_m(\mathbb{Q})$ to a block diagonal one with these matrices occurring as blocks. Let's evaluate some ϕ values

$$\phi(k) = \begin{cases} 1 & \text{if } k = 1 \\ 6 & \text{if } k = 7 \\ 16 & \text{if } k = 17 \\ 119 \cdot \left(\frac{6}{7}\right)\left(\frac{16}{17}\right) = 96 & \text{if } k = 119 = 7\cdot 17 \\ 17^2 \cdot \left(\frac{16}{17}\right) = 272 & \text{if } k = 289 = 17^2 \\ 2023 \cdot \left(\frac{6}{7}\right)\left(\frac{16}{17}\right) = 1632 & \text{if } k = 2023 \end{cases}$$

We want the matrix to have order $2023 = 17^2 \cdot 7$, so our most efficient choices would be $(1, 2023)$ and $(7, 17^2)$. $\phi(1)+\phi(2023) = 1633$ is greater than $\phi(7)+\phi(17^2) = 278$, so we choose the latter. The matrix is a block matrix where the first block is the 7th cyclotomic matrix and the second block is the 17^2 cyclotomic matrix.

2.8. The Galois correspondence

2.8.1. Galois extensions

November 14, 2023

In the homework, we proved the following:

Proposition 2.45

If F is a splitting field, and $p(x) \in k[x]$ such that p is irreducible and there is an $\alpha \in F$ such that $p(\alpha) = 0$, then p splits completely, i.e. $p(x) = \prod_i (x - \alpha_i)$ for some $\alpha_i \in F$.

Let F be a splitting field. An **intermediate field** is a field $k \subseteq L \subseteq F$. Let L_1 and L_2 be isomorphic intermediate fields via the isomorphism $\sigma\colon L_1 \to L_2$ such that $\sigma|_k = \mathrm{id}_k$. Then we can lift this isomorphism σ to an isomorphism $\widetilde{\sigma}\colon F \to F$.

For the following sections, it should be noted that when we write F/k, we are not taking a literal quotient, this is just shorthand for saying "F *over* k."

Definition 2.15

The **automorphism group** of F/k is defined as

$$\mathrm{Aut}(F/k) \coloneqq \left\{\sigma\colon F \xrightarrow{\sim} F \mid \sigma \text{ is a field isomorphism, } \sigma\big|_k \text{ is an isomorphism}\right\},$$

i.e. all field isomorphisms that fix k. If $\alpha \in F$ and $\sigma \in \mathrm{Aut}(F/k)$, then we let $\alpha^\sigma \coloneqq \sigma(\alpha)$. If $p \in F[x]$ such that $p(x) = \sum_n a_n x^n$, then $p^\sigma(x) \coloneqq \sum_n a_n^\sigma x^n$.

We have

$$0 = 0^\sigma = p(\alpha)^\sigma = p^\sigma(\alpha^\sigma) = p(\alpha^\sigma).$$

From this, it follows that $\{\alpha^\sigma \mid \sigma \in \mathrm{Aut}(F/k)\}$ consists of roots of m_α. Therefore, σ simply *permutes the roots* of the polynomial p.

Example 2.46 –

1. $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ consists of the identity, and complex conjugation. We will prove later that these are the only ones. Hence, $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2$.
2. $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}/\mathbb{Q})) = \{\mathrm{id}, \tau\}$, where $\tau(a + b\sqrt{2}) = a - b\sqrt{2}$. Hence, $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}/\mathbb{Q})) \cong \mathbb{Z}/2$ as well.

We observe in these examples that the group order is exactly the degree of the field extension. This leads us to the following proposition:

Proposition 2.47

$|\mathrm{Aut}(F/k)| \leq [F : k]$. Equality holds if and only if for all $\alpha \in F$ its minimal polynomial is separable and splits.

Proof. Induct on $[F : k]$. The base case is trivial. Let $\alpha \in F$ and let

$$N_\alpha := \#\{\sigma(\alpha) \mid \sigma \in \mathrm{Aut}(F/k)\} \leq \deg m_\alpha.$$

Claim 2.5. $N_\alpha = \deg m_\alpha$ if and only if m_α is separable and splits.

> **Proof.** ($\Longrightarrow$) m_α has $\deg m_\alpha$ distinct roots, all in F.
> ($\Longleftarrow$) Let β be another root of m_α (we have $\deg m_\alpha$ many choices). Then the isomorphism
> $$k(\alpha) \cong k[x]/(m_\alpha) \cong k(\beta)$$
> extends to an element $\sigma \in \mathrm{Gal}(F/k)$, so $N_\alpha = \deg m_\alpha$. ■

If $\sigma_1, \sigma_2 \in \mathrm{Aut}(F/k)$, then $\sigma_1(\alpha) = \sigma_2(\alpha) \iff \sigma_1^{-1}\sigma_2 \in \mathrm{Aut}(F/k(\alpha)) \iff \sigma_1 \in \sigma_1 \cdot \mathrm{Aut}(F/k(\alpha))$. Therefore, the size of the coset is

$$|\mathrm{Aut}(F/k)/\mathrm{Aut}(F/k(\alpha))| = N_\alpha.$$

It follows that

$$\begin{aligned} |\mathrm{Aut}(F/k)| &= |\mathrm{Aut}(F/k(\alpha))| \cdot |\mathrm{Aut}(F/k)/\mathrm{Aut}(F/k(\alpha))| \\ &= |\mathrm{Aut}(F/k(\alpha))| \cdot N_\alpha \\ &\leq [F : k(\alpha)] \\ &= [F : k(\alpha)][k(\alpha) : k] = [F : k]. \end{aligned}$$

Next we show equality holds $\iff \forall \alpha \in F$, m_α is separable and splits.
($\Longrightarrow$) If equality holds, then $N_\alpha = \deg m_\alpha$. So by the Claim 2.5, m_α is separable and splits.
($\Longleftarrow$) In this case, $N_\alpha = \deg m_\alpha$ and moreover, for any $\beta \in F$ its minimal polynomial over $k(\alpha)$ is separable and splits since this is true over k. By the inductive hypothesis, $|\mathrm{Aut}(F/k(\alpha))| = [F : k(\alpha)]$. □

The case of equality is special enough for us to delegate a new definition for it.

Definition 2.16

A finite extension F over k is **Galois** if any of the following equivalent conditions hold:

1. $|\mathrm{Aut}(F/k)| = [F : k]$,
2. for all $\alpha \in F$, m_α is separable and splits,
3. F is the splitting field for a separable polynomial.

We call $\mathrm{Aut}(F/k) =: \mathrm{Gal}(F/k)$ the **Galois group** if the extension is Galois.

Example 2.48 (Non-example of Galois extension) – $\mathbb{Q}(\sqrt[3]{3})$ is not a Galois extension over $\mathbb{Q}$. We can show this in two ways. By property (2), since $m_{\sqrt[3]{3}} = x^3 - 2$ and this polynomial does not split over $\mathbb{Q}(\sqrt[3]{3})$, since this field is contained in $\mathbb{R}$, but some roots belong in $\mathbb{C}$.

By property (1), if we assume $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q})$, then it must fix $\sqrt[3]{2}$. This implies $\sigma = \mathrm{id}$. Hence, $1 = \left|\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q})\right| \neq [\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$.

2.8.2. The primitive element theorem

Definition 2.17

If $G \leq \mathrm{Aut}(F/k)$, then its **fixed field** $\mathrm{Fix}_G(F) := \{x \in F \mid \sigma(x) = x, \forall \sigma \in G\}$. It is a field because $\sigma(x+y) = \sigma(x) + \sigma(y) = x + y$ and $\sigma(xy) = \sigma(x)\sigma(y) = xy$.

Lemma 2.49

Let F/k be Galois. Then $\mathrm{Fix}_{\mathrm{Aut}(F/k)}(F) = k$.

Proof. Let $G = \mathrm{Aut}(F/k)$ and $L := \mathrm{Fix}_G(F)$. Then F/L is Galois. Then $[F : L] = |\mathrm{Aut}(F/L)| = |\mathrm{Aut}(F/k)| = [F : k]$, where the middle inequality holds because any automorphism fixing k automatically fixed L. So $k = L$. □

Lemma 2.50

If F/k is Galois, then there are only finitely many intermediate fields.

Proof. Consider the maps

$$\begin{aligned} \{\text{intermediate fields}\} &\xrightarrow{f} \{\text{subgroups of } \mathrm{Aut}(F/k)\}, \\ L &\mapsto \mathrm{Aut}(F/L). \end{aligned}$$

$$\begin{aligned} \{\text{subgroups of } \mathrm{Aut}(F/k)\} &\xrightarrow{g} \{\text{intermediate fields}\}, \\ H &\mapsto \mathrm{Fix}_H(F). \end{aligned}$$

By the previous lemma, $\mathrm{Fix}_{\mathrm{Aut}(F/L)}(F) = L$, so $g \circ f = \mathrm{id}$, so f is injective. □

Theorem 2.51 (Primitive element theorem)
Let F/k be a finite extension with finitely many intermediate fields. Then there exists $\alpha \in F$ such that $F \cong k(\alpha)$.

Proof. If F is a finite field and α is a generator of the cyclic group $F^\times$, then $F \cong k(\alpha)$. So suppose k is an infinite field. Since F is a finite extension, $F = k(\alpha_1, \ldots, \alpha_n)$.

It suffices to show that $k(\alpha_1, \alpha_2) = k(\beta)$ for some $\beta \in F$. Since there exists finitely many intermediate fields, $L \coloneqq k(\alpha_1 + a\alpha_2) = k(\alpha_1 + b\alpha_2)$ for some $a, b \in k$, $a \neq b$. L contains $(\alpha_1 + a\alpha_2)$ and $(\alpha_1 + b\alpha_2)$, so it contains the difference $(a-b)\alpha_2$. So L contains

$$\alpha_2 = \frac{(a-b)\alpha_2}{(a-b)},$$

so L contains $\alpha_1 = \alpha_1 + a\alpha_2 - a\alpha_2$, so $L = k(\alpha_1, \alpha_2)$ (let $\beta = \alpha_1 + a\alpha_2$). □

Corollary 2.52
If $K/\mathbb{Q}$ is a finite extension, then $K = \mathbb{Q}(\alpha)$ for some α.

Proof. Suppose $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. Let m_{α_i} be the minimal polynomial of α_i. Let $p = \operatorname{lcm}(m_{\alpha_i})_{i=1}^n$. In $\mathbb{Q}[x]$, any product of distinct primes is separable, so the splitting field F of p is Galois, and contains K. Since F has finitely many intermediate fields between itself and $\mathbb{Q}$, so does K, so it satisfies the primitive element theorem. □

2.8.3. The Galois correspondence theorem

We now get to the celebrated Galois correspondence theorem. The theorem itself is important, but to get a sense for how to use it, we covered its use in certain fields we have encountered so far.

Theorem 2.53 (Galois correspondence theorem)
The maps

$$\begin{aligned} \{\text{intermediate fields}\} &\xrightarrow{f} \{\text{subgroups of } \operatorname{Aut}(F/k)\}, \\ L &\mapsto \operatorname{Aut}(F/L), \end{aligned}$$

$$\begin{aligned} \{\text{subgroups of } \operatorname{Aut}(F/k)\} &\xrightarrow{g} \{\text{intermediate fields}\}, \\ H &\mapsto \operatorname{Fix}_H(F), \end{aligned}$$

are bijections.

Proof. We have that f is an injection. We will show that g is an injection. Let $H \leq \operatorname{Aut}(F/k)$, and let $L = \operatorname{Fix}_H(F)$. We want to show that $\operatorname{Aut}(F/L) = H$. By the primitive element theorem, $F = L(\alpha)$ for some α. Let

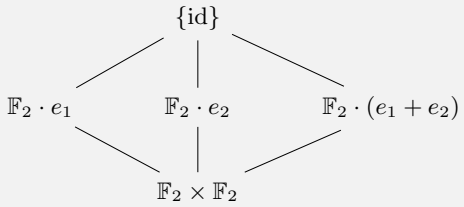
$$p(x) = \prod_{h \in H} (x - \alpha^h) = x^{|H|} - \left(\sum_{h \in H} \alpha^h \right) x^{|H-1|} + \cdots + (-1)^{|H|} \prod_{h \in H} \alpha^h.$$

Each of these coefficients are h invariant, since they are symmetric polynomials in $\{\alpha^h \mid h \in H\}$. Therefore, $p(x) \in L[x]$. $|H| \leq |\mathrm{Aut}(F/L)| = [F : L] = \deg m_\alpha \leq \deg p = |H|$. Therefore, $H = \mathrm{Aut}(F/L)$. □

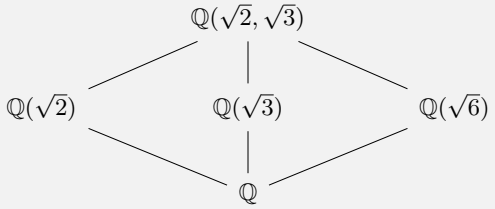
Example 2.54 – Let $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $(x^2 - 2)(x^2 - 3)$, so F is Galois. $|\mathrm{Aut}(F/k)| = 4$, so $\mathrm{Aut}(F/k) \cong \mathbb{Z}/4$, or $\mathbb{Z}/2 \times \mathbb{Z}/2$. The number of subgroups of $\mathbb{Z}/4$ is 3, so the Galois correspondence says that $\mathrm{Aut}(F/k) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.

Fix a basis (e_1, e_2) so that $\mathbb{F}_2^2 = \mathbb{F}_2 \cdot e_1 + \mathbb{F}_2 \cdot e_2$. We represent the correspondence with a diagram of the subgroups, where inclusion is going down, and the intermediate fields, where the inclusion is going up, to emphasize the connection between these.

Subgroups



Intermediate fields



November 16, 2023

Example 2.55 – Let $k = \mathbb{Q}$ and $F = \mathbb{Q}(\zeta_n)$. Then F/k is Galois because F is the splitting field of $\Phi_n(x)$. So $|\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

If $\sigma \in \mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. $\sigma(\zeta_n) = \zeta_n^d$ for d coprime to n (since roots are sent to roots of a polynomial in k). Write σ_d for the automorphism sending $\zeta_n \mapsto \zeta_n^d$. Recall the automorphism is a group where the operation is composition.

$$\sigma_{d_1} \circ \sigma_{d_2}(\zeta_n) = \sigma_{d_1}(\zeta_n^{d_2}) = \sigma_{d_1}(\zeta_n)^{d_2} = (\zeta_n^{d_1})^{d_2} = \zeta_n^{d_1 d_2} = \sigma_{d_1 d_2}(\zeta_n).$$

So there is an isomorphism

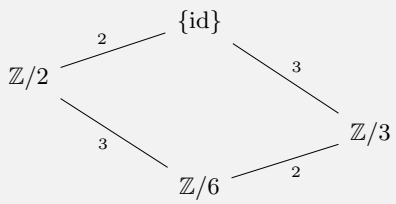
$$\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times,$$
$$\sigma_d \mapsto d.$$

Example 2.56 – Following the previous discussion, suppose we want to find all subfields of $\mathbb{Q}(\zeta_7)$. Then

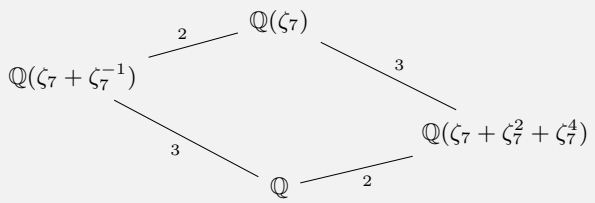
$$\mathrm{Aut}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong (\mathbb{Z}/7)^\times \cong \mathbb{Z}/6.$$

The subgroups of $\mathbb{Z}/6$ are $\{\mathrm{id}\}$, $\mathbb{Z}/2 = \langle -1 \rangle$, $\mathbb{Z}/3 = \langle 2 \rangle$, and $\mathbb{Z}/6$.

Subgroups of $(\mathbb{Z}/7)^\times$



Intermediate fields



Example 2.57 – Let p be prime and let $n > 0$. $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a Galois extension because it is a splitting field of $x^{p^n} - x$ (which is separable). We have

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = |\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)|\,.$$

Let $\sigma_p \colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} : x \mapsto x^p$. So σ_p^k fixes the elements of $\mathbb{F}_{p^n}$ that satisfy $x^{p^k} - x = 0$, i.e. the field $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^n}$. So $\mathrm{ord}(\sigma_p) = n$. Hence, $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma_p \rangle \cong \mathbb{Z}/n\mathbb{Z}$.

November 21, 2023

Lemma 2.58 (Normal subgroups correspond to Galois extensions)
Let F/k be Galois. Let L be an intermediate field such that $H = \mathrm{Aut}(F/L)$, $G = \mathrm{Aut}(F/k)$. Then the following are equivalent:

1. $\sigma(L) = L$ for all $\sigma \in G$,
2. $H \trianglelefteq G$,
3. L/k is Galois.

Moreover, $G/H \cong \mathrm{Gal}(L/k)$.

Proof. ((1) $\implies$ (2) & (3)) Then there exists a homomorphism

$$\begin{aligned} \mathrm{Res}_L \colon \mathrm{Aut}(F/k) &\to \mathrm{Aut}(L/k), \\ \sigma &\mapsto \sigma\big|_L. \end{aligned}$$

Then $\ker(\mathrm{Res}_L) = \mathrm{Aut}(F/L) \trianglelefteq \mathrm{Aut}(F/k)$. Moreover,

$$|\mathrm{im}(\mathrm{Res}_L)| = \frac{|\mathrm{Aut}(F/k)|}{|\mathrm{Aut}(F/L)|} = \frac{[F:k]}{[F:L]} = [L:k].$$

Since

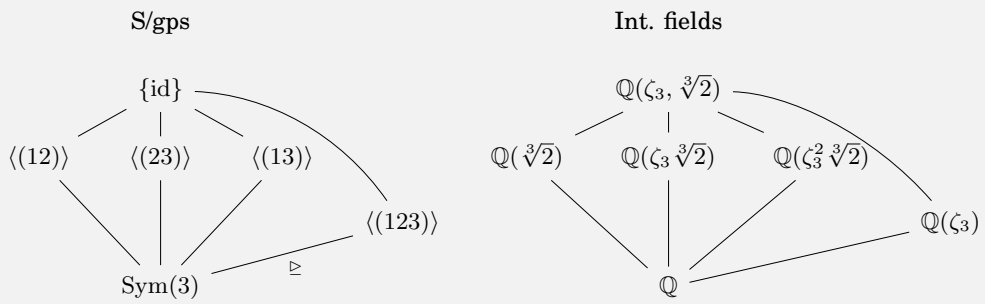
$$|\mathrm{im}(\mathrm{Res}_L)| \leq |\mathrm{Aut}(L/k)| \leq [L:k],$$

Res_L is surjective and L/k is Galois.

((3) $\implies$ (1)) Let L/k be Galois, so L is a splitting field, so L is preserved by any $\sigma \in \mathrm{Aut}(F/k)$.

((2) $\implies$ (1)) Assume $\mathrm{Aut}(F/L) \trianglelefteq \mathrm{Aut}(F/k)$. Let $\sigma \in \mathrm{Aut}(F/k)$. $\sigma(L)$ is a field fixed by $\sigma\,\mathrm{Aut}(F/L)\sigma^{-1} = \mathrm{Aut}(F/L)$, so $\sigma(L) = L$. □

Example 2.59 – Let $F = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$, which is a splitting field of $x^3 - 2$. $\mathrm{Gal}(F/\mathbb{Q}) = \mathrm{Sym}(3)$, which acts on the roots of $x^3 - 2$. We have the diagram



which shows that $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\zeta_3\sqrt[3]{2})$, and $\mathbb{Q}(\zeta_3^2\sqrt[3]{2})$ are not Galois extensions of $\mathbb{Q}$, while $\mathbb{Q}(\zeta_3)$ is. Indeed, $\mathbb{Q}(\zeta_3)$ is the splitting field of $\frac{x^3-1}{x-1} = x^2 + x + 1$.

2.8.4. Composites

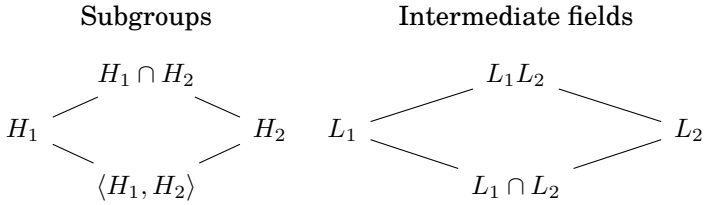
Definition 2.18

Let $L_1, L_2 \subseteq F$ be subfields. The **composite field** L_1L_2 is the smallest field in F containing L_1 and L_2.

The following lemma is immediate from the Galois correspondence:

Lemma 2.60

Let F/k be Galois with intermediate fields L_1, L_2. Set $H_i := \mathrm{Aut}(F/L_i)$. Then $\mathrm{Aut}(F/L_1 \cap L_2) = \langle H_1, H_2\rangle$, and $\mathrm{Aut}(F/L_1L_2) = H_1 \cap H_2$.



Proof. $L_1 \cap L_2$ is the biggest field contained in L_1 and L_2, so by the Galois correspondence it must be fixed by the smallest group containing H_1 and H_2.

L_1L_2 is the smallest field containing L_1 and L_2, so by the Galois correspondence it must be fixed by the biggest subgroup containing H_1 and H_2. □

Lemma 2.61

$[L_1L_2 : k] \leq [L_1 : k][L_2 : k]$.

Proof. Let $(\alpha_1, \ldots, \alpha_s)$, $(\beta_1, \ldots, \beta_r)$ be a basis of L_1 and L_2 respectively. Since L_1L_2 is a finite extension, $L_1L_2 = k(\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_r) = k[\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_r]$. Let $S = (\alpha_i\beta_j)_{ij}$. It suffices to let $p \in k[x_1, \ldots, x_s, y_1, \ldots, y_r]$ be a monomial (i.e. of the form $x_1^{a_1} \cdots x_s^{a_s} y_1^{b_1} \cdots y_r^{b_r}$) and to show that $p(\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_r) \in \mathrm{span}_k(S)$. Then

let
$$p(\alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_r) = \ell_1 \ell_2,$$
where $\ell_1 \in L_1$, $\ell_2 \in L_2$. But $\ell_1 \in \mathrm{span}_k(\alpha_1, \dots, \alpha_s)$, and $\ell_2 \in \mathrm{span}_k(\beta_1, \dots, \beta_r)$. □

By induction, we have that $[L_1 \cdots L_n : k] \leq [L_1 : k] \cdots [L_n : k]$.

2.9. The fundamental theorem of algebra

We will now apply the Galois correspondence to prove other theorems, starting with a (mostly) algebraic proof of the fundamental theorem of algebra. Before we begin the proof, we will need some group theory results.

Definition 2.19

Let p be a prime. A group G is a p-group if $|G| = p^k$ for some $k \in \mathbb{N}$.

Lemma 2.62

If G is a p-group, $Z(G) = \{g \in G \mid hg = gh, \forall h \in G\}$ has order divisible by p. Moreover, G has a nontrivial abelian quotient.

Proof. If G acts by permutations on a set X and $X = \bigcup_{i=1}^n G \cdot x_i$ for some $x_i \in X$, then
$$|X| = \sum_{i=1}^n |G \cdot x_i| = \sum_{i=1}^n \frac{|G|}{|\mathrm{Stab}_G(x_i)|}$$

This is the *orbit-stabilizer theorem*.

Let $X = G$. Let $G \curvearrowright G$ by conjugation. Applying the orbit-stabilizer theorem, if $x_1, \dots, x_n$ is a list of representatives for each conjugacy class in G,

$$|G| = \sum_{i=1}^n \frac{|G|}{|\mathrm{Stab}_G(x_i)|} = \sum_{i=1}^n \frac{|G|}{|C(x_i)|} = |Z(G)| + \sum_{x_i \notin Z(G)} \frac{|G|}{|C(x_i)|}.$$

Where $C(x_i) = \{h \in G \mid hx_i = x_i h\}$ is the centralizer of x_i. This is the *class equation*.

Since $x_i \notin Z(G)$, $|G| > |C(x_i)|$, and $\frac{|G|}{|C(x_i)|}$ is divisible by p for each i. This implies $|Z(G)|$ is divisible by p.

For the next claim, induct on $|G|$. For the base case, if $|G| = p$, then $G = \mathbb{Z}/p$. For the inductive step, if $G = Z(G)$ we are done. If $G \neq Z(G)$, then $G/Z(G)$ has smaller size, hence a nontrivial abelian quotient. □

Theorem 2.63 (Fundamental theorem of algebra)

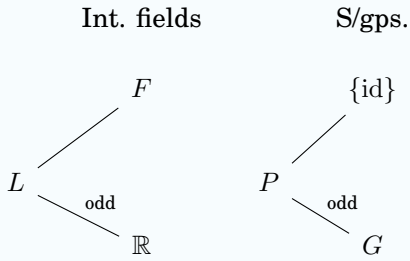
If $p \in \mathbb{C}[x]$ is non-constant, then p has a root in $\mathbb{C}$.

Proof. We want to show that $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$, i.e. for any monic irreducible $f \in \mathbb{R}[x]$, we want to show that all roots of f belong in $\mathbb{C}$. WLOG, assume $f(x) \neq x^2 + 1$. Let F be the splitting field of $f(x)(x^2 + 1)$. We want to show $F = \mathbb{C}$.

We can work with $\mathbb{R}$ because the algebraic closure of $\mathbb{C}$ is just $\mathbb{C}$ again.

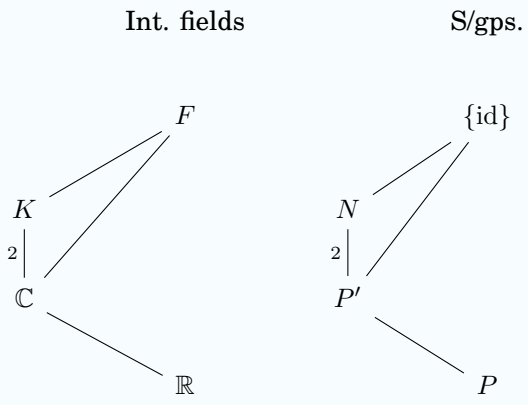
Let G be the Galois group of $F/\mathbb{R}$. Let P be the Sylow 2-subgroup of G, i.e. some subgroup such that $[G : P]$ is odd. Let $L = \mathrm{Fix}_P(F)$, the corresponding intermediate

field in the Galois correspondence.



Since $[L : \mathbb{R}]$ is odd, if $\alpha \in L$, then its minimal polynomial $m_\alpha \in \mathbb{R}[x]$ has odd degree. So m_α has a root in $\mathbb{R}$ by analysis (look at $x \to \infty$ and $x \to -\infty$ and use the intermediate value theorem). So $m_\alpha = x - \alpha$ (if it were higher degree it would reduce). So $L = \mathbb{R}$ and hence $G = P$.

Let $P' = \mathrm{Gal}(F/\mathbb{C})$. This is a 2-group, i.e. $|P'| = 2^k$. Suppose $k \neq 0$ for contradiction. By Lemma 2.62, there exists $N \trianglelefteq P'$ such that $P'/N \cong \mathbb{Z}/2$. So there exists K such that $K/\mathbb{C}$ is a quadratic extension of $\mathbb{C}$.



Thus, K is the splitting field of a quadratic polynomial in $\mathbb{C}[x]$, i.e. it is created by adjoining a root of some $ax^2 + bx + c \in \mathbb{C}[x]$. By the quadratic formula, $K = \mathbb{C}$, a contradiction. □

Remark 2.64. As should be expected, we need some analysis to complete the proof of the fundamental theorem of algebra (in this case, the mean value theorem). However, the majority of this proof is using Galois theory.

2.10. Algebraic number theory

This section is adapted from homework exercises.

Definition 2.20

Let K be a finite extension of $\mathbb{Q}$. We call K an **algebraic number field**. Define the **(algebraic) integers in K**, denoted $\mathcal{O}_K$, as the set of all $\alpha \in K$ such that there is a monic polynomial p with integer coefficients such that $p(\alpha) = 0$. In symbols,

$$\mathcal{O}_K := \{\alpha \mid \exists p \in \mathbb{Z}[x] \text{ monic}, p(\alpha) = 0\}.$$

Proposition 2.65

α is an algebraic integer $\iff$ its minimal polynomial has integer coefficients.

Proof. ($\implies$) $m_\alpha(x) \mid p(x)$, so by the division algorithm, we have $m_\alpha(x)g(x) = p(x)$ for some $g(x) \in \mathbb{Q}[x]$. $g(x)$ is monic by looking at the leading coefficients. By Gauss' lemma, $g, m_\alpha \in \mathbb{Z}[x]$.

($\impliedby$) Let $p = m_\alpha \in \mathbb{Z}[x]$. □

Example 2.66 – Let d be a squarefree integer. Determine $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

Let $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. Since $\mathbb{Q}(\sqrt{d})$ is a degree 2 extension, the minimal polynomial of any $a + b\sqrt{d}$ will be of degree 2. Then, in order for the coefficients to be rational, it will be of the form

$$(x - (a + b\sqrt{d}))(x - (a - b\sqrt{d})) = x^2 - 2ax + a^2 - b^2 d.$$

If we want the coefficients to lie in $\mathbb{Z}$, then we need $a \in \frac{1}{2}\mathbb{Z}$ by the degree 1 coefficient. If $a \in \mathbb{Z}$, then $b \in \mathbb{Z}$ by the constant term. It suffices to check $a = \frac{1}{2}$ and $b = \frac{1}{2}$. If $a = \frac{1}{2}$, then

$$\begin{aligned} &\left(\frac{1}{2}\right)^2 - b^2 d \in \mathbb{Z} \\ \implies &-4b^2 d \equiv -1 \pmod 4 \\ \implies &4b^2 d \equiv 1 \pmod 4 \\ \implies &b \notin \mathbb{Z}. \end{aligned}$$

If $b = \frac{1}{2}$, then we require

$$4\left(\frac{1}{2}\right)^2 d \equiv 1 \pmod 4 \implies d \equiv 1 \pmod 4.$$

If this holds, then $\frac{1}{2} + \frac{1}{2}\sqrt{d} \in \mathcal{O}_K$. Therefore,

$$\mathcal{O}_K = \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\right\},$$

or

$$\mathcal{O}_K = \left\{a + b\sqrt{d} + c\left(\frac{1}{2} + \frac{1}{2}\sqrt{d}\right) \mid a, b, c \in \mathbb{Z}\right\}, \qquad \text{if } d \equiv 1 \pmod 4.$$

Lemma 2.67

Let $\mathbb{Z}[\alpha] = \{p(\alpha) \mid p \in \mathbb{Z}[x]\}$. α is an algebraic integer $\iff$ $\mathbb{Z}[\alpha]$ is a finitely-generated free $\mathbb{Z}$-module.

Proof. ($\implies$) Let $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. If $p(\alpha) \in \mathbb{Z}[\alpha]$, then we can reduce the polynomial to a degree $n-1$ polynomial in α by the replacement

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0.$$

On the other hand, elements of the LHS are polynomials in α with coefficients in $\mathbb{Z}$. Hence,

$$\operatorname{span}_{\mathbb{Z}}\left\{1, \alpha, \ldots, \alpha^{n-1}\right\} = \mathbb{Z}[\alpha].$$

Suppose there exist $b_0, \ldots, b_{n-1} \in \mathbb{Z}$ that are not all zero such that

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = 0.$$

But then $\sum_n b_n x^n$ is a nonzero polynomial in $\mathbb{Q}[x]$ of degree $\leq n-1$ that had a root of α. If we make this monic by dividing by the leading coefficient, this contradicts the fact that m_α is a minimal polynomial. Hence, $1, \alpha, \ldots, \alpha^{n-1}$ are a basis for $\mathbb{Z}[\alpha]$.

($\Longleftarrow$) Let $\mathbb{Z}[\alpha] = \operatorname{span}_{\mathbb{Z}} \{e_1, \ldots, e_n\}$. Write

$$\alpha e_i = \sum_{j=1}^{n} c_{ij} e_j$$

for some constants $\{c_{ij}\}_{i,j}$. Then α is an eigenvalue of the matrix $[c_{ij}]$ because

$$\alpha \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix} = \begin{bmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \cdots & c_{nn} \end{bmatrix} \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix}.$$

α is then a root of the characteristic polynomial $\chi(x)$ of the matrix $[c_{ij}]$, which is monic and whose coefficients belong to $\mathbb{Z}$. □

Lemma 2.68

If α, β are algebraic integers, $\mathbb{Z}[\alpha, \beta]$ is a finitely generated free $\mathbb{Z}$-module.

Proposition 2.69

$\mathcal{O}_K$ is a ring.

Proof. $\mathbb{Z}[\alpha\beta], \mathbb{Z}[\alpha+\beta] \subseteq \mathbb{Z}[\alpha, \beta]$ are submodules of a free module over a PID, hence they are free. Since they are clearly finitely generated, it follows that $\alpha\beta, \alpha+\beta \in \mathcal{O}_K$ by Lemma 2.67. □

2.11. Computing Galois groups over $\mathbb{Q}$

November 28, 2023

Note that the splitting field of any polynomial $f \in \mathbb{Q}[x]$ is Galois because finite extensions of $\mathbb{Q}$ are separable. Let its splitting field be K. Define $G_f := \operatorname{Gal}(K/\mathbb{Q})$. The goal of this section is to compute G_f, and we will employ several tools, the strongest of which will be *Dedekind's theorem*, which gives us properties about how automorphisms permute the roots.

2.11.1. Irreducibility

Lemma 2.70 (Rational root test)

Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Then if $\frac{c}{d}$ is a root, where c, d are coprime integers, then $c \mid a_0$ and $d \mid a_n$.

Proof. $0 = d^n f\left(\frac{c}{d}\right) = a_n c^n + a_{n-1} c^{n-1} d + \cdots + a_c d^{n-1} + a_0 d^n$. The first $n-1$ terms on the RHS are divisible by c, and so is the 0 on the LHS. Since d shares no prime divisors with c, $c \mid a_0$ for the sum to be divisible by c.

The last $n-1$ terms on the RHS are divisible by d, so similarly we prove that $d \mid a_n$. □

Example 2.71 – For what $a \in \mathbb{Z}$ is $p(x) = x^3 + ax + 1$ irreducible?
If p is irreducible in $\mathbb{Q}[x]$, then it has a linear factor, hence a root in $\mathbb{Q}$. By Lemma 2.70, the only possible rational roots are ± 1. $p(1) = 0 \iff 2 + a = 0 \iff a = -2$. $p(-1) = 0 \iff -a = 0 \iff a = 0$s. So p is irreducible if and only if $a \notin \{-2, 0\}$.

Lemma 2.72 (Eisenstein's criterion)
Let $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$. Let p be a prime. Suppose

1. $p \nmid a_n$,
2. p divides all other coefficients,
3. $p^2 \nmid a_0$.

Then f is irreducible.

Proof. Suppose that $f = gh$, where $g, h \in \mathbb{Z}[x]$ and $\deg g, \deg h > 0$. So, reducing these polynomials $\mod p$,

$$\overline{a_n} x^n = \overline{f} = \overline{g}\overline{h},$$

so $\overline{g} = c_1 x^k$ and $\overline{h} = c_2 x^\ell$ for some constants c_1, c_2. So $p \mid g(0)$, $p \mid h(0)$, which implies

$$p^2 \mid h(0)g(0) = f(0) = a_0,$$

a contradiction. □

Definition 2.21
A **transitive subgroup** $G \leq \mathrm{Sym}(n)$ is a subgroup such that for all $1 \leq i, j \leq n$, there exists $g \in G$ such that $g \cdot i = j$.

For example, $\langle (1 \cdots n) \rangle$ is a transitive subgroup, but $\langle (12) \rangle$ is not.

Lemma 2.73
If $f \in \mathbb{Q}[x]$ irreducible has degree d, then G_f permutes the roots of f. In fact, G_f can be naturally identified with a subgroup of $\mathrm{Sym}(\deg f)$. If α, β are roots of f in a splitting field K of f, then $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f) \cong \mathbb{Q}(\beta)$. This isomorphism extends to an isomorphism of K to itself, so G_f are transitive.

Recall that if H is a subgroup of $\mathrm{Sym}(n)$ that contains the cycles $(12), (12 \cdots n)$, then $H = \mathrm{Sym}(n)$. With this fact, we prove the following lemma.

Lemma 2.74
Let $f \in \mathbb{Q}[x]$ irreducible with prime degree p. Suppose f has exactly two non-real roots. Then $G_f \cong \mathrm{Sym}(p)$.

Proof. Let K be a splitting field of f. Let α be a root of f. $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$. Moreover, $p = [\mathbb{Q}(\alpha) : \mathbb{Q}] \mid [K : \mathbb{Q}] = |G_f|$. By Cauchy's theorem, there is $g \in G_f$ with order p, so

g is a p-cycle. Moreover, complex conjugation is an automorphism that fixes all but 2 roots, so this is a transposition, so $G_f \cong \mathrm{Sym}(p)$. □

Lemma 2.75 (Polynomial with maximal Galois group)

Let $p \geq 5$ be prime. Let n_1 be a positive even integer and $n_2, \dots, n_{p-1}$ be distinct even integers. Let $g(x) = (x^2 + n_1)(x - n_2) \cdots (x - n_{p-1}) \in \mathbb{Z}[x]$ (all coefficients are even except the leading one). Let

$$e \coloneqq \min_{x, g'(x)=0} |g(x)|.$$

Suppose n is odd such that $\frac{2}{n} < e$. Let $f(x) = g(x) - \frac{2}{n}$. Then $G_f \cong \mathrm{Sym}(p)$.

Proof. By construction, f still has $p - 2$ real roots. Then it suffices to show that f is irreducible, which is the same as showing $nf(x) = ng(x) - 2$ is irreducible. This is easy to do by Lemma 2.72. The only interesting thing to check is $4 \nmid f(0)$. Since $g(0) = c2^{p-2}$ for some $c \in \mathbb{Z}$, so $nf(0) = ng(0) - 2 = c2^{p-2} - 2$, so $4 \nmid nf(0)$. □

2.11.2. Dedekind's theorem

We will use a restated version of the Chinese remainder theorem in this proof, which is as follows. Let R be a commutative ring with maximal ideals $I_1, \dots, I_n$, then if $r_1, \dots, r_n \in R$, there exists $b \in R$ such that $b - r_i \in I_i$ for all i. Since we are working with a field $\mathbb{Q}$, it has no interesting ideals, so the idea with Dedekind's theorem is to consider the integers instead and look at its prime/maximal ideals.

Recall that a permutation $\sigma \in \mathrm{Sym}(n)$ has **cycle of type** $(k_1, \dots, k_\ell)$, where $\sum_i k_i = n$ if it is a product of disjoint cycles of length $k_1, k_2, \dots, k_\ell$. For example, $(1)(23)(456) \in \mathrm{Sym}(6)$ is a $(1, 2, 3)$-cycle.

Theorem 2.76 (Dedekind's theorem)

Let $f \in \mathbb{Z}[x]$ be monic, and let p be prime. Suppose $\overline{f}$ is separable and $\overline{f} = \prod_{i=1}^{r} f_i$ is its prime factorization. Then G_f has a cycle of type $(\deg f_1, \dots, \deg f_r)$.

Proof. Let F be a splitting field of f. Let $\alpha_1, \dots, \alpha_m$ be the roots of f. Then $F = \mathbb{Q}[\alpha_1, \dots, \alpha_m]$. We shift to looking at the ring

$$A = \mathbb{Z}[\alpha_1, \dots, \alpha_m] \subseteq \mathcal{O}_F.$$

Note that

$$\mathcal{O}_F \cong \mathbb{Z}^{[F:\mathbb{Q}]}$$

as $\mathbb{Z}$-modules. Let P be the maximal ideal of A that contains $(p) = p\mathbb{Z}$. Define $E \coloneqq A/P$, a field containing $\mathbb{F}_p$.

Given $a \in A$, let $\widetilde{a}$ be its image in E. So $E = \mathbb{F}_p[\widetilde{\alpha_1}, \dots, \widetilde{\alpha_m}]$. Since $a \mapsto \widetilde{a}$ is a ring homomorphism, $\widetilde{\alpha_i}$ is still a root of f, so E is a splitting field of $\overline{f} \in \mathbb{F}_p[x]$. Since $\overline{f}$ is separable, this extension is Galois.

Let $G = \mathrm{Gal}(E/\mathbb{F}_p)$. Define D_P to be the set of field automorphisms in G_f that fix P:

$$D_P \coloneqq \{\sigma \in G_f \mid \sigma(P) = P\} \subseteq G_f \subseteq \mathrm{Sym}(\{\alpha_1, \dots, \alpha_m\}).$$

Since $\sigma(P) = P$ if $\sigma \in D_p$, it descends to a ring homomorphism $\widetilde{\sigma} \colon E \to E$.

So there exists a group homomorphism

$$\begin{aligned}\phi\colon D_P &\to \mathrm{Gal}(E/\mathbb{F}_p) = \langle \sigma_p \colon x \mapsto x^p \rangle \\ \sigma &\mapsto \widetilde{\sigma}\end{aligned}$$

Moreover, it is injective because each $\sigma \in D_P$ permutes the roots, so if $\phi(\sigma) = \mathrm{id}_E$, then $\sigma = \mathrm{id}_F$.

Claim 2.6. ϕ is an isomorphism.

Proof. By the primitive element theorem, $E = \mathbb{F}_p[\widetilde{a}]$ for some $a \in A$. By the Chinese remainder theorem, there exists $b \in A$ such that $b - a \in P$ and for all $\sigma \notin D_p$, $b \in \sigma(P) \implies \sigma^{-1}(b) \in P \implies \widetilde{\sigma(b)} = 0$. Hence, $\widetilde{a} = \widetilde{b}$. Let

$$h(x) \coloneqq \sum_{\sigma \in G_f} (x - \sigma(b)) \in \mathbb{Z}[x].$$

So

$$\underbrace{\overline{h}(x)}_{\in \mathbb{F}_p[x]} = \sum_{\sigma \in G_f} (x - \widetilde{\sigma(b)}) = x^{|G_f - D_p|} \overbrace{\sum_{\sigma \in D_p} (x - \widetilde{\sigma(b)})}^{\deg \le |D_p|}.$$

Notice that if $m_{\widetilde{b}}(x) \in \mathbb{F}_p[x]$ is the minimal polynomial of $\widetilde{b}$, then

$$|\mathrm{Gal}(E/\mathbb{F}_p)| = [E : \mathbb{F}_p] = \deg m_{\widetilde{b}} \le |D_p| \le |\mathrm{Gal}(E/\mathbb{F}_p)|. \qquad \blacksquare$$

To finish the proof, note that the Frobenius automorphism $\sigma_p\colon x \mapsto x^p$ cyclically permutes the roots of f_i for all i. So the corresponding element in D_p has a cycle of type $(\deg f_1, \dots, \deg f_n)$. $\square$

Example 2.77 – Find $G_f \subseteq \mathrm{Sym}(5)$, where $f(x) = x^5 - x - 1$.

- f reduces $\bmod 2$ to $\overline{f} = (x^2 + x + 1)(x^3 + x^2 + 1)$. This implies G_f has a $(2,3)$-cycle. Up to renaming elements, we can write it as $(12)(345)$.
- Suppose f is reducible $\bmod 3$. Then its reduction, $\overline{f} \in \mathbb{F}_3[x]$ has a linear or quadratic factor. The product of all degree 1 and 2 irreducible polynomials in $\mathbb{F}_3[x]$ is $x^{3^2} - x$ by Corollary 2.28. Since $\gcd(x^5 - x - 1, x^9 - x) = 1$, there are no quadratic or linear factors. This implies G_f has a 5-cycle.

$((12)(345))^3 = (12)$, so G_f has a transposition and a 5-cycle. Hence, $G_f = \mathrm{Sym}(5)$.

2.12. Insolvability of the quintic

November 30, 2023

Recall that $N \trianglelefteq \mathrm{Gal}(F/k) \iff N/k$ is Galois. We may generalize this to a descending normal sequence.

Corollary 2.78

$1 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq \mathrm{Gal}(F/k)$ has a bijection to $F \supseteq F_1 \supseteq \cdots \supseteq k$, where F_{i+1}/F_i is Galois.

Lemma 2.79 (Linear independence of characters, Dedekind)
Let G be a group and let F be a field. A **character of** G is a group homomorphism $\chi\colon G \to F^\times$. If distinct characters $\chi_1, \dots, \chi_n$ satisfy $\sum_{i=1}^n a_i\chi_i = 0$ (as a function), and $a_1, \dots, a_n \in F$, then $a_1 = \cdots = a_n = 0$.

Proof. Induct on n. $n = 1$ is clear. Let $g \in G$ such that $\chi_1(g) \neq \chi_i(g)$ for some i. Suppose that $\sum_i a_i\chi_I(x) = 0$. Then

$$\sum_i a_i\chi_i(gx) = 0 \implies \sum_i a_i\chi_i(g)\chi_i(x) = 0.$$

By multiplying by $\chi_1(g)^{-1}$, we have

$$a_1\chi_1(x) + a_2\chi_1(g)^{-1}\chi_2(g)\chi_2(x) + \cdots + a_n\chi_1(g)^{-1}\chi_n(g)\chi_n(x) = 0.$$

Now take the difference of this with $\sum_{i=1}^n a_i\chi_i = 0$ to find

$$a_2(\chi_1(g)^{-1}\chi_2(g) - 1)\chi_2(x) + \cdots + a_n(\chi_1(g)^{-1}\chi_n(g) - 1)\chi_n(x) = 0.$$

So $a_2 = \cdots = a_n = 0$ by the inductive hypothesis. So $a_1\chi_1 = 0 \implies a_1 = 0$ as well. □

Lemma 2.80
Let $n > 0$. Suppose k is a field with a primitive nth root of unity. Let F/k be a degree n Galois extension. Then $\mathrm{Gal}(F/k) \cong \mathbb{Z}/n \iff F = k(\alpha)$ where $\alpha \in F$ such that there is an $a \in k$ such that $\alpha^n = a$, but $\alpha^m \notin k$ for $0 < m < n$.

Proof. ($\implies$) Let $\mathrm{Gal}(F/k) = \langle\sigma\rangle$.

Claim 2.7. It suffices to find $\alpha \in F$ such that $\sigma(\alpha) = \zeta^{-1}\alpha$.

> **Proof.** Note that $\sigma^2(\alpha) = \sigma(\zeta^{-1}\alpha) = \zeta^{-2}\alpha$ and $\sigma^m(\alpha) = \zeta^{-m}\alpha$. So σ^m sends α to itself if and only if $n \mid m$, i.e. only the identity in $\mathrm{Gal}(F/k)$ fixes α. So $F = k(\alpha)$. Moreover, $\deg m_\alpha = n$. Roots of m_α are $\sigma^m(\alpha) = \zeta^{-m}\alpha$, so
>
> $$m_\alpha = \prod_{i=1}^{n-1}(x - \zeta^i\alpha) = x^n - \alpha^n \in k[x].$$
>
> So $\alpha^n \in k$. No smaller α^m is in k because $\deg m_\alpha = n$. ■

Notice that $F^\times$ is a group and $\sigma^k\colon F^\times \to F^\times$ are distinct characters for $0 \leq k \leq n-1$. Therefore, $\sum_{i=0}^{n-1} \zeta^i\sigma^i$ is not the zero function. Suppose therefore that γ is some input so that

$$\alpha = \gamma + \zeta\sigma(\gamma) + \cdots + \zeta^{n-1}\sigma^{n-1}\gamma \neq 0.$$

Therefore,

$$\sigma(\alpha) = \sigma(\gamma) + \zeta\sigma^2(\gamma) + \cdots + \zeta^{n-1}\gamma = \zeta^{-1}\alpha.$$

($\impliedby$) Suppose $F = k(\alpha)$, where $\alpha = \sqrt[n]{a}$ for $a \in k$. Moreover, suppose $\alpha^m \notin k$ for any $0 < m < n$. Since F/k is a degree n extension, $\deg m_\alpha = n$, so $m_\alpha = x^n - a$. The roots of m_α are $\zeta^i\alpha$. Let $\sigma \in \mathrm{Gal}(F/k)$ such that $\sigma(\alpha) = \zeta\alpha$. Then $\sigma^2(\alpha) = \zeta^2\alpha \neq \alpha$.

Similarly, we see that $\sigma^m(\alpha) = \alpha \iff n \mid m$. So the order of σ is n, so σ generates the Galois group. □

Definition 2.22

A group G is **solvable** if there exists $1 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq G$ such that N_{i+1}/N_i is cyclic or, equivalently in this case, abelian.

Proposition 2.81

Quotients and subgroups of solvable groups are solvable.

Example 2.82 (Nonexamples of solvable groups) – A_n and $\mathrm{Sym}(n)$ are not solvable for $n \geq 5$.

Definition 2.23

A **radical tower starting at** k_1 is $k_1 \subseteq \cdots \subseteq k_m$ such that $k_{i+1} = k_i(\sqrt[n_i]{a_i})$ for $a_i \in k_i$. A polynomial $f \in k[x]$ is **solvable by radicals** if there exists a radical tower starting at k such that all roots of f belong to k_m.

Theorem 2.83 (Galois solvability theorem)

Let $f \in k[x]$, where k is a characteristic zero field. Let K be a splitting field of f over k. Let $G_f \coloneqq \mathrm{Gal}(K/k)$. Then G_f is solvable $\iff$ f is solvable by radicals.

Proof. ($\implies$) Let $N = (\deg f)!$. Let ζ be a primitive Nth root of unity. Let $F = k(\zeta)$. Let L be a splitting field of f over F.

Claim 2.8. $\mathrm{Gal}(L/F)$ is solvable, since it can be identified with a subgroup of $\mathrm{Gal}(K/k)$.

Proof. Let $\alpha_1, \ldots, \alpha_m$ be roots of f in L. So $K = k(\alpha_1, \ldots, \alpha_m)$. So $\mathrm{Gal}(L/F)$ permutes the roots of f, so each element of $\mathrm{Gal}(L/F)$ sends K to itself. This gives us a restriction

$$\begin{array}{ccc} \mathrm{Gal}(L/F) & \xrightarrow{\text{Res}} & \mathrm{Gal}(K/k) \\ & \searrow & \downarrow \\ & & \mathrm{Sym}(\text{roots of } f) \end{array}$$

■

Because $\mathrm{Gal}(L/F)$ is solvable, there exists sequence

$$1 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_m = \mathrm{Gal}(L/F),$$

which is in bijection with

$$L \supseteq F_1 \supseteq \cdots \supseteq F_m = F = K(\zeta) \supseteq K$$

such that N_{i+1}/N_i is cyclic. Then applying Lemma 2.80, f is Solvable by radicals.

($\Longleftarrow$) By assumption, K is contained in the final field of a radical tower. It suffices to show that $K \subseteq E$ where E is a Galois extension of k such that $\mathrm{Gal}(E/k)$ is solvable, because $G_f = \mathrm{Gal}(K/k) = \mathrm{Gal}(E/k)/\mathrm{Gal}(E/K)$, and quotients of solvable groups are solvable.

$K \subseteq K(\alpha_1) \subseteq \cdots \subseteq K(\alpha_1, \ldots, \alpha_m) =: L$, where $\alpha_i = \sqrt[r_i]{a_i}$ with a_i in the ith field in the sequence. Let E be the splitting field of $m_\alpha(x)(x^N - 1)$, where $N = r_1 \cdots r_m$.

Let $G = \mathrm{Gal}(E/k) = \{g_1, \ldots, g_\ell\}$.

$$K \overset{\text{ab.}}{\subseteq} K(\zeta_N) \overset{\text{cyc.}}{\subseteq} K(\zeta_N, \alpha_1) \overset{\text{cyc.}}{\subseteq} K(\zeta_N, g_1(\alpha_1), \alpha_1) \overset{\text{cyc.}}{\subseteq} \cdots \overset{\text{cyc.}}{\subseteq} K(\zeta_N, \overbrace{g_1(\alpha_1), \ldots, \gamma_\ell(\alpha_1)}^{G\cdot\alpha_1})$$
$$\overset{\text{cyc.}}{\subseteq} K(\zeta_N, G\cdot\alpha_1, \alpha_2) \overset{\text{cyc.}}{\subseteq} \cdots \overset{\text{cyc.}}{\subseteq} K(G\cdot\alpha_1, G\cdot\alpha_2) \overset{\text{cyc.}}{\subseteq} \cdots \overset{\text{cyc.}}{\subseteq} K(G\cdot\alpha_1, \ldots, G\cdot\alpha_m) = E.$$

As a result, K is solvable. □

Example 2.84 – We showed that $f(x) = x^5 + x + 1$ has $G_f = \mathrm{Sym}(5)$, so its roots are not expressible by adjoining successive roots to $\mathbb{Q}$.

Remark 2.85. There is a real analytic function that inputs coefficients of a quintic and outputs its roots.

2.13. The Artin-Schreier theorem

December 5, 2023

We would like to be able to say more about the algebraic closure of a field beyond "it exists and is unique." The following theorem establishes a classification of algebraic closures for field with characteristic zero and finite degree closures, with the prototypical example being $\overline{\mathbb{R}} = \mathbb{C}$.

Theorem 2.86 (Artin-Schreier)
Let k be a field with characteristic 0. If the algebraic closure F of k is a finite extension of k, then $[F : k] = 2$ and $F = k(i)$.

Most of the work was done on the worksheet through the following lemma:

Lemma 2.87
Suppose that $F = \overline{k}$ is a degree p extension for a prime p over a characteristic 0 field L. Then $p = 2$.

Proof. The following sequence of claims will prove that $p = 2$.

Claim 2.9. $\zeta_p \in L$.

Proof. $[L(\zeta_p) : L] = \deg m_{\zeta_p} \leq \deg \Phi_p = p - 1 < p$. Since F is a Galois extension of degree p, $\mathrm{Gal}(F/L) \cong \mathbb{Z}/p$. The only proper subfield of F contained in L is L, so $L(\zeta_p) = L$. ■

Note that by Lemma 2.80, $F = L(\sqrt[p]{a})$ for some $a \in L$. Let b be an element such that $b^p = \sqrt[p]{a}$. The Galois conjugates of b are some roots of $x^{p^2} - a = 0$, so we have a form for any $\sigma \in \mathrm{Gal}(F/L)$.

Claim 2.10. Let $\sigma(b) = \zeta_{p^2}^m b$ for some integer m. Then $\zeta_{p^2}^{mn} \sqrt[p]{a} \in L$ for some n. Moreover, $p \nmid m$.

Proof. Let $\sigma(\zeta_{p^2}) = \zeta_{p^2}^{\ell}$ for some integer ℓ. Then by induction, we can show that $\sigma^k(b) = \zeta_{p^2}^{(*)m} b$, where $*$ is some integer. The constant term of $m_b \in L[x]$ is the product of the Galois conjugates of b, i.e.

$$\zeta_{p^2}^{m \cdot n} b^p = \zeta_{p^2}^{m \cdot n} \sqrt[p]{a}.$$

Suppose $p \mid m$. Write $m = kp$, so

$$\underbrace{\left(\zeta_{p^2}^{p}\right)^{kn}}_{\in L} \cdot \sqrt[p]{a} \in L \implies \sqrt[p]{a} \in L,$$

a contradiction. ■

Claim 2.11. $\sigma(\zeta_{p^2}) = \zeta_{p^2} \zeta_p^c$ for some integer c.

Proof. Since $\zeta_p \in L$, $\sigma \in \mathrm{Gal}(F/L)$ fixes ζ_p. Let $\sigma(\zeta_{p^2}) = \zeta_{p^2}^{\ell}$ for some $\ell \in \mathbb{Z}$. Then

$$\zeta_p = \sigma(\zeta_p) = \sigma(\zeta_{p^2}^p) = \sigma(\zeta_{p^2})^p = \zeta_{p^2}^{p\ell} = \zeta_p^{\ell}.$$

Hence, ℓ is congruent to 1 modulo p, from which the result follows. ■

Let p be an *odd* prime. Then $p \mid 1 + 2 + \cdots + (p-1)$. Therefore,

$$b = \sigma^{p-1} \circ \sigma^{p-2} \circ \cdots \circ \sigma(b) = \zeta_{p^2}^{p-1} \zeta_p^{(*)} b,$$

a contradiction. □

We now continue to the proof of Artin-Schreier.

Proof of Theorem 2.86. By the previous lemma, we just need to prove that the degree of the extension is always of degree 2. Let $G = \mathrm{Gal}(F/k)$. Suppose $p \mid |G|$. Then G contains a subgroup $H := \langle x \rangle$ of size p. Let $L = \mathrm{Fix}_H(F)$. F is the algebraic closure of L and $[F : L] = [H : \{\mathrm{id}\}] = p$. So $p = 2$ and $|G| = 2^k$ for some k.

For contradiction, we suppose $k \geq 2$. If $|G| \neq 2$, then either there is an $x \in G$ such that $\mathrm{ord}(x) = 4$ and $H = \langle x \rangle \cong \mathbb{Z}/4$, or there do not exist $x \in G$ that are of order 4, hence every element is of order 2, so $G \cong (\mathbb{Z}/2)^k$ and we can find a subgroup $H \leq G$ such that $H \cong (\mathbb{Z}/2)^2$. As a result, we have found an order 4 subgroup.

Let L be the fixed field of H. There exists an intermediate field E (by the Galois correspondence) such that $L \subseteq E \subseteq F$, and $[L : E] = [E : F] = 2$. By the lemma, $F = E(i)$. Let $M = L(i)$. Applying the lemma again, $F = M(i) = L(i)(i) = L(i) = M$. But F is a degree 4 extension and M is a degree 2 extension over L, a contradiction. So $|G| = 2$, and by the lemma, $F = K(i)$. □

2.14. Jordan-Chevalley

December 7, 2023

We now cover the final theorem of this class, which brings together ideas from module theory and field theory together to solve an issue we faced before: Jordan canonical form did not work when the eigenvalues did not belong to the field the vector space was over.

Definition 2.24

Let $U, W \subseteq V$ be k-vector spaces. Then $V = U \oplus W$ if any of the equivalent definitions hold.

1. $\forall v \in V$, there exists unique $u \in U$, $w \in W$ such that $v = u + w$,
2. $V = U + W$ and $U \cap W = \{0\}$,
3. $V = U + W$ and $\dim U + \dim W = \dim V$.

Definition 2.25

Let k be a field and V a finite dimensional k-vector space. Let $A \colon V \to V$ be a linear map. A is **semisimple** if for all A invariant subspaces $W \subseteq V$, there exists an A-invariant subspace $U \subseteq V$ such that V decomposes as $V = W \oplus U$.

A is **simple** if the only A-invariant subspace are 0 and V. Note that V is simple implies A is simple (hence semisimple).

We will now discuss several equivalent definitions of semisimple, which we will use to prove the Jordan-Chevalley theorem.

Lemma 2.88

Let $V = k[x]/(p^n)$ where $p \in k[x]$ is prime and $n \in \mathbb{Z}_{>0}$. Let $A \colon V \to V$ be given by $A(f) = xf$. Then A is semisimple $\iff n = 1$.

Proof. A-invariant subspaces of V are $k[x]$-submodules, i.e. $I/(p^n)$ where $I \subseteq k[x]$ is an ideal that contains (p^n). $I = (q)$ for some $q \implies q \mid p^n \implies q = p^k$ for $0 \leq k \leq n$.

If $n = 1$, there exist two invariant subspaces, so A is simple. If $n > 1$, $(p)/(p^n)$ is a proper invariant subspace that contains all other invariant subspaces. So there is not a complementary subspace. □

Lemma 2.89 (Semisimple restriction)

Let $A \colon V \to V$ be semisimple. Let $W \subseteq V$ be A-invariant. Then $A|_W$ is semisimple.

Proof. Let $V = W \oplus U$, where W, U are A-invariant, be the decomposition guaranteed by the definition of semisimple. Let $W_1 \subseteq W$ be A-invariant. Since A is semisimple, there exists W_2 such that $V = (W_1 \oplus U) \oplus W_2$. Let

$$\pi_W \colon V \to W$$

be the **projection onto** W. Then $W = \pi_W(V) = W_1 + \pi_W(W_2)$. To show this is a direct sum,

$$\dim W = \dim W_1 + \dim W_2 \geq \dim W_1 + \dim \pi_W(W_2),$$

which implies equality, so $W = W_1 \oplus \pi_W(W_2)$. □

Lemma 2.90

Let $A \colon V \to V$. Then A is semisimple $\iff V = \bigoplus_i V_i$, where each V_i are A-invariant and simple.

Proof. Induct on $\dim V$.

($\implies$) Let A be semisimple. If V is semisimple, we are done. Otherwise, write $V = W_1 \oplus W_2$ for A-invariant subspaces W_1, W_2 and $A|_{W_i}$ is semisimple. By induction, $V = \bigoplus_i W_{1i} \oplus \bigoplus_j W_{2j}$.

($\impliedby$) If V is simple, then we are done. Let

$$V = V_1 \oplus \underbrace{W}_{=\bigoplus_{i>0} V_i},$$

where V_1 is A-invariant and simple and W is A-invariant. Let $U \subseteq V$ be an A-invariant subspace. Let U' be an A-invariant complement of $\pi_W(U)$ in W, so $W = \pi_W(U) \oplus U'$.

If $U \cap V_1 = 0$, then the invariant complement is just $V_1 \oplus U'$. If $U \cap V_1 = V_1$, then the invariant complement is U'. □

Lemma 2.91

Let $A \colon V \to V$. A is semisimple $\iff$ its minimal polynomial is squarefree.

Proof. By the elementary divisor theorem, as a $k[x]$-module,

$$V = \bigoplus_i \underbrace{k[x]/(p_i^{e_i})}_{=:V_i}$$

for prime polynomials p_i and integers $e_i > 0$. A is semisimple $\iff$ $A|_{V_i}$ is semisimple for all i $\iff$ $e_i = 1$ $\iff$ m_A is squarefree. □

Definition 2.26

A field k is **perfect** means if $\operatorname{char}(k) = p$, then either $p = 0$ or $p > 0$ and for all $a \in k$, there exists $b \in k$ such that $a = b^p$.

Recall if k is perfect, then any irreducible polynomial is separable. Equivalently, $p \in k[x]$ is squarefree $\iff$ p is separable. Moreover, any splitting field L/k over a perfect field k is Galois.

Example 2.92 – Given $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \colon \mathbb{Q}^2 \to \mathbb{Q}^2$. But $A_{\mathbb{R}} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \colon \mathbb{R}^2 \to \mathbb{R}^2$ and $A_{\mathbb{C}} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \colon \mathbb{C}^2 \to \mathbb{C}^2$ also are well-defined maps. We summarized before the *extension of scalars* that we can perform: if $A \colon V \to V$ is a linear map of k-vector spaces and L/k is a field extension, then $A_L \coloneqq A \otimes_k \mathrm{id}$ is a linear map from $V_L \coloneqq V \otimes_k L$ to itself given by the same matrix.

Lemma 2.93

Let k be perfect and let V be a k-vector space. Let $A\colon V \to V$. The following are equivalent:

1. A is semisimple,
2. $m_A \in k[x]$ is squarefree,
3. m_A is separable.

If L/k is a field extension then A_L is semisimple $\iff$ A is semisimple.
If L/k contains the splitting field of m_A, A is semisimple $\iff$ A_L diagonalizable.

Definition 2.27

Let $A\colon V \to V$. A is **nilpotent** if there exists $m > 0$ such that $A^m = 0$.

Lemma 2.94

1. If $A, B\colon V \to V$ that commute with each other and are both semisimple (resp. nilpotent), then $A + B$ is semisimple (resp. nilpotent),
2. The only semisimple and nilpotent linear map is 0.

Proof. (1) For semisimplicity, there exists a field L/k such that A_L and B_L are diagonalizable. Commuting diagonalizable matrices are simultaneously diagonalizable. For nilpotency, suppose there exists N such that $A^N = B^N = 0$. Then by the binomial theorem,

$$(A+B)^{2N} = \sum_{i+j=2N} \binom{2N}{i} A^i B^j = 0.$$

(2) If A is semisimple and nilpotent, then there is a field L/k such that A_L is diagonalizable. But the only diagonalizable and nilpotent matrix is 0. □

Theorem 2.95 (Jordan-Chevalley)

Let k be perfect and let V be a k-vector space. Let $A\colon V \to V$ be a linear map. Then there exist *unique* polynomials $p, q \in k[x]$ such that A decomposes into a sum of a semisimple and nilpotent map.

$$A = \underbrace{p(A)}_{\text{semisimple}} + \underbrace{q(A)}_{\text{nilpotent}}.$$

Remark 2.96. Recall in Jordan canonical form, we wrote a matrix A, up to conjugation,

as

$$BAB^{-1} = \begin{bmatrix} \lambda_1 & 1 & & & & & & \\ & \ddots & \ddots & & & & & \\ & & \ddots & 1 & & & & \\ & & & \lambda_1 & & & & \\ & & & & \lambda_2 & 1 & & \\ & & & & & \ddots & \ddots & \\ & & & & & & \ddots & 1 \\ & & & & & & & \lambda_2 \\ & & & & & & & & \ddots \end{bmatrix} = \underbrace{\begin{bmatrix} \lambda_1 & & & & & & & \\ & \ddots & & & & & & \\ & & \ddots & & & & & \\ & & & \lambda_1 & & & & \\ & & & & \lambda_2 & & & \\ & & & & & \ddots & & \\ & & & & & & \lambda_2 & \\ & & & & & & & \ddots \end{bmatrix}}_{\text{semisimple}} + \underbrace{\begin{bmatrix} 0 & 1 & & & & & & \\ & \ddots & \ddots & & & & & \\ & & \ddots & 1 & & & & \\ & & & 0 & & & & \\ & & & & 0 & 1 & & \\ & & & & & \ddots & \ddots & \\ & & & & & & \ddots & 1 \\ & & & & & & & 0 \\ & & & & & & & & \ddots \end{bmatrix}}_{\text{nilpotent}}.$$

Proof of Theorem 2.95. We first show uniqueness. Suppose $p(A) + q(A) = \widetilde{p}(A) + \widetilde{q}(A)$. Then $\underbrace{p(A) - \widetilde{p}(A)}_{\text{semisimple}} = \underbrace{q(A) - \widetilde{q}(A)}_{\text{nilpotent}}$. The only semisimple and nilpotent linear map is 0 (exercise), so $p(A) = \widetilde{p}(A)$ and $q(A) = \widetilde{q}(A)$.

Let L be a splitting field of m_A. This is a Galois extension. Then by Jordan canonical form, we can write

$$A_L = \begin{bmatrix} \lambda_1 & 1 & & & & & & \\ & \ddots & \ddots & & & & & \\ & & \ddots & 1 & & & & \\ & & & \lambda_1 & & & & \\ & & & & \lambda_2 & 1 & & \\ & & & & & \ddots & \ddots & \\ & & & & & & \ddots & 1 \\ & & & & & & & \lambda_2 \\ & & & & & & & & \ddots \end{bmatrix}$$

Let $\chi_A = \prod_i (x - \lambda_i)^{d_i} \in L[x]$. Then $V_L = \bigoplus_i V_i$, where $V_i = \ker\left((A_L - \lambda_i I)^{d_i}\right)$. By the Chinese remainder theorem, there exists a polynomial $p(x) \in L[x]$ such that $p(x) \cong \lambda_i \bmod (x - \lambda_i)^{d_i}$ for all i. Equivalently, we can write $p(x) = \lambda_i + g_i(x)(x - \lambda_i)^{d_i}$ for some $g_i \in L[x]$ for all i.

Let $v \in V_i$. $p(A) \cdot v = \lambda_i v + g_i(A_L)(A_L - \lambda_i I)^{d_i} \cdot v = \lambda_i v$. So $p(A)$ is diagonalizable. Define $g(x) = x - p(x)$. $g(A)^{d_i} = (A_L - p(A)|_{V_i})^{d_i} = (A_L - \lambda_i I)^{d_i} \cdot v = 0$, so $g(x)$ is nilpotent. Moreover, $A_L = p(A_L) + g(A_L)$.

We need to prove that $p(x)$ (which we defined to be in $L[x]$) actually has coefficients in k. Let $\sigma \in \mathrm{Gal}(L/k)$. Note $A = p(A) + q(A)$. Note $A \in \mathrm{Mat}_{\dim V \times \dim V}(k)$, so $A^\sigma = A$.

$$A = A^\sigma = \underbrace{p(A)^\sigma}_{\text{semisimple}} + \underbrace{q(A)^\sigma}_{\text{nilpotent}} = p^\sigma(A) + q^\sigma(A).$$

By uniqueness, $p^\sigma(A) = p(A)$ and $q^\sigma(A) = q(A)$. By the classification of $L[x]$ modules, we have

$$V_L \cong \bigoplus_i L[x]/(d_i),$$

where $d_1 \mid \cdots \mid d_m$ are the invariant factors, where A acts by multiplication by x. So $p(A)$ acts by multiplication by $p(x)$. But multiplication by $p(x)$ is multiplication by $p^\sigma(x)$, so $p(x) = p^\sigma(x)$ and $q(x) = q^\sigma(x)$ for all $\sigma \in \mathrm{Gal}(L/k)$. So $p, q \in k[x]$. □

References

[DF03] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2003.