Math 494 Notes

Kellen Kanarios

October 15, 2023

Abstract

This is a compilations of all of my notes for Math 494. The course is taught by Professor Andrew Snowden.

Contents

Chapter 1

Ring Theory

Lecture 1: First Lecture

4 Jan. 02:00

1.1 Rings

Definition 1.1.1 (Ring). A ring is a set R with two binary operations $+$ (addition) and $\cdot$ (mult) such that

(1) $(R, +)$ is an abelian group

- identity element 0,
- additive inverse of x, which is $-x$.

(2) $(R, \cdot)$ is a monoid:

- Multiplication is associative,
- There exists an identity element 1.

(3) Distributive law

$$x \cdot (y + z) = x \cdot y) + (x \cdot z)$$
$$(y + z) \cdot x = (y \cdot x) + (z \cdot x).$$

Definition 1.1.2 (Commutative Ring). A ring is called commutative if multiplication is commutative.

Example. Consider the following examples:

- $\mathbb{Z}$ is a ring,
- $\mathbb{Z}[x]$ i.e. polynomial w/ $\mathbb{Z}$ coefficients,
- Any field is a ring,
- If R is a ring then $M_n(R)$ is a ring (non-commutative in general),
- The zero ring $R = \{0\}$.
  - Not a field,
  - If $1 = 0$ in R then $R = 0$.

Remark. If R is any commutative ring then $R[x] = \{\text{polys in var } x \text{ with coefficients in } R\}$ is a commutative ring. Can also do $R[x_1, \ldots, x_n]$.

Exercise. The following are homework exercises:

- $x \cdot 0 = 0$, for every $x \in R$,
- $(-1) \cdot x = -x$.

1.2 Ring Homomorphisms

Definition 1.2.1 (Ring Homomorphism)**.** Let R, S be rings. Then a ring homomorphism $f : R \to S$ is a function such that

(1) $f(x + y) = f(x) + f(y)$,

(2) $f(x \cdot y) = f(x) \cdot f(y)$,

(3) $f(1) = 1$.

Note. If $f(x) = 0$ for every x then f is compatible with (1) and (2) but $f(1) \neq 1$ unless $S = 0$.

Exercise. Why do we require $f(1) = 1$?

Answer. It gives us the following useful properties:

- An element x of a ring R is called a unit if it is invertible under multiplication i.e. $\exists! y \in R$ such that $xy = yx = 1$.
- The set $R^{\times}$ of units is a group under multiplication.
- If $f : R \to S$ is a ring homomorphism it induces a group homomorphsim $f : R^{\times} \to S^{\times}$.

$\circledast$

Example. The following are examples of ring homomorphisms:

- $id_R : R \to R$,
- For any R, $\exists!$ ring homomorphism $R \mapsto 0$,
  - 0 is a final object in category of rings.
- For any R, $\exists!$ ring homomorphism: $\mathbb{Z} \to R$ defined by $n \mapsto \underbrace{1 + \cdots + 1}_{n\text{times}}$.
  - $\mathbb{Z}$ is the initial object in the category of rings.
- $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ quotient map,
- $\mathbb{C} \to \mathbb{C}$ defined by $x \mapsto \overline{x}$.

Remark. In the theme of category theory,

- In groups, the trivial group is initial and final object,
- The category of fields have no initial or final object.

Example. Let R be a commutative ring. Then there exists a ring homomorphism $R[x] \to R$ defined by $a_0 + a_1 x + \cdots + a_n x^n \mapsto a_0 + \cdots + a_n$. More generally, if $c \in R$, then we get a ring homomorphism

$R[x] \to R$ defined by $\phi \mapsto \phi(c)$.

Proposition 1.2.1 (Mapping property for polynomial rings)**.** Let R, S be commutative rings. Giving a ring homomorphism $\phi : R[x] \to S$ is the same as giving $\phi_0 : R \to S$ and $c \in S$

$$\begin{aligned} \phi_0 &= \phi|_R \\ c &= \phi(x). \end{aligned}$$

Basic Idea. Given $\phi_0 : R \to S$ and $c \in S$ we define $\phi : R[x] \to S$ by $\phi\left(\sum_{i=1}^n a_i x^i\right) = \sum_{i=1}^n \phi_0(a_i)c^i$. Check that this is a well-defined ring homo and inverse to the construction $\phi \mapsto (\phi_0, c)$. ■

Another Explanation. Given $\phi_0 : R \to S$ and $c \in S$.

$$R[x] \mapsto S[x] \mapsto S,$$

where

$$\sum a_i x^i \mapsto \sum \phi_0(a_i) x^i.$$

■

Remark. $R[x, y] \cong R[x][y]$.

Definition 1.2.2 (Kernel)**.** Let $f : R \to S$ be a ring homomorphism. The kernel of f is $f^{-1}(0)$.

Remark. The following are familiar and useful facts:

- The kernel is an additive subgroup of R.
- f is injective if and only if $\ker(f) = 0$.

Lemma 1.2.1. If $x \in \ker(f)$ and $y \in R$, then $xy \in \ker(f)$.

Proof.

$$\begin{aligned} f(xy) &= f(x)f(y) \\ &= 0 \cdot f(y) \\ &= 0. \end{aligned}$$

■

Definition 1.2.3 (Ideal)**.** An ideal of R is an additive subgroup $I \subset R$ that is closed under multiplication:

$$a \in R, b \in I \Rightarrow ab \in I.$$

Remark. In non-commutative case, we have left, right, and 2-sided ideals.

Example. The kernel of a ring homomorphism is an ideal.

Proposition 1.2.2. The converse of the previous example is also true.

Proof. Suppose $I \subset R$ is an ideal. Can consider R/I (as an abelian group). Define a multiplication on R/I by

$$(a+I)(b+I) = ab + I.$$

Note. It is important that I is an ideal because

$$(a+I)(b+I) = (a+x)b + I.$$

We need $bx \in I$ for this multiplication to be well-defined. This is okay because I is an ideal.

This makes R/I a commutative ring. The quotient $\pi : R \to R/I$ is a ring homomorphism, where $\ker(\pi) = I$. ■

Lecture 2: Second Lecture

6 Jan. 02:00

Definition 1.2.4 (Subring)**.** Let R be a ring. A subgring of R is a subset S that is closed under addition and multiplication and contains 1.

Note. Ideals are closed under $+$ and $\cdot$, but usually not subrings (Do not contain 1). If they do contain 1 then it is the whole ring.

Definition 1.2.5 (Generated Subring)**.** Let R be a ring, $X \subset R$ is a subset of R. The subring of R generate by X is the smallest subring of R containing X i.e. $\bigcap\limits_{\substack{X \subset S \\ S \text{ subring}}} S$.

Example. The Gaussian integers.

$$\begin{aligned}\mathbb{Z}[i] &= \text{subring of } \mathbb{C} \text{ generated by } i = \sqrt{-1} \\ &= \{a + bi \mid a, b \in \mathbb{Z}\}.\end{aligned}$$

Example. $R = \mathbb{C}[x, y]$, $X = \mathbb{C} \cup \{x^2, xy, y^2\}$. Subring generated by X is all polynomials in x, y with coefficients in $\mathbb{C}$ in which all monomials $x^i y^j$ have $i + j$ even.

Remark. This is known as a Veronese subring of R.

Note. The following is a surjective ring homomorphism.

$$\begin{aligned}\mathbb{C}[T_1, T_2, T_3] &\to S \\ T_1 &\mapsto x^2 \\ T_2 &\mapsto xy \\ T_3 &\mapsto y^2.\end{aligned}$$

Remark. If R is a ring and I is an ideal of R then $R\,/\,I$ naturally has the structure of a ring called quotient ring. Some properties are

1. Mapping property

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[d, "\pi"'] & S \\ R/I \arrow[ur, dashed, "\psi"] & \end{tikzcd}$$

where π is the quotient map. Given ϕ such that $I \subset \ker(\phi)$ $\exists!\psi$ such that $\phi = \psi \circ \pi$.

2. Corr. theorem for ideals

$$\{\text{ideals of } R/I\} \longleftrightarrow \{\text{ideals of } R \text{ containing } I\}.$$

3. 1st isomorphism theorem: If $\phi : R \to S$ is a surjective homo of rings then ϕ induces an isomorphism

$$\overline{\phi} : R/\ker\phi \to S.$$

Definition 1.2.6 (Generated Ideals). Given a ring R and elements $f_1, \dots, f_n \in R$ the ideal of R generated by $f_1, \dots, f_n$ is

$$(f_1, \dots, f_n) = \{g_1 f_1 + \cdots + g_n f_n \mid g_1, \dots, g_n \in R\}.$$

An ideal I is called principle if $I = (f)$ for some $f \in R$.

Example. Consider the following examples:

1. Every ideal of $\mathbb{Z}$ is principle,
2. If F is a field, every ideal of $F[x]$ is principle,
3. Every ideal of $\mathbb{Z}[i]$ is princple,
4. The ideal (x, y) of $F[x, y]$ is not principle.

Definition 1.2.7 (Presentation of ring). A presentation of a ring R is an isomorphism,

$$Z[x_1, \dots, x_n]/(f_1, \dots, f_m) \cong R,$$

where $f_1, \dots, f_m \in \mathbb{Z}[x_1, \dots, x_n]$.

Remark. More generally, a (finite) presentation of R relative to a ring S is an isomorphism

$$S[x_1, \dots, x_N]/(f_1, \dots, f_m) \cong R.$$

Example. Presentation for $\mathbb{Z}[i]$.

$$\mathbb{Z}[x]/x^2+1 \xrightarrow{\phi} \mathbb{Z}[i].$$

1. There exists the ring map $\tilde{\phi} : \mathbb{Z}[x] \to \mathbb{Z}[i]$ defined by $x \mapsto i$.
2. $\tilde{\phi}(x^2 + 1) = i^2 + 1 = 0 \Rightarrow (x^2 + 1) \subset \ker(\tilde{\phi})$

3. Mapping property for quotients $\Rightarrow$ there exists a ring homomorphism
$$\phi \cdot \mathbb{Z}[x] \big/ (x^2+1) \to \mathbb{Z}[i]$$
such that $\phi(\overline{x}) = i$.
4. Clear that $\tilde{\phi}$ and therefore ϕ is surjective.
5. Every element of $\mathbb{Z}[x] \,/\, (x^2+1)$ has the form $a\overline{x} + b$ for $a, b \in \mathbb{Z}$ i.e.
$$x^5 = x^5 - x^3(x^2+1) + x^3(x^2+1) \Rightarrow \overline{x}^5 = -\overline{x}^3.$$
Say $a\overline{x} + b \in \ker(\phi)$. Then
$$\phi(a\overline{x} + b) = ai + b = a = b = 0 \Rightarrow \ker(\phi) = 0.$$

Definition 1.2.8 (Integral domain)**.** A commutative ring R is an (integral) domain if

- $xy = 0 \Rightarrow x = 0$ or $y = 0$,
- $1 \neq 0 \in R$.

Example. The following are examples of domains:

- Any field is a domain,
- $\mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[x], \mathbb{Q}[x]$,
- $\mathbb{Z}/6\mathbb{Z}$.

Remark. Every domain embeds into a field.

Definition 1.2.9 (Fraction field)**.** Given a domain R. Define a field $\mathrm{Frac}(R)$ (fraction field of R). An element is an equivalence class of pairs a, b, where $a, b \in \mathbb{R}$ and $b \neq 0$. We say $(a, b) \sim (a', b')$ if $ab' = a'b$.

Notation. Write $\frac{a}{b}$ for the class (a, b).

Then
$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + ba'}{bb'}, \quad \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}.$$
There exists an injective ring homomorphism
$$\begin{aligned} R &\to \mathrm{Frac}(R) \\ a &\mapsto \frac{a}{1}. \end{aligned}$$

Example. Examples of fraction fields:

- $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$,
- $\mathrm{Frac}(\mathbb{Q}[x]) = \mathbb{Q}(x)$,

Example. $R = \mathbb{C}[x, y] \,/\, (y - x^3 - x)$. This is a domain. $\mathrm{Frac}(R)$ is a field. This field, we have $\mathbb{C}(x) \subset \mathrm{Frac}(R)$. $y^2 = x^3 + x \in \mathrm{Frac}(R)$.

Lecture 3: Third Lecture

6 Jan. 02:00

Remark. Recall example. For any ring R, we can consider $R[x]/(x^2+1)$.

Example. $R = \mathbb{F}_7$, $7 \equiv 3 \bmod 4 \Rightarrow -1$' is not a square in $\mathbb{F}_7$. Put $E = \mathbb{F}_7[x] \,/\, (x^2+1)$.

Claim. E is a field, $\#E = 49$. ($E = \mathbb{F}_{49}$)

Proof. Let $j =$ img of x in E. (Note: $j^2 = -1$) Then every element of $\mathbb{F}_7$ uniquely has the form $a + bj$ for $a, b \in \mathbb{F}_7$. This implies that $\#E = 49$ because it is 2-dimensional.

$$\frac{1}{a+bj} = \frac{1}{a+bj} \cdot \frac{a-bj}{a-bj} = \frac{a-bj}{a^2+b^2}.$$

Note. The key point is that $a^2 + b^2 \neq 0$. This is because if $a^2 + b^2 = 0$ then $a^2 = -b^2 \Rightarrow \left(\frac{a}{b}\right)^2 = -1$

Therefore, $\frac{a-bj}{a^2+b^2}$ is a well defined element of E and is the inverse of $a + bj$. ■

Example. Let $R = \mathbb{C}$, $E = \mathbb{C}[x] \,/\, (x^2+1)$, $j =$ img of x in E satisfying $j^2 = -1$. Every element of E can be written uniquely as $a + bj$ for $a, b \in \mathbb{C}$. (i.e. $1, j \in E$ form a basis of E as a $\mathbb{C}$-vector space).

$$x^2 + 1 = (x+i)(x-i) \text{ holds in } \mathbb{C}[x].$$

From our map to E ,

$$(j+i)(j-i) = 0.$$

Since $j + i, j - i \neq 0$, E is not a domain. In fact, $E \cong \mathbb{C} \times \mathbb{C}$[a].

[a] In general, if A and B are ring then $A \times B$ is a ring with component wise operations known as the product ring

First try. Consider the map defined by $(1,0) \mapsto 1$ and $(0,1) \mapsto j$. This does not work because $(1,1) \mapsto 1 + j$ and we need $(1,1) \mapsto 1$. ■

Remark. Think about $A \times B$ having elements $e = (1,0)$ and $f = (0,1)$. Following properties

- $e^2 = e$, $f^2 = f$, [a]
- $ef = 0$,
- $e + f = 1$.

In general, if R is a ring, e, f are idempotents such that $ef = 0$, $e + f = 1$. Then $R \cong A \times B$ where $A = eR$[b], $B = fR$.

[a] We say e, f are idempotents
[b] Is not a subring because it does not have the identity element

Correct Approach. Look at $(1 + ij)$. Note that

$$\begin{aligned}(1+ij)^2 &= 1 + 2ij + (ij)^2 \\ &= 2(1+ij).\end{aligned}$$

Then,

$$\left(\frac{1+ij}{2}\right)^2 = \left(\frac{1+ij}{2}\right).$$

Therefore, $\underbrace{\frac{1+ij}{2}}_{e}$ and $\underbrace{\frac{1-ij}{2}}_{f}$ are idempotents of E and $ef = 0$ and $e+f = 1$. These give the decomposition, $E = \underbrace{eE}_{\mathbb{C}} \times \underbrace{fE}_{\mathbb{C}}$. ■

Remark (More generally). Let R be any commutative ring. Let $h(u) \in R[u]$ be a monic polynomial:

$$h(u) = u^n + a_{n-1}u^{n-1} + \cdots + a_0, \qquad a_0, a_{n-1} \in R.$$

Consider $E = R[u] \,/\, (h(u))$. E is obtained by "adjoining a root of h" to R.

Proposition 1.2.3. Every element of E can be written uniquely as $b_0 + b_1 u + \cdots + b_{n-1}u^{n-1}$ for $b_0, \ldots, b_{n-1} \in R$. In other words, $E \underbrace{\cong}_{\text{not as a ring}} R^n$ with an interesting multiplication.

Note. When h is not monic things can be more complicated. Consider $h(u) = au - 1$. Then $E = R[u] \,/\, (h(u))$ is often denoted $R[\frac{1}{a}]$.

Example. Let $R = \mathbb{Z}$, $a = 2$. Consider $\mathbb{Z}[\frac{1}{2}]$. This is isomorphic to the subring of Q consisting of elements $\frac{a}{b}$, where $b = 2^k$ for some $k \in \mathbb{Z}$.

Example (More generally). If R is a domain, then $R[\frac{1}{a}]$ is the subring of $\mathrm{Frac}(R)$, consisting of elements $\frac{x}{a^n}$ with $x \in R$, $n \in \mathbb{N}$.

Example. $R = \mathbb{Z}$, $a = 1$, $E = \mathbb{Z}[u] \,/\, (u-1)$. Then

$$\begin{aligned} \mathbb{Z} \to {}^{\mathbb{Z}[u]}\big/_{(u-1)} &\to \mathbb{Z} \\ u &\mapsto 1. \end{aligned}$$

Therefore, if a is a unit, $R[\frac{1}{a}] = R$.

Example (Maximal degeneracy). Let $E = R[\frac{1}{0}]$. Then $E = 0$ because $h(u) = -1$ is a unit, the ideal $(h(u))$ is all of R.

Example. Let $R = \mathbb{Z}/6\mathbb{Z}$, $a = 3$. Then $R[\frac{1}{3}] = \mathbb{Z}\,/\,2\mathbb{Z}$. Note

$$\begin{gathered} {}^{\mathbb{Z}}\big/_{6\mathbb{Z}} \cong {}^{\mathbb{Z}}\big/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\big/_{3\mathbb{Z}} \\ 3 \mapsto (1, 0) \\ {}^{\mathbb{Z}}\big/_{3\mathbb{Z}}[\frac{1}{0}] = 0 \\ {}^{\mathbb{Z}}\big/_{2\mathbb{Z}}[\frac{1}{1}] = {}^{\mathbb{Z}}\big/_{2\mathbb{Z}}. \end{gathered}$$

Thus,

$$\mathbb{Z}/_{6\mathbb{Z}[\frac{1}{3}]} = \mathbb{Z}/_{2\mathbb{Z}}.$$

Lecture 4: Fourth Lecture

6 Jan. 02:00

Definition. Let R be a commutative ring.

Definition 1.2.10 (Multiplicative Set)**.** A multipliative set in R is a subset S such that $1 \in S$ and $x, y \in S \Rightarrow xy \in S$

Definition 1.2.11 (Localization)**.** Given a multiplicative set $S \subset R$, the localization $S^{-1}R$ is

$$R\left[\frac{1}{s}\right]_{s \in S}.$$

Remark. This is the iterated version of $R\left[\frac{1}{a}\right]$ from last time.

Example. R is a domain, $0 \notin S$. Then $S^{-1}R$ is the subring of $\mathrm{Frac}(R)$ consisting of elements $\frac{x}{s}$ with $x \in R$ and $s \in S$.

Example. Let $R = \mathbb{Z}$, fix prime p. $S =$ all integers coprime to P. Then $S^{-1}R$ is subring of $\mathbb{Q}$ of fractions with denominator prime to p.

Problem 1.2.1. What are the ideals of $\mathbb{Z}_{(p)}$?

Answer. The ideals are (p^n) for $n \geq 0$. ⊛

Remark. $\mathbb{Z}_{(p)} \subset \mathbb{Z}_p$. More specifically, $\mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q}$.

As previously seen. $\mathbb{F}_7[x] / (x^2+1)$ is a field with 49 elements.

Problem 1.2.2. When is R / I a field? What does this say about I?

Answer. When I is a maximal ideal. ⊛

Definition 1.2.12. A maximal ideal of a ring R is a proper ideal that is not strictly contained in any other proper ideal.

Lemma 1.2.2. A ring is a field if and only if it has exactly two ideals: $(0), (1)$.

Proof.

$\Rightarrow$ Say F is a field and $I \subset F$ is a non-zero ideal. Let $x \neq 0 \in I$ then $xx^{-1} = 1 \in I$. Thus, $I = (1)$.

$\Leftarrow$ Say F is a ring with exactly two ideals (0) and (1). Say $x \in F$ is non-zero. Then (x) is not zero, so it must be (1). Therefore, $\exists y$ such that $xy = 1$, so $y = x^{-1}$ and F is a field. ∎

Proposition 1.2.4. Let R be a commutative ring and $I \subset R$ be an ideal. I is maximal if and only if $R\,/\,I$ is a field.

Proof. Ideal correspondence theorem:

$$\underbrace{\{\text{ ideals of } R \text{ containing } I\ \}}_{\text{Has two elements iff } I \text{ maximal}} \leftrightarrow \underbrace{\{\text{ideals of } {}^{R}\big/_{I}\ \}}_{\text{Has two elements if and only if } R\,/\,I \text{ is a field}}.$$

■

Problem 1.2.3. What are max ideals of $\mathbb{Z}$?

Answer. Every ideal of $\mathbb{Z}$ has the form (n) for some n. However, $\mathbb{Z}\,/\,n\mathbb{Z}$ is a field if and only if n is prime. Therefore, the max ideals are

$$\{(p) \mid p \text{ is prime}\}.$$

⊛

Example. $R = \mathbb{Q}\,[x]$.

$$\mathbb{Q}\,[i]\big/(x^2+1) = \underbrace{\mathbb{Q}\,[i]}_{\{a+bi \mid a,b\in\mathbb{Q}\}} = \underbrace{\mathbb{Q}(i)}_{\text{Smallest sub field of } \mathbb{C} \text{ containing } i}.$$

Therefore, (x^2+1) is a max ideal of $\mathbb{Q}[x]$.

Remark (Generalized Chinese Remainder Theorem)**.**

$$\mathbb{Q}[x]\Big/\big((x^2+1)(x-1)\big) \cong \mathbb{Q}[x]\big/(x^2+1) \times \mathbb{Q}[x]\big/(x-1).$$

This is not a field, so ideal is not maximal.

Proposition 1.2.5. Let R be a ring. $I \subset R$ is a proper ideal, then there exists a maximal ideal J of R such that $I \subset J$.

Sketch. Define

$$\Sigma \coloneqq \{\text{ all proper ideals } J \text{ such that } I \subset J\ \}.$$

Want to show that Σ has a maximal element. Suppose $J_1 \subset J_2 \subset \cdots$ is a chain in Σ. Put $J = \bigcup_{i=1}^{\infty} J_i$. J is proper because if not then $1 \in J$ which implies $1 \in J_i$ for some i and J_i is not proper. Now from Zorn's lemma, there exists a maximal element of Σ. ■

Problem 1.2.4. Consider $R = \mathbb{C}\,[x_1, \ldots, x_n]$. What are the maximal ideals?

Answer. The following are maximal ideals:

- $(x_1, \ldots, x_n)$ is maximal because $R\,/\,(x_1, \ldots, x_n) \cong C$.
- Given $a \in \mathbb{C}^n$, then $J_a = (x_1 - a_1, \ldots, x_n - a_n)$ because $R\,/\,(x_1 - a_1, \ldots, x_n - a_n) \cong C$.

This is actually all of them from the theorem. ⊛

Theorem 1.2.1. Every max ideal of R is one of the J_a's.

Proof. Let $J =$ max ideal of R, $K = R \,/\, J$ is a field. Then

$$\mathbb{C} \hookrightarrow R \to K$$

composite is injective because $\mathbb{C}$ is a field. $\mathbb{C} \subset K$. Note that $\dim_{\mathbb{C}} R$ is countable, so the same is true for K. $\dim_{\mathbb{C}} \mathbb{C}(x)$ is uncountable:

$$\left\{ \frac{1}{x-a} \mid \alpha \in \mathbb{C} \right\}$$

are $\mathbb{C}$-linearly independent. If $\mathbb{C} \subset K$ then $\exists a \in K \,/\, C$ and $\mathbb{C}(a) \cong \mathbb{C}(x)$ (using $\mathbb{C}$ is algebraically closed). Contradicts dimension count. Therefore, $K = \mathbb{C}$.

$$\begin{aligned} J &= \ker(R \to {}^{R}\!\big/_{J} = \mathbb{C}) \\ x_i &\mapsto a_i \\ J &= J_a \\ &. \end{aligned}$$

■

Problem 1.2.5. What fields contain $\mathbb{C}$ as a subfield?

Answer. $\mathbb{C}$, $\mathbb{C}(x)$, $\mathbb{C}(x_1, \ldots, x_n)$. ⊛

Remark.

Lecture 5: Fifth Lecture

6 Jan. 02:00

Claim. Let $R = \mathbb{C}[x_1, \ldots, x_n,\ a \in \mathbb{C}^n,\ J_a = (x_1 - a_1, \ldots, x_n - a_n)$. Consider the ring homomorphism $ev_a : R \to \mathbb{C}$ defined by $f \mapsto f(a)$. Then $J_a = \ker(ev_a)$

Proof. For the containment $J_a \subset \ker(ev_a)$ it is clear. For the reverse containment, change of variables to reduce to $a = 0$ (think about monomials) note

$$R = \mathbb{C}[x_1, \ldots, x_n] = \mathbb{C}[x_1 - a_1, \ldots, x_n - a_n].$$

■

Proposition 1.2.6. The J_a's give all max ideals of R.

Proof. Let $J \subset R$ be a max ideal. Last time $R \,/\, J \cong \mathbb{C}$. Consider the map

$$\phi : R \to {}^{R}\!\big/_{J} = \mathbb{C}.$$

Let $a_i = \phi(x_i) \in \mathbb{C}$. Since $J_a \subset \ker(\phi)$, $J_a = \ker(\phi)$ because J_a is maximal. ■

Remark. Let $f \in R$. From the above claim, $f \in J_a \Leftrightarrow f(a) = 0$. Additionally, we know that $(f) \subset J_a \Leftrightarrow f \in J_a$ Consider the set

$$\{z \in \mathbb{C}^n \mid f(z) = 0\} \subset \mathbb{C}^n.$$

This set is naturally in bijection with the set of maximal ideals of $\underbrace{{}^{R}\!\big/_{(f)}}_{\text{the max ideals here are } J_a \text{ with } (f) \subset J_a}$.

Example. $n = 2$, $f = x_1^2 + x_2^2 - 1$.

$$\{z \mid f(z) = 0\}.$$

Complex points of unit circle correspond to max ideals of $\mathbb{C}[x_1, x_2] \,/\, (x_1^2 + x_2^2 - 1)$

Remark. Let R be a ring. Define $\operatorname{MaxSpec}(R)$[a] $= \{\text{max ideals of } R\}$. For $x \in \operatorname{MaxSpec}(R)$ write $m_x \subset R$ for corresponding maximal ideal. We also have the quotient field $\kappa_x = R \,/\, m_x$. For each $x \in \operatorname{MaxSpec}(R)$ define $f(x) \in \kappa_x$ to be the image of f.

[a]Carries a natural topology

Example. Given an ideal I, $V(I) = \{x \in \operatorname{MaxSpec} \mid I \subset m_x\}$. If $R = \mathbb{C}[x_1, \ldots, x_n]$, $I = (f)$, then

$$V(I) = \{J_a \mid f(a) = 0\}.$$

The $V(I)$'s are exactly the closed sets of $\operatorname{MaxSpec}(R)$.

Remark. If the ring is a domain, then the topology is not Hausdorff.

Proposition 1.2.7. $R = \mathbb{C}[x_1, \ldots, x_n]$. Let $f_1, \ldots, f_r \in R$. Then the following are equivalent:

(a) $(f_1, \ldots, f_r) = (1)$,

(b) $\{z \in \mathbb{C}^n \mid f_1(z) = \cdots = f_r(z) = 0\} = \emptyset$

Proof. Suppose (a) is true. Then $1 = \sum_{i=1}^r g_i f_i$. Given $z \in \mathbb{C}^n$, $1 = \sum_{i=1}^r g_i(z) f_i(z)$, so not all $f_i(z)$ vanish. Now suppose $\neg$(b). Assume $(f_1, \ldots, f_r) \neq (1)$. Then $(f_1, \ldots, f_r)$ is contained in a maximal ideal. This max ideal is some J_a with $a \in \mathbb{C}^n$. Then for every i, $f_i \in J_a$ and $f_i(a) = 0$. ∎

Chapter 2

Factorization

Theorem 2.0.1 (Fundamental Theorem of Arithmetic)**.** If n is a non-zero integer, $\exists$ factorization

$$n = \pm p_1 \cdots p_r,$$

where p_i is prime. This is unique up to permuting the p_i's.

Problem 2.0.1. Is there an analog of this in more general rings?

Answer. Sometimes... ⊛

Example. The following are some examples:

1. $F[x]$, F is a field. In this case, there is a theory of unique factorization.
2. Also true for $F[x_1, \ldots, x_n]$.
3. $\mathbb{Z}[i]$ has a unique factorization.
4. $\mathbb{Z}[\sqrt{-5}]$. Not true: $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$

Problem 2.0.2. In $\mathbb{Z}$, $6 = 2 \cdot 3 = (-2) \cdot (-3)$. Why do we have a unique factorization for $\mathbb{Z}$.

Answer. Because the factorizations differ by units. ⊛

Remark. From here on, R is a domain. For $x, y \in R$, we say that x divides y written $x|y$, if $y = wx$ for some $w \in R$ ($\Leftrightarrow y \in (x) \Leftrightarrow (y) \subset (x)$).

Lemma 2.0.1. If $x|y$ and $y|x$ then $x = u \cdot y$ for a unit u.

Proof. $x = uy$, $y = vx$ for some $u, v \in R$. Therefore,

$$x = uvx \Rightarrow x(1 - uv) = 0 \overset{x \neq 0}{\Rightarrow} 1 - uv = 0 \Rightarrow uv = 1.$$

Thus, u, v are units. ■

Definition 2.0.1. We say x and y are associates if $x = uy$ for some unit u.

Definition 2.0.2. An element π of R is irreducible if ($\pi \neq 0, \pi \neq$ unit)

$$\pi = xyx = \text{unit or } y = \text{unit}.$$

Example. The following are a few examples:

(1) $R = \mathbb{Z}$ irreducible elements are $\pm$ primes.

(2) $R = F[x]$ with F as a field are irreducible polynomials.

Definition 2.0.3 (Unique Factorization Domain)**.** A unique factorization domain is a domain R such that $\forall 0 \neq x \in R$, there exists a factorization

$$x = \pi_1 \cdots \pi_r$$

with π_i irreducible and it is unique in the sense that if

$$x = \pi_1' \cdots \pi_s'$$

then $r = s$ and there exists a permutation σ such that $\pi_i \sim \pi_{\sigma(i)}'$.

Lecture 6: Sixth Lecture

18 Jan. 02:00

Remark. If R is a commutative ring and $I, J \subset R$ are ideals then

$$IJ = \text{ideal generated by } ab \text{ with } a \in I, b \in J.$$

Remark. Say R is a domain. To be a UFD, we need two things:

(1) Every element factors into irreducibles.

(2) This factorization is approximately unique.

Problem 2.0.3. When can (1) fail?

Answer. $\mathbb{C}[x_1, x_2, \ldots]$. This fails because all polynomials only use finitely many variables. In fact, this ring is a UFD. ⊛

Answer. $R =$ continuous functions : $[-1, 1] \to \mathbb{C}$ with

- Addition = pointwise addition.
- Multiplication = poinwise multiplication.

This is a commutative ring but is not a domain. ⊛

Answer. $R =$ analytic functions : $\mathbb{R} \to \mathbb{C}$.

- Addition = pointwise addition.
- Multiplication = poinwise multiplication.

This is a domain. Consider $\sin(x)$. Then

$$\begin{aligned}\sin(x) &= x \cdot \frac{\sin(x)}{x} \\ &= x \cdot (x - 2\pi) \cdot \frac{\sin(x)}{x(x-2\pi)} \cdots \\ .\end{aligned}$$

Up to associates, the irreducible elements of S are $x - a$, $a \in \mathbb{R}$. (1) seems to fail here? ⊛

Answer. Consider $S = \mathbb{C}[x^{\frac{i}{2^k}}]_{i \le k}$. Then

$$S = \mathbb{C}[y_0, y_1, y_2, \dots] \Big/ (y_i^2 - y_{i-1}).$$

Then

$$\begin{aligned} x &= x^{\frac{1}{2}} \cdot x^{\frac{1}{2}} \\ &= x^{\frac{1}{2}} \cdot x^{\frac{1}{4}} \cdot x^{\frac{1}{4}} \cdots . \end{aligned}$$

⊛

Proposition 2.0.1. Let R be a ring. The following are equivalent:

(1) Ideals of R satisfy the ascending chain condition (ACC) i.e. If $I_1 \subset I_2 \subset \cdots$ are ideals, then there exists an n such that

$$I_n = I_{n+1} = \cdots .$$

(2) Every ideal is finitely generated.

Proof.

(b) $\Rightarrow (a)$. Consider $I_1 \subset I_2 \subset \cdots$. Put $J = \bigcup_{n=1}^{\infty} I_n$. This is an ideal. By (b), J is finitely generated. Therefore $J = (a_1, \dots, a_r)$ for some $a_1, \dots, a_r \in R$. Since there exists an n such that $a_1, \dots, a_r \in I_n$, $J \subset I_n$. So $I_n = I_{n+1} = \cdots = J$.

$\neg(b) \Rightarrow \neg(a)$ Let J be an ideal that is not finitely generated. Pick $a_1 \in J$. Then $(a_1) \subset J$. Note $(a_1) \neq J$ because J is not finitely generated. Now pick $a_2 \in J$ (a_1) then $(a_1, a_2) \subset J$, which is also strict. Continuing we get,

$$(a_1) \not\subset (a_1, a_2) \not\subset \cdots .$$

Thus, (a) fails. ■

Definition 2.0.4. A commutative ring R is noetherian if (a) and (b) hold.

Remark. This is a very important idea!

Example. A PID is noetherian. (b) holds because it is generated by one thing.

Proposition 2.0.2. Let $R =$ noetherian domain. Let $x_1, x_2, \dots, \in R$ be elements such that

$$x_2 | x_1, x_3 | x_2, \dots .$$

Then there exists an n such that $x_n \underbrace{\sim}_{\text{associate}} x_{n+1} \sim x_{n+2} \cdots$

Proof. Note $x|y \Leftrightarrow (y) \subset (x)$. We have

$$(x_1) \subset (x_2) \subset (x_3) \cdots .$$

Since (ACC) holds, there exists an n such that $(x_n) = (x_{n+1}) = \cdots$. Thus, $x_n \sim x_{n+1} \sim \cdots$. ■

Proposition 2.0.3. If R is a noetherian domain then every element factors into irreducibles.

Proof. Let $x \in R$ be given. Say $x \neq 0$, unit.

Claim. x is divisible by some irreducible element.

Proof. Follows from previous proposition. ∎

Now, choose irreducible $\pi_1 | x$. Write $x = \pi_1 x_2$. Now choose $\pi_2 | x_2$. Then $x = \pi_1 \pi_2 x_3$. Process stops by previous proposition. ∎

Remark. Say $p \geq 2$ is an integer. The following are equivalent:

(a) If $p = xy$ then $x = \pm 1$ or $y = \pm 1$.

(b) $p | xy \Rightarrow p | x$ or $p | y$.

In a general ring, (a) leads to idea of irreducible element and (b) leads to the idea of a prime element.

Definition 2.0.5 (Prime element)**.** Suppose R is a domain, $\pi \neq 0$, unit. We say π is prime if $\pi | xy \Rightarrow \pi | x$ or $\pi | y$

Remark. Prime elements are always irreducible.

Proof. Say π is prime. If $\pi = xy$ then $\pi | xy \Rightarrow \pi | x$ or $\pi | y$, so $\pi \sim x$ or $\pi \sim y$. ∎

Proposition 2.0.4. Let R be a domain in which all elements have irreducible factorzations. Then the following are equivalent:

(a) R is a UFD.

(b) All irreducible elements are prime.

Proof.

(b) $\Rightarrow (a)$ Say $x = \pi_1 \cdots \pi_r = \pi'_1 \cdots \pi'_s$ are two factorizations of x. Since π_r divides x, it divides $\pi'_1 \cdots \pi'_s$. Since π_r is prime, there exists an i such that $\pi_r | \pi'_i$, so $\pi_r \sim \pi'_i$. Now cancel π_r and π'_i. Continue by induction we now have fewer factors.

(a) $\Rightarrow (b)$ Let π be irreducible. We need to show

$$\pi \not| x, \pi \not| y \Rightarrow \pi \not| xy.$$

Let x, y with irreducible factorizations

$$x = \sigma_1 \cdots \sigma_r$$
$$y = \sigma'_1 \cdots \sigma'_s.$$

Then

$$xy = \sigma_1 \cdots \sigma_r \sigma'_1 \cdots \sigma'_s.$$

Since π doesn't appear and this is the only irreducible factorization of xy, $\pi \not| xy$ because R is a UFD.

∎

Lecture 7: Seventh Lecture

20 Jan. 02:00

As previously seen. We talked about UFD's namely

- If R is noetherian then every element factors into irreducibles.
- If R has factorization into irreducibles then R is a UFD iff all irreducible elements are prime.

Theorem 2.0.2. Every PID is a UFD

Proof. Let R be a PID. R is noetherian because every ideal is generated by one element (and therefore finitely generated). Let π be an irreducible element. Then we need to show that π is prime. Say $\pi | xy$. Consider the ideal (π, x). Since R is a PID, there exists some $a \in R$ such that $(\pi, x) = (a)$. Since $\pi \in (a)$, $a|\pi$. Since π is irreducible, there are two cases:

Case 1: a is associate to π

Since $x \in (a)$, $a|x$, so $\pi|x$.

Case 2: a is a unit.

Then $(\pi, x) = (1)$. Therefore, $\exists u, v \in R$ such that $u\pi + vx = 1$. It follows that

$$u\pi y + vxy = y.$$

Since π divides π and π divides x, π divides y.

■

Remark. In any domain, we can define the notion of a gcd:

$$d \text{ is a gcd of } x \text{ and } y \text{ if } d|x \text{ and } d|y, \text{ and } (e|x \text{ and } e|y \Rightarrow e|d).$$

Remark. gcd's always exists in a UFD but we don't always have Bézout.

Remark. In a PID, do get Bézout i.e.

$$(x, y) = (d) \Leftrightarrow d = \gcd(x, y).$$

Definition 2.0.6. R is a domain. A Euclidean function on R is a function

$$\phi : R \setminus \{0\} \longrightarrow \{0, 1, 2, \dots\}$$

such that the following version of the division algorithm holds:

- Given $x, y \in R$, $y \neq 0$, $\exists q, r \in R$ with $q \neq 0$ such that $x = yq + r$ and either $\phi(r) < \phi(y)$ or $r = 0$.

Definition 2.0.7. A Euclidean domain is a domain with a Euclidean function.

Proposition 2.0.5. Every Euclidean domain is a PID.

Proof. Let $I \subset R$ be a non-zero ideal. Pick $y \in I$ with $\phi(y) \neq 0$ minimial.

Claim. $I = (y)$

Proof. Let $x \in I$ be given. Write $yq + r$, where $r = 0$ or $\underbrace{\phi(r) < \phi(y)}_{\text{not possible by choice of } y}$. Note $r \in I$ because

$$r = \underbrace{x}_{\in I} - \underbrace{yq}_{\in I}.$$

■

From the claim, it follows that I is principle. ■

Example. $\mathbb{Z}$ is a Euclidean domain. $\phi(x) = |x|$.

Example. If F is a field then $F[x]$ is a Euclidean ring with $\phi(f) = \deg(f)$.

Example. $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ is a Euclidean domain, with $\phi(a + bi) = a^2 + b^2$.

Reason. Say $x, y \in \mathbb{Z}[i]$, $y \neq 0$. Let $q \in \mathbb{Z}[i]$ be nearest Gaussian integer to $\frac{x}{y}$ i.e. $\frac{x}{y} = q + \epsilon$. Then $x = qy + \underbrace{\epsilon y}_{r}$. Therefore,

$$\phi(r) = \phi(\epsilon)\phi(y) < \phi(y) \text{ because } \phi(\epsilon) < 1.$$

Note:

$$\epsilon = \alpha + i\beta \text{ and } |\alpha|, |\beta| \leq \frac{1}{2},$$

so $\phi(\epsilon) = \alpha^2 + \beta^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$. ■

Example. $\omega = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}$ 3rd root of 1. Then

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

ring of Einstein integers. This is a Euclidean function $\phi(z) = |z|^2$ integer because

$$\phi(a + b\omega) = a^2 - ab + b^2.$$

Example. The ring of integers in $\mathbb{Q}(\sqrt{d})$ for $d \in \mathbb{Z}$ is

$$R_d = \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{if } d = 2, 3 \bmod (4) \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}], & \text{if } d = 1 \bmod (4) \end{cases}.$$

The definition is

$$R_d = \{x \in \mathbb{Q}(\sqrt{d}) \mid \exists \text{monic } f \in \mathbb{Z}[T] \text{ such that } f(x) = 0\}.$$

There is a norm

$$N(x + y\sqrt{d}) = x^2 - dy^2.$$

Remark. The following are some facts:

(1) R_{-1}, R_{-3} are Euclidean ($\Rightarrow$ PID $\Rightarrow$ UFD)

(2) R_{-5} is not a UFD $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$

(3) R_{-19} is a PID, but not Euclidean.

(4) R_{69} is Euclidean, not norm-Euclidean (N not Euclidean)

(5) For R_d, PID iff UFD.

(6) $\exists$ exactly 9 $d < 0$ such that R_d is a PID.

(7) Unknown if $\exists\infty$ many $d > 0$ such that R_d is a PID.

(8) If $d < 0$ then $R_d^\times$ is finite. For $d > 0$, $R_d^\times$ is $\mathbb{Z}$ or $Z \times \mathbb{Z}/2$

$$x^2 - dy^2 = 1 \qquad \text{(Pell's Equation)}.$$

Solutions are units of R_d.

Lecture 8: Eighth Lecture

23 Jan. 02:00

Remark. For $x \in \mathbb{Z}[i]$, put $N(x) = x\overline{x}$ (norm). If $x = a + bi$ then $N(x) = a^2 + b^2$ is a non-negative integer. Also:

$$N(xy) = N(x) \cdot N(y).$$

Remark. $x \in \mathbb{Z}[i]$ is a unit iff $N(x) = 1 \Leftrightarrow x \in \{\pm 1, \pm i\}$.

Reason. If x is a unit then

$$xy = 1 \Rightarrow N(x)N(y) = 1 \Rightarrow N(x) = 1.$$

If $N(x) = 1$ then

x $\overline{x} = 1 \Rightarrow x$ is a unit. ■

Corollary 2.0.1. The units are $\{\pm 1, \pm i\}$

Reason. $1 = N(a + bi) = a^2 + b^2$. ■

Remark. If π is a Gaussian prime then π divides an (ordinary) prime number.

Reason. π divides $N(\pi) = \pi \cdot \overline{\pi}$. Since $N(\pi)$ is an integer, it factors into primes i.e.

$$N(\pi) = p_1 \cdots p_r.$$

Since π is prime, π divides some p_i. ■

Remark (Strategy to understand Gaussian primes)**.** Factor ordinary primes in $\mathbb{Z}[i]$.

Example.

$$\begin{aligned} 2 &= 1^2 + 1^2 = N(1+i) \\ 2 &= \underbrace{(1+i)(1-i)}_{\text{associates}} \\ &= -i(i+1)^2. \end{aligned}$$

Thus,

$$N(1+i) = 2 \Rightarrow 1 + i \text{ is prime}.$$

Remark. If $\pi \in \mathbb{Z}[i]$ has prime norm then π is a Gauss prime.

Reason. If $\pi = xy$ then $N(\pi) = N(x) \cdot N(y)$. Therefore,

$$N(x) = 1 \quad \text{or} \quad N(y) = 1.$$

Thus,

$$x \text{ or } y \text{ is a unit.}$$

■

Note. If $n \in \mathbb{Z} \subset \mathbb{Z}[i]$. Then $N(n) = n^2$.

Example. 3 is prime because if $3 = xy$ then $9 = N(x) \cdot N(y)$. Therefore, $N(x) = 3$. However, this implies that $3 = a^2 + b^2$ which is not possible.

Example. $5 = \underbrace{(2+i)(2-i)}_{\text{prime b/c } N \text{ is prime}}$ (not associates).

Remark.

$$\begin{aligned} 3 \text{ is prime } &\Leftrightarrow (3) \text{ is maximal} \\ &\Leftrightarrow \text{no ideals above } (3) \text{ except } (1). \end{aligned}$$

From previous example,

$$5 = (2+i)(2-i) \Leftrightarrow (5) \text{ is contained in (2 + i) and (2 - i).}$$

Remark (General Strategy). Given a prime number p. Try to find ideals of $\mathbb{Z}[i]$ containing (p). By ideal forrespondence theorem, these correspond to ideals of $\mathbb{Z}[i] \,/\, p\mathbb{Z}[i]$.

Problem 2.0.4. What does $\mathbb{Z}[i] \,/\, p\mathbb{Z}[i]$ look like?

Answer.

$$\mathbb{Z}[i] \big/ p\mathbb{Z}[i] \cong \mathbb{Z}[x] \big/ (p, x^2+1) \cong \mathbb{F}_p[x] \big/ (x^2+1).$$

⊛

Note ($p = 2$). When $p = 2$, $(x^2+1) = (x+1)^2$. Therefore, $x+1$ is nilpotent in $\mathbb{F}_2[x] \,/\, (x^2+1)$. You only see nilpotent elements when $p = 2$. Note

$$\mathbb{F}_2[x] \big/ (x^2+1) \cong \mathbb{F}_2[y] \big/ (y^2),$$

where $y = x + 1$.

Remark (Key point). If $x^2 + 1$ has a root in $\mathbb{F}_p$

Case 1: If it does not, then x^2+1 is an irreducible polynomial in $\mathbb{F}_p[x]$ Therefore, it generates a maximal ideal such that $\mathbb{F}_p[x] \,/\, (x^2+1)$ is a field and p is prime in $\mathbb{Z}[i]$.

Case 2: If it does let α be the root. Then $-\alpha$ is also a root and $\alpha \neq -\alpha$ because p is odd.

Therefore, $x^2+1=(x+\alpha)(x-\alpha)$. Thus,

$$\mathbb{F}_p[x]\Big/(x^2+1) \overset{\text{CRT}}{\cong} \mathbb{F}_p[x]\Big/(x+\alpha) \times \mathbb{F}_p[x]\Big/(x+\alpha) \cong \mathbb{F}_p \times \mathbb{F}_p.$$

Therefore, there exists two ideals strictly between (p) and (1) in $\mathbb{Z}[i]$. Thus, p factors as a product of two distinct primes.

Note. To determine which case we're in, we need to know if x^2+1 has a root in $\mathbb{F}_p$ i.e. if -1 is a square in $\mathbb{F}_p$

Proposition 2.0.6. If p is an odd prime, then -1 is a square in $\mathbb{F}_p$ iff $p \equiv 1 \bmod 4$

Proof. Recall $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. If $p \equiv 3 \bmod 4$ then $\mathbb{F}_p^\times$ has order $p-1 \equiv 2 \bmod 4$. If $p \equiv 1 \bmod 4$ then $4|_{p-1} \Rightarrow \mathbb{F}_p^\times$ has an element of order 4, its a $\sqrt{-1}$. ■

Remark (Summary)**.** Let p be a prime.

(a) $p=2$, $2=-i(1+i)^2$

(b) $p \equiv 1 \bmod 4$, $p=\pi_1\pi_2$ in $\mathbb{Z}[i]$. In fact, $\pi_2=\overline{\pi_1}$. Note if $\pi=a+bi$

$$\begin{aligned} p &= \pi \cdot \overline{\pi} \\ p &= a^2+b^2. \end{aligned}$$

Thus, p is a sum of two squares iff $p \equiv 1 \bmod 4$.

(c) $p \equiv 3 \bmod 4$, p is a Gauss prime.

Lecture 8: Ninth Lecture

25 Jan. 02:00

Definition 2.0.8. A number field is a subfield of $\mathbb{C}$ that is finite dimensional as a $\mathbb{Q}$-vector space.

Definition 2.0.9. An algebraic number is a complex number that is a root of a polynomial with rational coefficients.

Remark. If K is a number field then every element is an algebraic number.

Proof. Given $x \in K$, $1, x, x^2, x^3, \ldots \in K$. Since K is finite dimensional this list is linearly dependent over $\mathbb{Q}$. Then x satisfies the polynomial constructed by their linearly dependent relation. ■

Remark. If R is a subring of $\mathbb{C}$ containing $\mathbb{Q}$ and finite dimensional as a $\mathbb{Q}$-vector space then R is a field.

Proof. Let $x \in R$ be non-zero. Consider

$$\begin{aligned} m_x : R &\longrightarrow R \\ a &\longmapsto m_x(a) = xa. \end{aligned}$$

This is a $\mathbb{Q}$-linear map. It is injective because R is a domain. Since R is finite dimensional as a $\mathbb{Q}$-vector space, m_x is surject. Therefore, $\exists y$ such that $m_x(y)=1$. Thus, R is a field. ■

Remark. If $x \in \mathbb{C}$ is an algebraic number then

$$\mathbb{Q}[x] = \mathbb{Q}\text{-span}(1, x, x^2, \ldots)$$

is a number field.

Proof. Since x is an algebraic number, there exists some non zero $f(T) \in \mathbb{Q}[T]$ such that $f(x) = 0$. Therefore,

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$

It follows that

$$x^n = -a_{n-1}x^{n-1} - \cdots - a_0 \in \text{span}(1, x, \ldots, x^{n-1}).$$

Similarly,

$$x^{n+1} = -a_{n-1}x^n - \cdots - a_0 \in \text{span}(1, x, \ldots, x^n) = \text{span}(1, x, \ldots, x^{n-1}).$$

Continuing in this way, we get that $\dim \mathbb{Q}[x] \leq n$. By the above remark, $\mathbb{Q}[x]$ is a field. ■

Note. This gives us that $\mathbb{Q}[x] \subset \mathbb{Q}(x)$. Since $\mathbb{Q}(x)$ is the smallest field containing x, we get that $\mathbb{Q}[x] = \mathbb{Q}(x)$.

Theorem 2.0.3. The set of algebraic numbers forms a subfield of $\mathbb{C}$.

Proof. If x is non-zero algebraic number then $\frac{1}{x}$ is algebraic.

Reason 1. $\frac{1}{x} \in \mathbb{Q}[x]$ because any element of an algebraic number field is algebraic. ■

Reason 2. If $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$. Dividing by x^n, we get

$$1 + a_{n-1}x^{-1} + \cdots + a_0 x^{-n} = 0.$$

Note x^{-1} satisfies this polynomial. ■

Say x, y are algebraic numbers. Then we need to show that $x + y$ and xy are algebraic numbers. Consider

$$\mathbb{Q}[x, y] = \text{span}\{x^i y^j \mid i, j \geq 0\} \subset \mathbb{C}.$$

This is finite dimesnional for same reason as $\mathbb{Q}[x]$ is. If x and y satisfy polynomials of degrees n and m then $\mathbb{Q}[x, y]$ will be spanned by $x^i y^j$ for $0 \leq i \leq n - 1$, $0 \leq j \leq m - 1$. ■

Remark. Say $a \in \mathbb{C}$ is an algebraic number. Then $\exists!$ monic polynomial $f(T) \in \mathbb{Q}[T]$ of minimal degree such that $f(a) = 0$. Moreover, if $g(T) \in \mathbb{Q}[T]$ has $g(a) = 0$ then $f(T)|g(T)$.

Proof. Consider the map

$$\begin{aligned} ev_a : \mathbb{Q}[T] &\longrightarrow \mathbb{C} \\ g(T) &\longmapsto ev_a(g(T)) = g(a). \end{aligned}$$

Then $f(T)$ is the unique monic generator of $\ker(ev_a)$. Key point is that $\mathbb{Q}[T]$ is a PID. ■

Definition 2.0.10. $f(T)$ is the minimal polynomial of a.

Remark. $\mathbb{Q}[T] / (f(T)) \underbrace{\cong}_{1st \text{ isomorphism theorem}} \mathbb{Q}[a] = \mathbb{Q}(a)$. Therefore, $\dim \mathbb{Q}[a] = \deg f(T)$.

Example. $a = \sqrt{-1}$, $f(T) = T^2 + 1$. Then $\mathbb{Q}[a] = \mathbb{Q}(a)$ is 2-d as a $\mathbb{Q}$-vector space.

Definition 2.0.11. A complex number a is an algebraic integer if $\exists$ monic polynomial $f(T) \in \mathbb{Z}[T]$ such that $f(a) = 0$.

Example. A rational number that is an algebraic integer is an ordinary integer.

Remark. The set of all algebraic integers is a subring of $\mathbb{C}$. If K is a number field, we define

$$\mathcal{O}_k = \{\text{algebraic integers that belong to } K\}.$$

This is a subring of K, called the ring of integers of K.

Example. If $\dim_{\mathbb{Q}}(K) = 2$ then $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ is square free. Then

$$\mathcal{O}_k = R_d = \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{if } d = 2, 3 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}], & \text{if } d = 1 \bmod 4 \end{cases}.$$

Problem 2.0.5. Understand factorizations in $\mathcal{O}_k$ i.e. for which K is this a UFD?

Example. $K = \mathbb{Q}(\sqrt{d})$ with $d < 0$ square free. $\mathcal{O}_k$ is a UFD for exactly 9 values of d.

Definition 2.0.12. An ideal I is prime if $xy \in I \Rightarrow x \in I$ or $y \in I$.

Remark. Every max ideal is prime.

Example. $\mathbb{Z}[\sqrt{-5}]$. Then $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. $(2, 1 + \sqrt{-5})$ is a prime ideal?

As previously seen. If I and J are ideals then $IJ =$ ideal generated by xy with $x \in I$ and $y \in J$

Example. $(x)(y) = (xy)$

Theorem 2.0.4. Let K be a number field. $I \subset \mathcal{O}_k$. $I \neq 0$. Then $\exists!$ factorization

$$I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_1^{e_r}.$$

where the $\mathfrak{p}_i$'s are distinct prime ideals $e_i \geq 1$.

Remark. There is an idea of fractional ideal of $\mathcal{O}_k$ i.e. a fractional ideal of $\mathbb{Z}$ is $\frac{1}{2}\mathbb{Z}$.

Remark. The fractional ideals form a group under multiplication with a subgroup of principal fractional ideals. The ideal class group of K is

$$\mathrm{Cl}(K) = {}^{X}\big/_{Y}$$

where X is the fractional ideals group and Y is the subgroup of principal fractional ideals.

Remark. The following are equivalent

- $\mathcal{O}_k$ is a UFD.
- $\mathcal{O}_k$ is a PID.
- $\mathrm{Cl}(K)$ is trivial.

Remark. $\mathrm{Cl}(K)$ is finite.

Chapter 3

Module Theory

Lecture 10: Tenth Lecture

25 Jan. 02:00

Definition 3.0.1. An R-module is an abelian group M equipped with a map $R \times M \to M$ defined by $(a, x) \mapsto ax$ such that

(1) $1 \cdot x = x$

(2) $a \cdot (x + y) = ax + ay$, $(a + b)x = ax + bx$

(3) $a \cdot (bx) = (ab) \cdot x$

Definition 3.0.2. If M and N are R-modules an R-module homomorphism is a function $\phi : M \to N$ that is compatible with addition and scalar multiplication i.e.

- $\phi(x + y) = \phi(x) + \phi(y)$ for every $x, y \in M$
- $\phi(ax) = a\phi(x)$ for every $a \in R$, $x \in M$.

Definition 3.0.3. An R-module isomorphism is a bijective R-module homomorphism.

Example. R is an R-module via $ax = ax$

Example. $\mathbb{Z}[i]$ is a $\mathbb{Z}$-module. More generally, if $\phi : R \to S$ is a ring homomorphism then S is an R-module via $a \cdot x = \phi(a) \cdot x$.

Example (Restriction of scalars). Even more generally, if N is an S-module then N becomes an R-module via $a \cdot x = \phi(a) \cdot x$ for $a \in R$ and $x \in N$, where $\phi(a) \cdot x$ is the multiplication defined by the S-module.

Example. If $I \subset R$ is an ideal then I is a R-module using usual multiplication.

Definition 3.0.4. If M is an R-module then an R-submodule of M is a subgroup that is closed under scalar multiplication.

Note. In fact, ideal $=$ R-submodule of R.

Example. If M is an abelian group we have defined $2x = x + x$. This gives M the structure of a

$\mathbb{Z}$-module. This is the unique $\mathbb{Z}$-module structure on M because

$$2x = (1+1)x = 1 \cdot x + 1 \cdot x = x + x.$$

Thus, $\mathbb{Z}$-modules are exactly abelian groups.

Example. $M_n(R)$ is an R-module. Use matrix addition, usual scalar multiplication.

Example. R^n is an R-module (column vectors with standard operations).

Example. $\mathbb{Z}/2\mathbb{Z}$ is a $\mathbb{Z}$-module. In general, if M is an R-module and $N \subset M$ is an R-submodule then M/N is naturally an R-module.

$$a(x + N) = ax + N.$$

Remark. Many constructions from group theory and linear algebra apply to modules:

- $\phi : M \to N$ homomorphism of modules, then
  1. $\ker(\phi) \subset M$ is a submodule
  2. $\operatorname{Im}(\phi) \subset N$ is a submodule.
- 1st isomorphism theorem:

  $$M \big/ \ker(\phi) \cong \operatorname{Im}(\phi)$$

  is an isomorphism of R-modules induced by ϕ.
- Direct sums: if M, N are R-modules then $M \oplus N$ is the R-modules whose elements are $M \times N$ with coordinate wise addition and scalar multiplication.
- R-module maps from $R^m \to R^n$ are described by $n \times m$ matrices with entries in R. If $A \in M_{n,m}(R)$ ($n \times m$ matrices with entries in R). Then $Ax \in R^n$ is defined by the usual formula

  $$\begin{aligned} R^m &\to R^n \\ x &\mapsto Ax. \end{aligned}$$

Example. $R^n \cong \underbrace{R \oplus \cdots \oplus R}_{n \text{ times}}$.

Definition 3.0.5. Say M is an R-module. A finite basis for M is a collection of elements $e_1, \ldots, e_r \in M$ such that every element of M can be written uniquely as a linear combination of these elements i.e.

$$a_1 e_1 + \cdots + a_r e_r, \qquad a_i \in R.$$

Example. If $M = R^n$ and $e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}$. Where $e_1 = 1$ in the ith spot then $e_1, \dots e_n$ is a basis for M.

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \sum_{i=1}^{n} a_i e_i.$$

Definition 3.0.6. M is a free R-module if it has a basis.

Example. R^n is free.

Example. $\mathbb{Z}/2\mathbb{Z}$ is not a free $\mathbb{Z}$-module. Only possible basis is $\overline{1} \in \mathbb{Z}/2\mathbb{Z}$. But this is not a basis because

$$0 = 0 \cdot \overline{1} = 2 \cdot \overline{1}.$$

Remark. Say that M is free with basis $e_1, \dots, e_n$. Then the map

$$\begin{aligned} \phi : R^n &\longrightarrow M \\ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} &\longmapsto \sum_{i=1}^{n} a_i e_i \end{aligned}$$

is an R-module isomorphism.

Example. $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is not a free $\mathbb{Z}$-module. This is because $(0, 1)$ is a torsion element.

Definition 3.0.7. R is a domain and M is an R-module. An element of M is called torsion if there exists $a \neq 0 \in R$ such that $ax = 0$.

Remark. $M_{\text{tors}} = \{x \in M \mid x \text{ is torsion}\}$ is a submodule of M.

Proof. Say $x, y \in M_{\text{tors}}$. We want to show $x + y \in M_{\text{tors}}$. Say $ax = 0$, $by = 0$, a, bR not zero. Then

$$ab(x + y) = abx + aby = 0.$$

Note that $ab \neq 0$ because R is a domain. If $c \in R$, then $a(cx) = 0$. Thus, $x + y, cx \in M_{\text{tors}}$ ■

Remark. If R is a domain and M is a free R-module then $M \cong R^n$ and so $M_{\text{tors}} = 0$, i.e. M is torsion-free.

Remark. If M is a finitely generated $\mathbb{Z}$-module that is torsion-free then M is free. (Same is true if $\mathbb{Z}$ is replaced by any PID)

Example. The following are torsion-free finitely generated but not free.

- $R = \mathbb{C}[x, y]$, $I = (x, y)$
- $R = \mathbb{Z}[\sqrt{-5}]$, $I = (2, 1 + \sqrt{-5})$

Lecture 11: Eleventh Lecture

25 Jan. 02:00

Definition. $M = R$-module.

Definition 3.0.8. Given any subset $S \subset M$ the R-submodule of M generated by S is the smallest submodule containing S i.e.

$$\bigcup_{\substack{S \text{ submodule} \\ S \subset N}} S.$$

The elements of this submodule are elements of the form

$$a_1 x_1 + \cdots + a_n x_n$$

with $a_i \in R$ and $x_i \in S$.

Definition 3.0.9. We say M is finitely generated if it is generated by a finite subset.

Example. If R is a field and M is an R-module (vector space) then M is finitely generated as an R-module if and only if it is finite dimensional.

Example. R^n is finitely generated if the basis vectors $e_1, \ldots, e_n$ generate it.

Example. If M, N are finitely generated so is $M \oplus N$.

Example. $R[x]$ is not a finitely generated R-module ($R \neq 0$).

Example. $\mathbb{Q}$ is not finitely generated as a $\mathbb{Z}$-module.

Theorem 3.0.1 (Mapping property for free modules)**.** Given any R-module M and $x_1, \ldots, x_n \in M$, $\exists!$ map of R-modules

$$\begin{aligned} \phi : R^n &\longrightarrow M \\ e_i &\longmapsto \phi(e_i) = x_i. \end{aligned}$$

Moreover, $\operatorname{im}(\phi) =$ submodule of M generated by $x_1, \ldots, x_n$.

Proof. $\phi(a_1 e_1 + \cdots + a_n e_n) = a_1 x_1 + \cdots + a_n x_n$. ∎

Corollary 3.0.1. M is finitely generated if and only if there exists a surjective map of R-modules $\phi : R^n \to M$.

Remark. Say M is a finitely generated module. Choose a surjection $\phi : R^n \to M$. By first isomorphism theorem, we know that

$$M \cong R^n \big/ \ker(\phi).$$

If $\ker(\phi)$ is generated by $y_1, \ldots, y_m$ then

$$M \cong R^n \big/ \langle y_1, \ldots, y_m \rangle.$$

Notation. $\langle , \rangle$ is submodule generated by elements.

Definition 3.0.10. We say that M is finitely presented if

$$M \cong R^n \big/ \langle y_1, \ldots, y_m \rangle \quad \text{for some } n$$

and some $y_1, \ldots, y_m \in R^n$ presentation of M.

Example. $R = \mathbb{Z}$. $M = \mathbb{Z} / 5\mathbb{Z} \oplus \mathbb{Z} / 7\mathbb{Z}$. Generated by $(1, 0)$ and $(0, 1)$. Therefore, M is finitely generated. Note that

$$\ker(\phi) = \{k(5e_1) + j(7e_2)\}.$$

Therefore, $\ker(\phi) = \langle 5e_1, 7e_2 \rangle$ and M is finitely presented.

Example. $R = \mathbb{C}[x, y]$, $M = (x, y) \subset R$. M is finitely generated because it is generated by x and y. Consider

$$\begin{aligned} \phi : R^2 &\longrightarrow R \\ e_1 &\longmapsto \phi(e_1) = x \\ e_2 &\longmapsto \phi(e_2) = y \end{aligned}.$$

Problem 3.0.1. Is $\ker(\phi)$ finitely generated?

Answer. $-ye_1 + xe_2 \in \ker(\phi)$. To see this is the only one consider an arbitrary element in the kernel i.e.

$$\phi(fe_1 + ge_2) = fx + gy = 0.$$

Then

$$f = -\frac{y}{x} g.$$

Therefore,

$$fx + gy = \frac{g}{x}(-ye_1 + xe_2)$$

so it is generated by our initial element. ⊛

Remark. Say M is a finite presentation

$$M \cong R^n \big/ \langle y_1, \ldots, y_m \rangle.$$

Let

$$\begin{aligned} \psi : R^m &\longrightarrow R^n \\ e_j &\longmapsto \psi(e_j) = y_j. \end{aligned}$$

Then $\mathrm{im}(\psi) = \langle y_1, \ldots, y_m \rangle \subset R^n$. The matrix of ψ given by an $m \times n$ matrix with coefficients in R is the presentation matrix.

As previously seen. If $\phi : M \to N$ is a map of modules, then

$$\mathrm{coker}(\phi) = {}^{N}\big/_{\mathrm{Im}(\phi)}.$$

Example. $R = \mathbb{Z}$, $M = \mathbb{Z} / 5\mathbb{Z} \oplus \mathbb{Z} / 7\mathbb{Z}$, then

$$M \cong {}^{\mathbb{Z}^2}\big/_{\underbrace{\langle 5e_1, 7e_2 \rangle}_{\begin{bmatrix} 5 & 0 \\ 0 & 7 \end{bmatrix}}} \cong {}^{\mathbb{Z}}\big/_{\underbrace{\langle 35 \rangle}_{[35]}}.$$

Example. $R = \mathbb{C}[x, y]$, $M = (x, y)$, $M = R^2 / \langle -ye_1 + xe_2 \rangle$ with

$$\begin{aligned} \psi : R &\longrightarrow R^2 \\ 1 &\longmapsto \psi(1) = -ye_1 + xe_2. \end{aligned}$$

Then $\begin{bmatrix} -y \\ x \end{bmatrix}$ is the presentation matrix.

Example. $R = \mathbb{Z}$, M is module with presentation matrix $A = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$. Then $M = \mathrm{coker}(\psi)$, where

$$\begin{aligned} \psi : \mathbb{Z}^2 &\longrightarrow \mathbb{Z}^2 \\ e_1 &\longmapsto \psi(e_1) = e_1 + 2e_2 \\ e_2 &\longmapsto \psi(e_2) = 2e_1 + e_2. \end{aligned}$$

Note. Invertible as rational matrix but not as integer matrix. Need $-\frac{1}{3}$.

Note that any combination of $\psi(e_1), \psi(e_2)$ are multiples of 3.

Exercise. Work out why $M \cong \mathbb{Z} / 3\mathbb{Z}$.

Remark. Say M is a finitely generated R-modules. Then there exists a surjective $\phi : R^n \to M$. For M to be finitely presented we would like $\ker(\phi)$ to be finitely generated. This does not need to be true!

Problem 3.0.2. It is possible that a submodule of a finitely generated module is not finitely generated.

Example. $R = \mathbb{C}[x_1, x_2, x_3, \ldots]$, $M = (x_1, x_2, \ldots)$. R is finitely generated as an R-module, but M is not finitely generated.

Example. $R \,/\, M \cong \mathbb{C}$. $\mathbb{C}$ is finitely generated as an R-module but not finitely presented.

Lecture 12: Twelth Lecture

1 Feb. 02:00

Example. Say M is finitely generated. Pick a surjection $\phi : R^n \to M$.

Problem 3.0.3. $\ker \phi$ may not be finitely generated.

Definition 3.0.11. An R-module M is called noetherian if the following equivalent conditions hold:

(1) Every R-submodule of M is finitely generated.

(2) Ascending chain condition holds for submodules i.e. if

$$N_1 \subset N_2 \subset \cdots \subset M$$

then $\exists n$ such that $N_n = N_{n+1} = \cdots$

Remark. R is noetherian as a ring if and only if R is noetherian as an R-module.

Remark. Suppose that R^n is a noetherian R-module for all n. Then every finitely generated R-module is finitely presented.

Definition 3.0.12. Consider maps of R-modules, $M_1 \xrightarrow{\phi} M_2 \xrightarrow{\psi} M_3$. We say this is exact at M_2 if $\operatorname{im}(\phi) = \ker(\psi)$ (this implies $\psi \circ \phi = 0$).

Remark. Two important cases:

- $0 \xrightarrow{\phi} M_2 \xrightarrow{\psi} M_3$. Exact at M_2 if and only if ψ is injective.
- $M_1 \xrightarrow{\phi} M_2 \xrightarrow{\psi} 0$. Exact at M_2 if and only if ϕ is surjective.

Definition 3.0.13. A short exact sequence is a sequence

$$0 \to M_1 \xrightarrow{\phi} M_2 \xrightarrow{\psi} M_3 \to 0$$

that is exact at M_1, M_2, M_3. Explicitly,

- ϕ is injective,
- ψ is surjective,
- $M_3 \cong M_2 \,/\, \phi(M_1)$.

Remark. In the above situation, we say that M_2 is an extension of M_3 by M_1.

Example. Say $R = \mathbb{Z}$, $M_1 = M_3 = \mathbb{Z} \,/\, 2\mathbb{Z}$.

$$0 \to \mathbb{Z}\big/2\mathbb{Z} \to \mathbb{Z}\big/4\mathbb{Z} \overset{\text{reduce mod 2}}{\to} \mathbb{Z}\big/2\mathbb{Z} \to 0.$$

Defined by $1 \mapsto 2$.

Example. Similarly,

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

Example. Say $R = \mathbb{Z}$, $M_1 = \mathbb{Z} / 3\mathbb{Z}$, $M_3 = \mathbb{Z} / 5\mathbb{Z}$.

$$0 \to \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z} \overset{\text{reduce mod 5}}{\to} \mathbb{Z}/5\mathbb{Z} \to 0.$$

Example. Say $R = \mathbb{Z}$, $M_1 = \mathbb{Z} / 2\mathbb{Z}$, $M_3 = \mathbb{Z}$.

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z} \to 0.$$

Only extension is $\mathbb{Z} / 2\mathbb{Z} \oplus \mathbb{Z}$.

Example. Say $R = \mathbb{Z}$, $M_3 = \mathbb{Z} / 2\mathbb{Z}$, $M_1 = \mathbb{Z}$.

$$0 \to \mathbb{Z} \to M_2 \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

Can take

- ϕ as multiplication by 2 and ψ reduction mod 2.
- $M_2 = \mathbb{Z} \oplus \mathbb{Z} / 2\mathbb{Z}$.

Example. $R = F$ is a field. Suppose

$$0 \to V_1 \to V_2 \to V_3 \to 0$$

is a SES of finite dimensioal vector spaces. Then

(1) $\dim V_1 - \dim V_2 + \dim V_3 = 0$

(2) $0 \to V_3^* \to V_2^* \to V_1* \to 0$ is a SES, where $*$ is the dual space.

Lemma 3.0.1. Suppose we have a SES

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

such that M_1 and M_3 are finitely generated. Then M_2 is finitely generated.

Equivalently, if M_2 is a module that contains a finitely generated submodule M_1 such that M_1 / M_2 is finitely generated then M_2 is finitely generated.

Proof. Replacing M_1 with $\phi(M_1)$, can assume $M_1 \subset M_2$ and ϕ is the inclusion map. Let $x_1, \ldots, x_n$ be generators for M_1 and $\overline{x}_1, \ldots, \overline{x}_m$ be generators for M_2. Choose $yi \in M_2$ such that $\psi(y_i) = \overline{y}_i$ (possible b/c ψ is surjective).

Claim. $x_1, \ldots, x_n$ and $y_1, \ldots, y_m$ generate M_2.

Let $z \in M_2$ be given. Write

$$\psi(z) = \sum_{i=1}^{m} b_i \overline{y}_i,$$

where $b_1, \ldots, b_m \in R$. Then

$$\psi(z - \sum_{i=1}^{m} b_i \overline{y}_i) = 0.$$

Therefore, $z - \sum_{i=1}^{m} b_i \overline{y}_i \in \ker(\psi) = M_1$. So, we can write $z - \sum_{i=1}^{m} b_i \overline{y}_i = \sum_{i=1}^{n} a_i x_i$ with $a_i \in R$. ■

Corollary 3.0.2. If M_1 and M_3 are noetherian, so is $M_1 \oplus M_3$.

Proof. Let $N_2 \subset M_2$ be a submodule. Assume $M_1 \subset M_2$ and ϕ is the inclusion map. Put $N_3 = \psi(N_2) \subset M_3$. Then

$$\ker(\psi : N_2 \to N_3) = \underbrace{N \cap M_1}_{N_1}.$$

Now we have a SES,

$$0 \to N_1 \to N_2 \to N_3 \to 0.$$

Since we assume M_1 and M_3 are noetherian, N_1 and N_3 are finitely generated. Thus, by the previous lemma, N_2 is finitely generated and M_2 is noetherian. ■

Lemma 3.0.2. Suppose we have a SES,

$$0 \to M_1 \to M_2 \to M_3 \to 0,$$

such that M_2 is noetherian, then M_1 and M_3 are noetherian.

Proof. Any submodule of M_1 is also a submodule of M_2 so it is finitely generated because M_2 is noetherian. Therefore, M_1 is noetherian. Say $N_3 \subset M_3$ is submodule. Then

$$\phi^{-1}(N_3) \to N_3$$

where $\phi^{-1}(N_3)$ is finitely generated because M_2 is noetherian. Therefore, N_3 is finitely generated because it is the quotient of a finitely generated module. ■

Proposition 3.0.1. Suppose R is noetherian. Then every finitely generated R-module is a noetherian module.

> **Note.** In particular, R^n is a noetherian R-module for every n, so any finitely generated module is finitely presented.

Proof. Let M be a finitely generated R-module. Then there exists a surjection $\phi : R^n \to M$. Then

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

is noetherian because a direct sum of noetherian modules is noetherian. Therefore, M is noetherian because it is a quotient of R^n. ■

Example. Any $\mathbb{Z}$-submodule of $\mathbb{Z}^n$ is finitely generated.

Lecture 13: Thirteenth Lecture

3 Feb. 02:00

Theorem 3.0.2 (Hilbert basis theorem)**.** If R is a noetherian ring so is $R[x]$.

Problem 3.0.4 (Idea). (if $I \neq 0$) choose $f \in I$ of minimal degree. Maybe it generates?

Answer. We'd like to say if $g \in I$ then $\exists h$ such that $g - hf$ has smaller degree. If $g = ax^n + \cdots + a_0$ and $f = bx^m + \cdots + b_0$, $h = cx^{n-m} + \cdots + c_0$. Then

$$hf = bcx^n + \cdots .$$

For the leading term to cancel in $g - hf$ we need that $a \in (b)$. ⊛

Proof. Let $I \subset R[x]$ be given. Say $f_1 = a_1x^{n_1} + \cdots$, $f_2 = a_2x^{n_2} + \cdots$, where $f_1, f_2 \in I$ and $g = bx^m + \cdots \in I$. If $b \in (a_1, a_2)$ and $m \geq n_1, n_2$ then $\exists h_1, h_2$ such that in $g - h_1f_1 - h_2f_2$ the leading term cancels. ∎

Definition 3.0.14. The initial coefficient of $f \neq 0 \in R$, denoted $\text{in}(f)$ is its leading coefficient (if $f = ax^n + \cdots$ then $\text{in}(f) = a$).

Definition 3.0.15. The initial ideal of I is

$$\text{in}(I) = \{\text{in}(f) \mid f \in I \setminus \{0\}\} \cup \{0\}.$$

Lemma 3.0.3. $\text{in}(f)$ is an ideal of R.

Proof. Say $a, b \in \text{in}(I)$, not zero. Then

$$\begin{aligned} a &= \text{in}(f), \quad f = ax^n + \cdots \\ b &= \text{in}(g), \quad g = bx^m + \cdots . \end{aligned}$$

Given $c \in R$, if $a = 0$ then $ca \in \text{in}(I)$. Otherwise, $ca = \text{in}(cf) \in \text{in}(I)$. We can assume $n = m$ (if $n < m$ replace f with $x^{m-n}f$) $a + b$ is either 0 ($\in \text{in}(I)$) or $\text{in}(f + g) \in \text{in}(I)$. ∎

Remark. Since R is noetherian, $\text{in}(I)$ is finitely generated. Choose $f_1, \ldots, f_r \in I$ such that $\text{in}(f_1), \ldots, \text{in}(f_r)$ that generate $\text{in}(I)$.

Lemma 3.0.4. Given $g \in I$ such that $\deg(g) \geq \deg(f_i)$ for every i. Then $\exists h_1, \ldots, h_i$ such that

$$\deg(g - hf_1 \cdots h_rf_r) < \deg(g).$$

Proof. $g = bx^m + \cdots$, $f_i = a_ix^{n_i} + \cdots$. Then $a_1, \ldots, a_r$ generate $\text{in}(I)$ and $b \in \text{in}(I)$. So $b = c_1a_1 + \cdots c_ra_r$. Take $h_i = c_ix^{m-n_i}$ for some $c_i \in I$. ∎

Corollary 3.0.3. $N = \max\{\deg(f_i)\}_{1 \leq i \leq r}$. Define

$$I_{\leq N} = \{f \in I \mid \deg(f) \leq N\}.$$

Then $I = (f_1, \ldots, f_r) + I_{\leq n}$.

Remark. Note that $I_{\leq n} \subset R \oplus R \cdot x \cdots \oplus R \cdot x^n$. Since R is noetherian, $I \leq N$ is finitely generated. If $f_1', \ldots, f_s'$ generated $I_{\leq n}$ as an R-module then $I = (f_1, \ldots, f_r, f_1', \ldots, f_s')$. Thus, I is finitely generated.

Corollary 3.0.4. If R is noetherian then $R[x_1, \ldots, x_n]$ is noetherian.

Note. If R is noetherian so is any quotient ring of R.

Corollary 3.0.5. If R is noetherian then any $\underbrace{\text{finitely generated } R\text{-algebra}}_{R[x_1,\ldots,x_n]}$ is noetherian.

Problem 3.0.5 (Invariant Theory). G acting on $\mathbb{C}[x_1,\ldots,x_n]$. Describe $\mathbb{C}[x_1,\ldots,x_n]^G$ (the G invariant polynomials)

Example. Consider homogeneous degree 2 polynomials in 2 variables.

$$aX^2 + bXY + cY^2.$$

Given $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C})$. Then

$$\begin{aligned} g \cdot F &= F(\alpha X + \beta Y, \gamma X + \delta Y) \\ &= a(\alpha X + \beta Y)^2 + b(\alpha X + \beta Y)(\gamma X + \delta Y) + c(\gamma X + \delta Y)^2 \\ &= (a \cdot \alpha^2 + b\alpha\gamma + c\gamma^2)X^2 + (\cdots)XY + (\cdots)Y^2. \end{aligned}$$

For $G = \mathrm{SL}_2(\mathbb{C})$, $C[a,b,c]$ and $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C})$. Then

$$g \cdot a = \alpha a^2 + b\alpha\gamma + c\gamma^2.$$

Then $\mathbb{C}[a,b,c]^G$ is the polynomial functions of the coefficients of a quadratic form that are invariant under linear change of variables. Then

$$\mathbb{C}[a,b,c] \cong \mathbb{C}[T]$$

where $T \Leftrightarrow b^2 - ac$.

Example. Consider $F = a_0X^n + a_1X^{n-1}Y + a_nY^n$. Then for $G = \mathrm{SL}_2(\mathbb{C})$, acting on $C[a_0,\ldots,a_n]$ the invariant rings are

$n = 2$: Invariant ring is polynomial ring in 1 generator.

$n = 3$: Invariant ring is polynomial ring in 2 generators.

Remark. Paul Gordon proved for this family the invariant ring is a finitely generated $\mathbb{C}$-algebra for every n. Finite generation from Hilbert proof for a large class of G, $\mathbb{C}[x_1,\ldots,x_n]^G$ is a finitely generated $\mathbb{C}$-algebra.

3.1 Exam

3.1.1 Rings

- Rings, homomorphisms, subrings, ideals, quotient rings.
- Presentations of rings i.e. $\mathbb{Z}[i] = \mathbb{Z}[x] / x^2 + 1$ how to prove this.
- Adjoining elements. $R[x] / (f(x))$
  - f is monic of degree d this ring is a free R-module with basis $1, x, x^2, \ldots, x^{d-1}$
  - $f(x) = ax - 1$, $R[\frac{1}{a}]$.
    - $\mathbb{C}[x] / (x^2+1) \cong \mathbb{C} \times \mathbb{C}$
    - $\mathbb{F}_2[x] / (x^2+1) \cong \mathbb{F}_2[u] / (u^2)$. Shows this ring is not even reduced because nilpotent element.

- Fractional fields of domain.
- Maximal ideals
  - Max if and only if quotient is a field
- Classified maximal ideals of $\mathbb{C}[x_1, \dots, x_n]$
  - All of the form $(x_1 - \alpha_1, \dots, x_n - \alpha_n)$ for $\alpha_i \in \mathbb{C}$.

3.1.2 Factorization

- Unit, divisibility, associate elements.
- Irreducible elements and prime elements.
  - Used to define a UFD
- Criterion for UFD
  - If R is noetherian and all irreducible elements are prime then R is a UFD.
  - Noetherian gives termination.
  - Prime gives uniqueness.
- Euclidean ring $\Rightarrow$ PID $\Rightarrow$ UFD.
- $\mathbb{Z}[i]$ are Euclidean, understood primes.

Lecture 14: Fourteenth Lecture

3.2 Back to modules

8 Feb. 02:00

As previously seen. An element $x \in M$ is torsion if $\exists 0 \neq a \in R$ such that $ax = 0$.

- An R-module is torsion if every element is torsion.
- If M is a free R-module then M is torsion-free, i.e. $M_{\text{tors}} = 0$.

Example. $\mathbb{Z} \oplus \mathbb{Z} / 2\mathbb{Z}$ is not free as a $\mathbb{Z}$-module.

Remark. Free implies torsion free but reverse implication not true in general.

- If you can find a non principle ideal then it will not be free as a module. This is because the relations will create a torsion element.

Example. The ideal (x, y) in $\mathbb{C}[x, y]$ is a torsion-free $\mathbb{C}[x, y]$-module but not free.

Theorem 3.2.1. If M is a finitely generated torsion-free $\mathbb{Z}$-module then M is free.

Remark. Finite generation is necessary.

Example. $\mathbb{Q}$ is a $\mathbb{Z}$-module that is torsion free, but it is not free. This is because any two elements satisfy a linear relation. Therefore, basis could only have size 1. However, $\mathbb{Q} \neq \mathbb{Z}$.

Definition. Let R be a ring and $M_1, M_2, \dots$ be R-modules.

Definition 3.2.1. $\prod_{n=1}^{\infty} M_n$ = all tuples $(x_1, x_2, \dots)$ for $x_i \in M_i$ with coordinate wise operations.

Definition 3.2.2. $\bigoplus_{n=1}^{\infty} M_n \subset \prod_{n=1}^{\infty} M_n$ tuples with finitely many non-zero entries.

Example. $\bigoplus_{n=1}^{\infty} R$ is a free R-module with basis:

$$e_i = (0, \dots, \underbrace{1}_{i\text{th spot}}, 0, \dots).$$

Example. $\prod_{n=1}^{\infty} \mathbb{Z}$ = all infinite tuples of integers.

Note. This is not $\bigoplus_{n=1}^{\infty} \mathbb{Z}$. In $\bigoplus$, there are only finitely many non-zero entries.

This is not free.

As previously seen. Recall that

- $\mathrm{Frac}(R)$ is a field, where all elements have the form $\frac{a}{b}$ for $a, b \in \mathbb{R}$ with $b \neq 0$.
- A multiplicative set $S \subset R$ is a subset of R that contains one and is closed under multiplication.
- $S^{-1}R = \{\frac{a}{s} \mid a \in R, s \in S\} \subset \mathrm{Frac}(R)$.

Problem 3.2.1. Given an R-module M we want to create an $S^{-1}R$-module $S^{-1}M$.

Answer. Elements of $S^{-1}M$ are represented by expressions $\frac{m}{s}$ with $m \in M$ and $s \in S$. We say $\frac{m_1}{s_1} = \frac{m_2}{s_2}$ if $\exists s \in S$ such that $s(s_2 m_1 - s_1 m_2) = 0$. This is an $S^{-1}R$ module via

$$\frac{a}{s_1} \cdot \frac{m}{s_2} = \frac{am}{s_1 s_2}$$

and

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}.$$

⊛

Note. The intuition for this is $\frac{m}{1} = \frac{sm}{s}$ for every $s \in S$. So $\frac{m}{1} = 0$ if $\exists s \in S$ such that $sm = 0$.

Example. $\mathbb{R} = \mathbb{Z}$, $S = \{1, 2, 3, 4, \dots\}$, $M = \mathbb{Z}/2\mathbb{Z}$. Then $S^{-1}M = 0$. This is because for any element x in M we have that $2x = 0$. Therefore,

$$x = \frac{2}{2} \cdot \frac{x}{1} = \frac{2x}{2} = \frac{0}{2} = 0.$$

Since $2 \in S$, we have that $S^{-1}M = 0$.

Example. $\mathbb{R} = \mathbb{Z}$, $S = \{1, 2, 3, 4, \dots\}$, $M = \mathbb{Z}/3\mathbb{Z}$. Then $S^{-1}M = \mathbb{Z}/3\mathbb{Z}$. Note that

$$\frac{1}{2} = \frac{2}{1}, \quad \frac{1}{4} = \frac{4}{1}, \dots.$$

Then it is easy to see that every element of $S^{-1}M$ has the form $0, \frac{1}{1}, \frac{2}{1}$. This is because that everything in S is already a unit in $\mathbb{Z}\,/\,3\mathbb{Z}$.

Example. $R = \mathbb{Z}$, $S = \{1, 2, 4, \ldots\}$, $M = \mathbb{Z}\,/\,6\mathbb{Z}$. Then $S^{-1}M \cong \mathbb{Z}\,/\,3\mathbb{Z}$.

Example. $R = \mathbb{Z}$, $S = \mathbb{Z} \setminus \{0\}$, $M = \mathbb{Z}^n$, $S^{-1}M = \mathbb{Q}^n$.

Remark. R is a domain. Let $S = \mathbb{R} \setminus \{0\}$, $K = S^{-1}R = \operatorname{Frac}(R)$. If M is any R-module then $S^{-1}M$ is an $S^{-1}R$-module i.e. a K-vector space.

Remark. Suppose $f : M \to N$ is an R-module homomorphism. This induces a homomorphism of $S^{-1}R$-modules

$$\begin{aligned} S^{-1}F : S^{-1}M &\longrightarrow S^{-1}N \\ \frac{x}{s} &\longmapsto \frac{f(x)}{s}. \end{aligned}$$

If $g : N \to L$ is another R-module map then

$$S^{-1}(gf) = (S^{-1}g)(S^{-1}f).$$

This can be seen by:

$$\begin{tikzcd} S^{-1}M \arrow[r, "S^{-1}f"] \arrow[rr, bend right, "S^{-1}(gf)"'] & S^{-1}N \arrow[r, "S^{-1}g"] & S^{-1}L \end{tikzcd}$$

Lecture 15: Fifteenth Lecture

3.3 Exam Answers

10 Feb. 02:00

Problem 3.3.1. Find maximal ideal of $C[x, y]/(f)$ with $f = xy(x + y) - 1$

Answer. Max ideals of $\mathbb{C}[x, y]/(f)$ correspond to max ideals of $\mathbb{C}[x, y]$. Max ideals of $\mathbb{C}[x, y]$ are $(x - a, y - b)$ which is $\ker(\mathbb{C}[x, y] \to \mathbb{C})$ defined by $g \mapsto g(a, b)$. Therefore, we just need $(a, b) \in \mathbb{C}^2$ such that $f(a, b) = 0$. ⊛

Problem 3.3.2. $\phi : R \to S$ is a surjective ring map such that every element of the kernel is nilpotent. Given a unit $y \in S$ show that there exists a unit $x \in R$.

Answer. We know $\exists y' \in S$ such that $yy' = 1$. Pick $x, x' \in R$ such that $\phi(x) = y$ and $\phi(x') = y'$. Therefore, $\phi(xx') = yy' = 1 = \phi(1)$. Therefore, $xx' = 1 + z$ where $z \in \ker \phi$. Since z is nilpotent, $1 + z$ is a unit. Therefore,

$$x \underbrace{x'(1 + z)^{-1}}_{x^{-1}} = 1.$$

⊛

Problem 3.3.3. $\mathbb{Z}\left[\frac{1}{6}\right] \subset \mathbb{Q}$ and $I \subset \mathbb{Z}\left[\frac{1}{6}\right]$ is the ideal generated by 60. Define $J = I \cap \mathbb{Z}$. Show that J is an ideal. Find a generator.

Answer. Since I and $\mathbb{Z}$ are both subgroups, there intersection is an ideal.

$$\frac{60a}{6^n} = \frac{6 \cdot 6 \cdot 5b}{6^n}.$$

Therefore, $5 \in I$ and $(5) \subset J$. Therefore, $J = (5)$ or $J = (1)$. Since $1 \notin J$, $J = (5)$.

Note. General fact: if $f, g \in R$ then $R\left[\frac{1}{fg}\right] = R\left[\frac{1}{f}, \frac{1}{g}\right]$.

⊛

Problem 3.3.4. Factor $4 + 7i$ into Gaussian primes.

Answer. $N(4 + 7i) = 65 = 5 \cdot 13$. Since these are 1 mod 4, they factor into $\pi\overline{\pi}$. Note that

$$5 = (2 + i)(2 - i) \quad \text{and} \quad 13 = (3 + 2i)(3 - 2i).$$

Thus,

$$4 + 7i = (2 + i)(3 + 2i).$$

⊛

Problem 3.3.5. Find a PID with exactly three maximal ideals.

Answer. $\mathbb{Z}[\frac{1}{p}]_{p\neq 2,3,5}$. Let $I \subset \mathbb{Z}[\frac{1}{p}]_{p\neq 2,3,5}$. Consider $I \cap \mathbb{Z} = n\mathbb{Z}$. Then $n \in I \Rightarrow (n) \subset I$. Given $x = \frac{a}{b} \in I$, $bx \in I \cap \mathbb{Z}$ we have that $bx = n \cdot c$ and $x = \frac{n \cdot c}{b}$. Therefore, $\frac{c}{b} \in R$ and $x \in n \cdot R$. Thus, $I = nR$. ⊛

3.3.1 Back to modules again

As previously seen. R-domain. $S \subset R$ is a multiplicative set, where

$$S^{-1}R = \left\{ \frac{x}{s} \mid x \in R, s \in S \right\} \subset \operatorname{Frac}(R).$$

For an R-mod M, $S^{-1}M$ has elements $\frac{x}{s}$ and $\frac{x_1}{s_1} = \frac{x_2}{s_2}$ if $\exists s$ such that $s(x_1 s_2 - x_2 s_1) = 0$.

Lemma 3.3.1. If f is injective, so is $S^{-1}f$.

Proof. Say $\frac{x}{s} \in S^{-1}M$ belongs to $\ker(S^{-1}f)$. Therefore,

$$0 = (S^{-1}f)(\frac{x}{s}) = \frac{f(x)}{s}.$$

It follows that $\exists s' \in S$ such that

$$s'(f(x) \cdot 1 - 0 \cdot s) = s'f(x) = 0 \text{ in } N.$$

Since f is a map of modules,

$$s'f(x) = f(s'x) = 0.$$

Because f is injective, $s'x = 0$ in M and $\frac{x}{s} = 0$ in $S^{-1}M$. Thus, $\ker(S^{-1}f) = 0$. ∎

Lemma 3.3.2. If f is surjective then $S^{-1}f$ is surjective.

Proof. Given $\frac{y}{s} \in S^{-1}N$, $\exists x \in M$ such that $f(x) = y$. Thus,

$$(S^{-1}f)\left(\frac{x}{s}\right) = \frac{y}{s}.$$

■

Lemma 3.3.3. Say M is a submodule of N, then f is the inclusion map i.e.

$$\frac{S^{-1}N}{S^{-1}M} \cong S^{-1}\left({}^{N}\big/_{M}\right).$$

Proof. Let $\pi : N \to N\,/\,M$ be the quotient map

$$S^{-1}\pi : S^{-1}N \longrightarrow S^{-1}\left({}^{N}\big/_{M}\right).$$

This is surjective by previous lemma.

Claim. $\ker(S^{-1}\pi) = S^{-1}M$.

Proof. First we will show that $S^{-1}M \subset \ker(S^{-1}\pi)$. If $x \in M$, $s \in S$ then

$$(S^{-1}\pi)\left(\frac{x}{s}\right) = \frac{\pi(x)}{s} = 0$$

. Then

$$0 = (S^{-1}\pi)\left(\frac{x}{s}\right) = \frac{\pi(x)}{s}.$$

Therefore, $\exists s' \in S$ such that $s'\pi(x) = 0$ in $N\,/\,M$. Since π is a module homomorpism,

$$s'\pi(x) = \pi(s'x) = 0.$$

It follows that $s'x \in \ker(\pi) = M$. Thus, $\frac{x}{s} = \frac{y}{ss'} \in S^{-1}N \in S^{-1}M$. ■

The result follows by first isomorphism theorem and the claim. ■

Remark. This can be rephrased in the language of SES. Consider the sequence

$$0 \to M_1 \to M_2 \to M_3 \to 0.$$

If this is a SES of R-modules then

$$0 \to S^{-1}M_1 \to S^{-1}M_2 \to S^{-1}M_3 \to 0.$$

is a SES of $S^{-1}R$-modules. Localization is an exact functor.

Lecture 16: Sixteenth Lecture

13 Feb. 02:00

Theorem 3.3.1 (Structure Theorem for finitely generated $\mathbb{Z}$-modules)**.** Any finitely generated $\mathbb{Z}$-module is a finite $\oplus$ of $\mathbb{Z}$'s and $\mathbb{Z}\,/\,n\mathbb{Z}$'s.

Proof strategy 1. Let M be a finitely generated $\mathbb{Z}$-modules. Choose a presentation

$$\mathbb{Z}^m \xrightarrow{\phi} \mathbb{Z}^n \to M \to 0.$$

where

$$M \cong \operatorname{coker}(\phi) = {\mathbb{Z}^n}\Big/{\operatorname{im}(\phi)}.$$

Then ϕ corresponds to an $n \times m$ matrix. Prove that you can essentially diagonalize this matrix with certain row and column operations. See the book for this proof. ■

We will follow strategy 2, which is more module-theoretic.

Step 1: We will show that a finitely generated torsion-free $\mathbb{Z}$-module F is free.

- Find a submodule $\mathbb{Z}x \subset F$.
- Claim $F \,/\, \mathbb{Z}x$ is smaller than F, so free by induction.
- $F = \mathbb{Z}x \oplus F \,/\, \mathbb{Z}x$ is free.

Problem 3.3.6. What does smaller mean?

Answer. We will take the $\mathbb{Q}$-dimension of the localization. ⊛

Problem 3.3.7. How do we pick x such that $F \,/\, \mathbb{Z}x$ is torsion-free?

Example. $F = \mathbb{Z}^2$, $x = \begin{pmatrix} 6 \\ 4 \end{pmatrix}$. Then $F \,/\, \mathbb{Z}x$ is not torsion free. Namely, $2 \cdot \begin{pmatrix} 3 \\ 2 \end{pmatrix} = 0$.

Answer. We will see in the proof below. ⊛

Proof. Let F be a finitely generated torsion-free $\mathbb{Z}$-module. Pick $x \in F$ non-zero. Define

$$L := \{y \in F \mid \exists n \neq 0, m \in \mathbb{Z} \text{ s.t. } ny = mx\} \subset F.$$

Note that L is the set of all elements that are a rational multiple of x.

Note. $S = \mathbb{Z} \setminus \{0\}$, $S^{-1}\mathbb{Z} = \mathbb{Q}$. If M is a $\mathbb{Z}$-module then $S^{-1}M$ is a $\mathbb{Q}$-vector space. We have a map

$$\begin{aligned} M &\longrightarrow S^{-1}M \\ x &\longmapsto \frac{x}{1} \end{aligned}$$

which is injective if M is torsion free. Note that

$$F \subset S^{-1}F \supset \mathbb{Q}x.$$

Therefore, $L = \mathbb{Q}x \cap F$.

Claim. L is finitely generated as a $\mathbb{Z}$-module.

Proof. $\mathbb{Z}$ is noetherian and F is a finitely generated $\mathbb{Z}$-module, so every submodule is finitely generated (including L). ■

Claim. $\exists y \in L$ such that $L = \mathbb{Z}y$.

Lemma 3.3.4. If N is a finitely generated $\mathbb{Z}$-submodule of $\mathbb{Q}$, $N = \mathbb{Z}y$ for some $y \in N$.

Proof of lemma. Let $z_1, \ldots, z_r \in N$ be generators. Pick $a \in \mathbb{Z}$ non-zero such that $az_i \in \mathbb{Z}$ for every i. Note that $aN \subset \mathbb{Z}$. Since $\mathbb{Z}$ is a PID, $aN = b\mathbb{Z} \Rightarrow N = \frac{b}{a} \cdot \mathbb{Z}$. ■

Proof of claim. L is a finitely generated $\mathbb{Z}$-submodule of $\mathbb{Q}$. Thus, the claim follows from the lemma. ■

Claim. $F \,/\, L$ is torsion-free.

Proof. Suppose that $\overline{z}$ is a torsion element of $F \,/\, L$, say $n\overline{z} = 0$ for $n \neq 0 \in \mathbb{Z}$. Let z be a lift of $\overline{z}$ to F. Since $n\overline{z} = 0$, we have that $nz \in L$. In $S^{-1}F$, nz is a rational multiple of x. Therefore, z is a rational multiple of x. Thus, $z \in L$ and $\overline{z} = 0$. ■

For a finitely generated $\mathbb{Z}$-module M, let $d(M) = \dim_{\mathbb{Q}}(S^{-1}M)$. We've already seen that if M is finitely generated then $d(M) < \infty$.

Claim. $d(F \,/\, L) < d(F)$

Proof. Recall that

$$S^{-1}({}^{F}\big/_{L}) \cong {}^{S^{-1}F}\big/_{S^{-1}L}.$$

Therefore,

$$\dim S^{-1}({}^{F}\big/_{L}) = \dim(S^{-1}F) - \underbrace{\dim(S^{-1}L)}_{1}.$$

■

We will now show that if F is a finitely generated torsion free module then F is free by induction on $d(F)$.

Base case: $d(F) = 0$

$$d(F) = 0 \Rightarrow S^{-1}F = 0 \Rightarrow F = 0 \quad \text{b/c } F \text{ is torsion free.}$$

Inductive step: Pick $0 \neq x \in F$. Let $L = \mathbb{Q}x \cap F \subset S^{-1}F$. By claim 2, $L \cong \mathbb{Z}$ $(L = \mathbb{Z}y)$. By claim 3, $F \,/\, L$ is torsion free. By claim 4, $d(F \,/\, L) < d(F)$. By our inductive step, $F \,/\, L$ is free.

> **Remark** (Situation).
>
> $$0 \to L \to F \to {}^{F}\big/_{L} \to 0.$$
>
> We want to show that F is free.

Lemma 3.3.5. R is any ring $M \subset N$ is an R-module such that $E = N \,/\, M$ is free. Then $N \cong E \oplus M$ i.e.

$$0 \to M \to N \to \underbrace{E}_{\text{free}} \to 0.$$

Main idea. Consider the quotient map π. Pick basis $e_1, \ldots, e_n$ of E. Pick $x_1, \ldots, x_n \in N$ such that $\pi(x_i) = e_i$. By mapping property for free modules, $\exists$ map of R-modules

$$\begin{aligned} \phi : E &\longrightarrow N \\ e_i &\longmapsto \phi(e_i) = x_i. \end{aligned}$$

Note. $\pi \circ \phi = id_E$

Then $N = M \oplus \mathrm{Im}(\phi)$ and $\pi : \mathrm{im}(\phi) \to E$ is an isomorphism. ■

The result now follows from the lemma. ■

Lecture 17: Seventeenth Lecture

15 Feb. 02:00

Proposition 3.3.1. Say M is a finitely generated $\mathbb{Z}$-module. Then

$$M \cong M_{\text{tors}} \oplus \underbrace{M \big/ M_{\text{tors}}}_{\text{free}}.$$

Proof. $M \,/\, M_{\text{tors}}$ is torsion-free and finitely generated. Therefore, $M \,/\, M_{\text{tor}}$ is free. As a SES,

$$0 \to M_{\text{tors}} \to M \to M \big/ M_{\text{tors}} \to 0.$$

By final lemma from last time, $\exists \phi$ such that $\pi \circ \phi = id$. Therefore,

$$M = M_{\text{tors}} \oplus \underbrace{\mathrm{im}(\phi)}_{= M \,/\, M_{\text{tors}}}.$$

■

Remark. If M finitely generated $\mathbb{Z}$-module, then M_{tors} is finite.

Proof. M_{tors} is finitely generated because $\mathbb{Z}$ is noetherian. Let $x_1, \ldots, x_n \in M_{\text{tors}}$ generate. Then $\exists 0 \neq N \in \mathbb{Z}$ such that $Nx_i = 0$ for every i. Therefore, $N \cdot x = 0$ for every $x \in M_{\text{tors}}$. So M_{tors} is naturally a $\mathbb{Z} \,/\, N\mathbb{Z}$ module. Therefore, $x_1, \ldots, x_n$ generate M_{tors} as a $\mathbb{Z} \,/\, N\mathbb{Z}$ module. We have a surjection

$$\left(\mathbb{Z} \big/ N\mathbb{Z} \right)^n \to M_{\text{tors}}.$$

■

3.3.2 Back to Structure Theorem

To prove the main theorem (i.e., every finitely generated $\mathbb{Z}$-module is $\oplus$ of cyclic modules), it sufficies to treat the case of a finite module.

If R and S are rings and M and N are R and S-modules then $M \oplus N$ is naturally an $R \times S$-module.

$$(r, s) \cdot (m, n) = (rm, sn).$$

And every $R \times S$-module has this form.

Let $L = R \times S$-module. Put $e = (1, 0)$, $f = (0, 1)$. These are idempotents in $R \times S$. Let $M = eL$ and $N = fL$. Then

$$L \cong M \oplus N.$$

Given $x \in L$, $x = 1 \cdot x = (e + f)x = -ex + fx$.

Say M is a finite $\mathbb{Z}$-module. $\exists N \in \mathbb{Z}$ such that $Nx = 0$ for every $x \in M$. Therefore, M is a $\mathbb{Z} / N\mathbb{Z}$-module. Factor N as $p_1^{e_1} \cdots p_r^{e_r}$, where p_i 's are distinct primes. By Chinese Remainder Theorem,

$$\mathbb{Z} \big/ N\mathbb{Z} \cong \mathbb{Z} \big/ p_1^{e_1}\mathbb{Z} \times \cdots \mathbb{Z} \big/ p_r^{e_r}\mathbb{Z}.$$

Thus, $M = M_1 \oplus \cdots \oplus M_r$, where M_i is a $\mathbb{Z} / p_i^{e_i}\mathbb{Z}$-module. Now it suffices to show that finitely generated $\mathbb{Z} / p^r\mathbb{Z}$-module is a $\oplus$ of cyclic modules.

Let M be a $\mathbb{Z} / p^r\mathbb{Z}$-module. Choose r to be minimal (e.g. if $p^{r-1}x = 0\ \forall x \in M$ then M is a $\mathbb{Z} / p^{r-1}\mathbb{Z}$-module, replace r with $r-1$). Therefore, $\exists x \in M$ such that $p^{r-1}x \neq 0$ and $\operatorname{ord}(x) = p^r$. The submodule generated by x is $\cong \mathbb{Z} / p^r\mathbb{Z}$.

Remark. If M is an R-module and $x \in M$. Then $\langle x \rangle =$ submodule generated by x. To understand this consider

$$\begin{aligned} \phi : R &\longrightarrow M \\ a &\longmapsto \phi(a) = ax. \end{aligned}$$

Then $\operatorname{im}(\phi) = \langle x \rangle$. By first isomorphis theorem, $\langle x \rangle \cong R / \ker(\phi)$, where

$$\ker(\phi) = \{a \in R \mid ax = 0\}.$$

This is denoted $\operatorname{ann}(x)$ and is known as the "annhilator" of x.

3.3.3 General discussion

Definition 3.3.1. Given an R-submodule $M \subset N$, a complementary submodule is $M' \subset N$ such that $N = M + M'$ and $0 = M \cap M'$ i.e. $N = M \oplus M'$ (internal $\oplus$).

Definition 3.3.2. We say a SES

$$0 \to M \xrightarrow{i} N \xrightarrow{\pi} L \to 0$$

is split if $\exists$ complementary submodule M' to M.

Remark. $\pi|_{M'} : M' \to L$ is an isomorphism.

Proposition 3.3.2. The following are equivalent:

(1) The SES is split

(2) $\exists \phi : L \to N$ such that $\pi \circ \phi = id_L$ $[M' = \operatorname{im}(\phi\ ]$

(3) $\exists \psi : N \to M$ such that $\psi \circ i = id_M$ $[M' = \ker \psi\ ]$

Remark. The lemma from last times says that if L is free then any SES as above is split. In fact, L is projective iff any such SES splits.

Definition 3.3.3. M is an injective module if any SES as above splits.

Remark. M is injective if and only if whenever $M \subset N$, $\exists$ complementary submodule M' to M.

Example. $2\mathbb{Z} \subset \mathbb{Z}$ has no complementary submodule. Therefore, $\mathbb{Z}$ is not injective as a $\mathbb{Z}$-module.

The SES

$$0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

is not split.

3.3.4 Back to Structure Theorem Again

Problem 3.3.8. Now we want to show that $\mathbb{Z}/p^r\mathbb{Z}$ is injective as a module over itself. Why?

Answer. Let M be a finitely generated $\mathbb{Z}/p^r\mathbb{Z}$-module with r minimal. Pick $x \in M$ such that $p^{r-1}x \neq 0$. Then

$$\underbrace{\langle x \rangle}_{=\mathbb{Z}/p^r\mathbb{Z}} \subset M.$$

If $\langle x \rangle$ is injective then $\exists$ a complementary module to $\langle x \rangle$, so $M = \langle x \rangle \oplus \underbrace{(?)}_{\text{smaller, so continue by induction}}$

⊛

Example. $M = \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ and we think of M as a $\mathbb{Z}/p^2\mathbb{Z}$-module. For $0 \neq x \in M$,

$$\langle x \rangle \cong \mathbb{Z}/p\mathbb{Z}.$$

This is not injective as a $\mathbb{Z}/p^2\mathbb{Z}$-module

Remark (Reason)**.**

$$0 \to p\mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0.$$

This does not split. Therefore, $\mathbb{Z}/p\mathbb{Z}$ is not injective as a $\mathbb{Z}/p^2\mathbb{Z}$-module.

Example. $M = \mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. $x = (p, 0)$. $\langle x \rangle = p\mathbb{Z}/p^2\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z}$. $\langle x \rangle$ is not injective as a module and does not split off M as a summand.

Lecture 18: Eighteenth Lecture

17 Feb. 02:00

Theorem 3.3.2 (Baer's Criterion)**.** Let R be any commutative ring. An R-module M is injective if and only if whenever $\phi : I \to M$ is a map of R-modules with $I \subset R$ an ideal, $\exists$ map of R-modules $\psi : R \to M$ such that $\psi|_I = \phi$.

Example. $\mathbb{Q}$ is injective as a $\mathbb{Z}$-module. Let $\phi : I \to \mathbb{Q}$ be given. (Say $I \neq 0$). We know $I = n\mathbb{Z}$ for some $n > 0$. Let $x = \phi(n) \in \mathbb{Q}$. Define

$$\begin{aligned} \psi : \mathbb{Z} &\longrightarrow \mathbb{Q} \\ 1 &\longmapsto \psi(1) = \frac{x}{n}. \end{aligned}$$

Then

$$\psi(n) = n\psi(1) = x = \phi(n).$$

Example. $\mathbb{Z}$ is not injective as a $\mathbb{Z}$-module. Take $I = 2\mathbb{Z}$ ($I \cong \mathbb{Z}$ as a $\mathbb{Z}$-module). Define

$$\begin{aligned} \phi : I &\longrightarrow Z \\ 2 &\longmapsto \phi(2) = 1. \end{aligned}$$

Then $\nexists \psi : \mathbb{Z} \to \mathbb{Z}$ extending ϕ because

$$2 \cdot \psi(1) = \psi(2) = \phi(2) = 1$$

and $\frac{1}{2} \notin \mathbb{Z}$.

Example. $R = \mathbb{Z} / p^2\mathbb{Z}$. R is injective as an R-module. Let $\phi : I \to R$ be given. Ideals of R are (0), (p), (1).

Case 1: $I = (0)$.

Then we have that $\phi = 0$, take $\psi = 0$.

Case 2: $I = (1)$.

Take $\psi = \phi$.

Case 3: $I = (p)$.

Then ϕ is determined by $\phi(p)$.

$$p \cdot \phi(p) = \phi(p^2) = 0.$$

Therefore, $\phi(p) = pa$, for some $a \in \mathbb{Z} / p^2\mathbb{Z}$. Define

$$\begin{aligned} \psi : R &\longrightarrow R \\ 1 &\longmapsto \psi(1) = a. \end{aligned}$$

Then

$$\psi(p) = p \cdot \psi(1) = p \cdot a = \phi(p).$$

Example. $R = \mathbb{Z} / p^r\mathbb{Z}$. Let $\phi : I \to R$ be given. $I = (p^s)$ for $0 \leq s \leq r$. Then

$$p^{r-s} \cdot \phi(p^s) = \phi(p^r) = 0.$$

Therefore, $\phi(p^s) = p^s \cdot a$, for some $a \in \mathbb{Z} / p^r\mathbb{Z}$. Define ψ by $1 \mapsto a$.

Proof of Baire's Criterion.

$\Leftarrow$ Let M be given and suppose the criterion holds. Then we want to show that M is an injective module. Let $i : M \to N$ be an injection of R-modules. Then we want to show that $i(M)$ has a complementary module in N. It is sufficient to show that $\exists s : N \to M$ such that $s \circ i = \mathrm{id}_M$ (complementary module is $\ker s$).

To begin, define s on $i(M)$ to be the inverse of i i.e. $s(i(x)) = x$ for every $x \in M$. We will then keep "enlarging the domain" of S. Suppose we have some submodule $i(M) \subset N_1 \subset N$ such that we have defined $s : N_1 \to M_1$. Let $x \in N$ such that $x \notin N_1$. Put $N_2 = N_1 + R_x$. We want to extend s to N_2.

Let $I = \{a \in R \mid ax \in N_1\}$. This is an ideal of R. We can define $\phi : I \to M$ by $a \mapsto s(ax)$. By our assumption, $\exists \psi : R \to M$, extending ϕ. Define s on N_2 by $s(n_1 + ax) = s(n_1) + \psi(a)$. Then s and ψ agree on the intersection, so we can path them together. Define

$$\Sigma = \left\{ (s, N') \mid {}^{\quad i(M) \subset N' \subset N}_{S : N' \to M, \ \ \text{inverse to } i} \right\}.$$

We then consider the ordering $(s_1, N_1') \leq (s_2, N_2')$ if $N_1' \subset N_2'$ and $s_2|N_1' = s_1$. By Zorn's lemma, there exists a maximal element of Σ. From the previous paragraph, we have that the maximal $N' = N$.

$\Rightarrow$ Now suppose M is injective. Let $\phi : I \to M$ be given.

$$\begin{tikzcd} M \arrow[r, hook] & N \arrow[l, bend right, "s"'] \\ I \arrow[u, "\phi"] \arrow[r, hook] & R \arrow[u, "t"'] \arrow[ul, dashed, "\psi"] \end{tikzcd}$$

Note (Pushout construction)**.** Given a diagram as above, the pushout is the module

$$N = {}^{M \oplus R}\Big/_{\{(\phi(x), 0) - (0, x) \mid x \in I\}}.$$

The point is $(\phi(x), 0) = (0, x)$ in N.

Since $M \hookrightarrow N$ is injective, it has a one-sided inverse s because M is injective. Thus, $\psi = s \circ t$.

■

3.3.5 Summary of Structure Theorem Proof

We have a finitely generated $\mathbb{Z}$-module M .

- If $M \,/\, M_{\text{tors}}$ is finitely generated and torsion free, then it is free
- Since $M \,/\, M_{\text{tors}}$ is free, the follow SES splits:

$$0 \longrightarrow M_{\text{tors}} \longrightarrow M \longrightarrow {}^{M}\Big/_{M_{\text{tors}}} \longrightarrow 0.$$

  Therefore, $M = M_{\text{tors}} \oplus \underbrace{{}^{M}\Big/_{M_{\text{tors}}}}_{\text{free}}$

- M_{tors} is finitely generated (because $\mathbb{Z}$ is noetherian) and torsion. Therefore, it is finite. Thus, it is a $\mathbb{Z} \,/\, N\mathbb{Z}$-module for some $N \geq 1$.
- CRT. $M_{\text{tors}} = \bigoplus_p M_p$, M_p is a $\mathbb{Z}$-module that is killed by a power of p. $M_p = 0$ for all but finitely many p.
- Fix p. Let r be minimal such that $p^r M_p = 0$. Choose $x \in M_p$ of order p^n. Then $\langle x \rangle \cong \mathbb{Z} \,/\, p^r\mathbb{Z}$
- Since $\mathbb{Z} \,/\, p^r\mathbb{Z}$ is injective as a module over itself, $\langle x \rangle$ is injective as a module. Thus,

$$M_p \cong \langle x \rangle \oplus \underbrace{\text{(smaller mod)}}_{\text{sum of cyclic mod by induction}}.$$

Lecture 19: Nineteenth Lecture

20 Feb. 02:00

Remark. The decomposition of M into a $\oplus$ of cyclic modules is not unique.

$$\mathbb{Z}\Big/_{6\mathbb{Z}} \cong \mathbb{Z}\Big/_{2\mathbb{Z}} \oplus \mathbb{Z}\Big/_{3\mathbb{Z}}.$$

In fact, CRT completely explains failure of uniqueness.

Proposition 3.3.3 (A uniqueness result)**.** Let M be a finitely generated $\mathbb{Z}$-module. Then $\exists$ isomorphism $M \cong \bigoplus_{i=1}^n C_i$, where C_i is either $\mathbb{Z}$ or a finite cyclic group of prime power order. If $M = \bigoplus_{i=1}^s C_i$ is a second such decomposition then $r = s$ and $\exists$ permutation $\sigma \in S_r$ such that

$C_i' \cong C_{\sigma(i)}$

Proof. If $S = \mathbb{Z} \setminus \{0\}$. Then

$$\#\{i \mid C_i = \mathbb{Z}\} = \dim_{\mathbb{Q}}(S^{-1}M) = d.$$

Therefore,

$$\#\{i \mid C_i' = \mathbb{Z}\} = d.$$

Assume $C_1 = \cdots = C_d = \mathbb{Z}$, $C_1' = \cdots C_d' = \mathbb{Z}$

Claim. $\bigoplus_{i=d+1}^{r} C_i \cong \bigoplus_{i=d+1}^{s} C_i'$

Proof. Both are M_{tors} ■

By looking at p-power torsion, we reduce to the case where C_i and C_i' are cyclic of p-power order. Now we proceed by proof by example (lol)

Problem 3.3.9. Why are $\mathbb{Z} / p^5\mathbb{Z} \oplus \mathbb{Z} / p^5\mathbb{Z} \oplus \mathbb{Z} / p^6\mathbb{Z}$ and $\mathbb{Z} / p^4\mathbb{Z} \oplus \mathbb{Z} / p^6\mathbb{Z} \oplus \mathbb{Z} / p^6\mathbb{Z}$ not isomorphic?

Answer. One has more elements of order p^6 then the other one. More generally, we can distinguish by counting elements of order p^i for all i. ⊛

■

Proposition 3.3.4 (Another uniqueness result). Let M be a finitely generated $\mathbb{Z}$-module. Then for $d_i \geq 2$, $\exists$ an isomorphism

$$M \cong \mathbb{Z}^r \oplus {}^{\mathbb{Z}}\big/_{d_1\mathbb{Z}} \oplus \cdots \oplus {}^{\mathbb{Z}}\big/_{d_n\mathbb{Z}} \quad \text{such that } d_2|d_1,\, d_3|d_2,\, \ldots .$$

This is unique.

Basic idea. Start by writing $M = \oplus(\mathbb{Z}'s$ or cyclic of prime power order). Say $p_1, \ldots p_n$ are the primes appearing. Say we have $\mathbb{Z} / p_1^{e_1}$, $\mathbb{Z} / p_2^{e_2}$, $\ldots$ among our summands with $e_1, \ldots, e_m$ maximal. By CRY,

$$ {}^{\mathbb{Z}}\big/_{p_1^{e_1}} \oplus {}^{\mathbb{Z}}\big/_{p_2^{e_2}} \oplus \cdots \oplus {}^{\mathbb{Z}}\big/_{p_m^{e_m}} = {}^{\mathbb{Z}}\big/_{d_1}.$$

for $d_1 = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$. Next say $\mathbb{Z} / p_1^{f_1}, \ldots \mathbb{Z} / p_m^{f_m}$ are next biggest remaining cyclic modules. Then $d_2 = p_1^{f_1} \cdots p_m^{f_m}$ ■

3.3.6 Structure Theorem for PIDs

Theorem 3.3.3. Let R be a PID, M be a finitely generated R-module. Then M is a $\oplus$ of R 's and $R / (a)$'s.

Remark. We have the following useful properties:

(1) If $a, b \in R$ are coprime, $R / (ab) \cong R / (a) \oplus R / (b)$. Therefore, if $a = \pi_1^{e_1} \cdots \pi_r^{e_r}$ with π_i disjoint prime elements. Then

$$ {}^{R}\big/_{(a)} \cong {}^{R}\big/_{(\pi_1^{e_1})} \oplus \cdots \oplus {}^{R}\big/_{(\pi_r^{e_r})}.$$

(2) Same uniqueness statements.

Example. $R = \mathbb{C}[t]$. This is a PID.

Remark. If F is a field, $F[t]$ is a PID and the prime elements are the irreducible polynomials.

Claim. The irreducible polynomials of R are $t - \alpha$ for some $\alpha \in \mathbb{C}$.

Proof. Say $h(t)$ is a monic irreducible polynomial in $\mathbb{C}[t]$. Because $\mathbb{C}$ is algebraically closed, $\exists \alpha \in \mathbb{C}$ such that $h(\alpha) = 0$. Therefore, $t - \alpha | h(t)$. Since $h(t)$ is irreducible, it must be the case that $h(t) = t - \alpha$. ∎

Remark (Structure Theorem for Finitely Generated R-modules)**.** In the case of $R = \mathbb{C}[\approx]$, we have a finite $\oplus$ of $\mathbb{C}[t]$'s and

$$\mathbb{C}[t] \Big/ \langle (t-\alpha)^n \rangle ' s.$$

Application: Jordan Normal Form

Definition 3.3.4. A Jordan block is a $n \times n$ matrix of the form

$$\begin{bmatrix} \alpha_1 & 1 & \cdots & 0 \\ 0 & \alpha_2 & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_n \end{bmatrix}.$$

Example. $\begin{bmatrix} \alpha \end{bmatrix}$, $\begin{bmatrix} \alpha & 1 \\ 0 & \alpha \end{bmatrix}$, $\begin{bmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \\ 0 & 0 & \alpha \end{bmatrix}$

Definition 3.3.5. Given an $n \times n$ complex matrix M, $\exists$ an invertible matrix A such that

$$AMA^{-1} = \begin{bmatrix} J_1 & 0 & \cdots & 0 \\ \vdots & J_2 & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_m \end{bmatrix}.$$

Remark. If all the blocks are size $|x|$ then M is diagonalizable.

Let V be a finite dimensional $\mathbb{C}$-vector space. Let $T : V \to V$ be a linear operator. We can give V the structure of a $\mathbb{C}[t]$-module via $t \cdot v = T(v)$.

Remark. More generally, if $f(t) \in \mathbb{C}[t]$ then $f(t) \cdot v = f(T)(v)$, where $f(T)$ is another linear operator.

As a $\mathbb{C}[t]$-module, we have

$$V \cong \mathbb{C}[t]^{\oplus r} \oplus \mathbb{C}[t] \Big/ \langle (t-\alpha_1)^{e_1} \oplus \cdots \mathbb{C}[t] \Big/ \langle (t-\alpha_m)^{e_m} \cdot$$

Our first observation is that $r = 0$ because $\dim_{\mathbb{C}}(V) < \infty$, but $\dim_{\mathbb{C}}(\mathbb{C}[t]) = \infty$.

Example. Say $V \cong \mathbb{C}[t] \,/\, (t^e)$. Let $\phi : V \to \mathbb{C}[t] \,/\, (t^e)$ be the isomorphism.

> **Note.** The key point is that ϕ is an isomorphism of $\mathbb{C}$-vector spaces such that
> $$\phi(Tv) = t \cdot \phi(v).$$

Let $x_1, \ldots, x_n$ be the $\mathbb{C}$-basis $1, t_1, \ldots, t^{e-1}$ of $\mathbb{C}[t] \,/\, (t^e)$. Then

$$\begin{aligned} tx_i &= x_{i+1} \quad \text{for } 1 \leq i \leq e-1, \\ tx_e &= 0. \end{aligned}$$

Put $y_i = \phi^{-1}(x_i)$. Then $y_1, \ldots, y_n$ is a basis for V.

$$\begin{aligned} T(y_i) &= y_{i+1}, \quad \text{for } 1 \leq i \leq e-1 \\ T(y_e) &= 0. \end{aligned}$$

Really use basis $ye, ye_1, \ldots, y_1$ (Andrew messed up). Then the matrix for T is a Jordan block of size e with 0's on the main diagonal.

Lecture 20: Tensor Products

Suppose we have a ring homomorphism $\phi : R \to S$ is a ring homomorphism. 22 Feb. 02:00

> **As previously seen.** Recall restriction of scalars i.e. if M is an S-module then we can give M the structure of an R-module by defining $r \cdot m = \phi(r) \cdot m$ for $r \in R$ and $m \in M$.

Remark. We also have extension of scalars, starting with an R-module and makes an S-module.

Say M is a finitely presented R-module. Then $\exists$ map $f : R^m \to R^n$ such that

$$M \cong \operatorname{coker}(f) = {R^n}\big/{\operatorname{im}(f)}.$$

Concretely, f is specified by an $n \times m$ matrix with entries in R.

Definition 3.3.6. Let $f' : S^m \to S^n$ be the map given by taking the matrix for f and applying ϕ to each entry. Define $\phi_*(M)$ to be the S-module $\operatorname{coker}(f')$. Then $\phi_*(M)$ is the extension of scalars of M from R to S.

Exercise. Show this is canonically independent of presentation.

Example. $\phi_*(R) = S$. Then $R = R \,/\, (0)$, $R = \operatorname{coker}(0 \mapsto R)$. Therefore, $\phi_*(R) = \operatorname{coker}(0 \mapsto S) = S$. Note

$$\phi^*(\phi_*(R)) = S.$$

Thought of as an R-module.

Example. $\phi_*(M \oplus N) \cong \phi_*(M) \oplus \phi_*(N)$. Therefore, $\phi_*(R^n) = S^n$.

Example. $\phi : \mathbb{Z} \to \mathbb{Q}$. $M = \mathbb{Z} \,/\, 3\mathbb{Z}$. Then

$$\phi_*(M) = {\mathbb{Q}}\big/{3\mathbb{Q}} = 0.$$

Using above notation, $f : \mathbb{Z} \xrightarrow{3} \mathbb{Z}$, where $M = \operatorname{coker}(f)$ and $f'\mathbb{Q} \xrightarrow{3} \mathbb{Q}$ with $\phi_*(M) = 0 = \operatorname{coker}(f')$.

Example. $\phi : \mathbb{Q} \to \mathbb{C}$. $\phi_*(\mathbb{Q}^n) = \mathbb{C}^n$. If V is an n-dimensional $\mathbb{Q}$-vector space then $\phi_*(V)$ is an n-dimensional $\mathbb{C}$-vector space. If $T : V \to V$ is a $\mathbb{Q}$-linear operator then $\exists$ induced operator $\phi_*(T) : \phi_*(V) \to \phi_*(V)$. $\phi_*(T)$ has the "same" matrix as T.

Example. If $\phi : R \to R \,/\, I$ then $\phi_*(M) = M \,/\, IM$.

3.3.7 $\mathbb{Z}$ Tensor Products

If M and N are $\mathbb{Z}$-modules a tensor product is a $\mathbb{Z}$-module T equipped with a $\mathbb{Z}$-bilinear map $M \times N \to T$ that is universal i.e. if $M \times N \to T'$ is some other bilinear map ! $\mathbb{Z}$-module homomorphism $T \xrightarrow{\alpha} T'$ such that

$$\begin{tikzcd}
M \times N \arrow[r, "b"] \arrow[dr, "b'"'] & T \arrow[d, "a"] \\
& T'
\end{tikzcd}$$

Easy to see that it is unique if it exists.

We construct as follows:

$$\frac{(\text{free } \mathbb{Z}\text{-module with basis symbols } [m,n] \text{ for } m \in M \text{ and } n \in N)}{\text{Submodule generated by } \substack{[a_1m_1+a_2m_2,n]=a_1[m_1,n]+a_2[m_2,n] \\ [m,a_1n_1+a_2n_2]=a_1[m,n_1]+a_2[m,n_2]}}.$$

We have the following properties:

(1) $\mathbb{Z} \otimes M \cong M$

(2) $M \otimes N \cong N \otimes M$

(3) $(M_1 \oplus M_2) \otimes N \cong (M_1 \otimes N) \oplus (M_2 \otimes N)$

(4) $M \otimes -$ is a right exact functor i.e. if

$$0 \to N_1 \to N_2 \to N_3 \to 0$$

is a SES of $\mathbb{Z}$-modules then

$$M \otimes N_1 \to M \otimes N_2 \to M \otimes N_3 \to 0$$

is exact

Notation. $M \otimes N$ or $M \underset{\mathbb{Z}}{\otimes} N$. For $m \in M$, $n \in N$ we write $m \otimes n$ for the class of $[m,n]$ in $M \otimes N$.

Example. $\mathbb{Z} \,/\, 3\mathbb{Z} \underset{\mathbb{Z}}{\otimes} \mathbb{Z} \,/\, 5\mathbb{Z}$.

$$\underbrace{\mathbb{Z}/5\mathbb{Z} \xrightarrow{3} \mathbb{Z}/5\mathbb{Z}}_{\text{surjective}} \to \mathbb{Z}/5\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z} \to 0.$$

Alternatively, consider $m \otimes n \in \mathbb{Z} \,/\, 3\mathbb{Z} \otimes \mathbb{Z} \,/\, 5\mathbb{Z}$. Then

$$\begin{aligned} 3(m \otimes n) &= m \otimes n + m \otimes n + m \otimes n \\ &= (3m) \otimes n = 0. \end{aligned}$$

Similarly,

$$5(m \otimes n) = m \otimes (5n) = 0.$$

> Thus, $M \otimes N$ killed by $(3,5) = (1)$.

3.3.8 R Tensor Products

Let R be a general ring with M and N two R-modules. Then $M \underset{R}{\otimes} N$ receives the universal R-bilinear map from $M \times N$.

If $\phi : R \to S$ is a ring homomorphism then S is naturally an R-module. For an R-module M,

$$\phi_*(M) = S \underset{R}{\otimes} M.$$

The reason for this is as follows. Pick a presentation for M. Then

$$R^m \xrightarrow{f} R^n \to M \to 0.$$

Therefore,

$$\underbrace{S \otimes R^m}_{S^m} \xrightarrow{f} \underbrace{S \otimes R^n}_{S^n} \to \underbrace{S \otimes M}_{\phi_*(M)} \to 0.$$

Let $S \subset R$ be a multiplicative set.

$$\begin{aligned} \phi : R &\longrightarrow S^{-1}R \\ x &\longmapsto \frac{x}{1}. \end{aligned}$$

Then $\phi_*(M) = S^{-1}M = S^{-1}R \otimes M$.

Chapter 4

Field theory

Contrary to popular belief, this is not the study of fields but rather field extensions.

Lecture 21: Field Extensions introduction

24 Feb. 02:00

Definition 4.0.1. Let F be a field. A field extension of F is a pair (E, i) where E is a field and $i : F \to E$ is a field homomorphism.

Remark. i is injective because $\ker(i)$ is a proper ideal of F i.e. its (0). Therefore, we can regard F as a subfield of E

Notation. We write E/F to indicate E is an extension of F (i is implicit).

Definition 4.0.2. Let E/F be given. An element of $\alpha \in E$ is algebraic over F is $\exists$ non-zero $f \in F[x]$ such that $f(\alpha) = 0$. α is transcendental if it is not algebraic.

Example. $\mathbb{C} / \mathbb{Q}$. The elements of $\mathbb{C}$ that are algebraic over $\mathbb{Q}$ are just the algebraic numbers.

Example. Every element of $\mathbb{C}$ is algebraic over R. The reason: if $z \in \mathbb{C}$ then $z + \overline{z}$, $z\overline{z}$ are real and z is a root of the polynomial

$$(x - z)(z - \overline{z}) = x^2 - (z + \overline{z})x + z\overline{z} \in \mathbb{R}[x].$$

Definition 4.0.3. E/F is algebraic if every element of E is algebraic over F.

Definition 4.0.4. E/F is transcendental if not algebraic.

Example. The following are some examples:

- $\mathbb{C}/\mathbb{R}$ is an algebraic extension
- $\mathbb{Q}(i)/\mathbb{Q}$ is an algebraic extension.
- $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$ is an algebraic extension because algebraic numbers are a subfield.
- $\mathbb{C}/\mathbb{Q}$ is a transcendental extension.
- $\mathbb{C}(x)/\mathbb{C}$ is a transcendental extension.

Definition. If E/F is an extension then we can think of E as an F-vector space.

Definition 4.0.5. The degree of E/F, denoted $[E : F]$, is the dimension of E as an F-vector space.

Definition 4.0.6. E/F is finite if $[E : F] < \infty$.

Proposition 4.0.1. If E/F is finite then it is algebraic.

Proof. Given $\alpha \in E$, the elements $1, \alpha, \alpha^2, \dots$ must be F-linearly dependent because they belong to a finite dimensional F-vector space. A linear dependence gives a polynomial that satisfies. ■

Example. Let $\overline{\mathbb{Q}} \subset \mathbb{C}$ denote the set of all algebraic numbers. We have shown that this is a subfield of $\mathbb{C}$.

$$[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty.$$

Therefore, $\overline{\mathbb{Q}} \,/\, \mathbb{Q}$ is an algebraic extension of ∞ degree.

Proposition 4.0.2 (Transitivity of degree)**.** Given E/F and K/E

$$[K : F] = [K : E][E : F].$$

Proof. Put $n = [K : E]$ and $m = [E : F]$. Let $x_1, \dots, x_n$ be an E-basis of K and $y_1, \dots, y_m$ an F-basis of E.

Claim. $\{x_i, y_j\}_{\substack{1 \le i \le n \\ 1 \le j \le m}}$ is an F-basis of K.

Proof. Let $\alpha \in K$ be given. Then we first want to show that $\alpha \in \operatorname{span}(x_i, y_j)$. Since the x_i's are an E-basis of K we can write

$$\alpha = \sum_{i=1}^{n} \beta_i x_i, \quad \beta_i \in E.$$

Since the y_i 's are an F-basis of E, we can write

$$\beta_i = \sum_{j=1}^{m} \gamma_{i,j} y_j, \quad \gamma_{i,j} \in F.$$

Thus,

$$\alpha = \sum_{i=1}^{n} \sum_{j=1}^{m} \gamma_{i,j} x_i y_j.$$

Now we must show that $\{x_i, y_j\}_{\substack{1 \le i \le n \\ 1 \le j \le m}}$ are F-linearly independent. Suppose

$$\alpha = \sum_{i=1}^{n} \sum_{j=1}^{m} \gamma_{i,j} x_i y_j = 0.$$

Then

$$\alpha = \sum_{i=1}^{n} \left(\underbrace{\sum_{j=1}^{m} \gamma_{i,j} y_j}_{\text{belongs to } E} \right) x_i = 0.$$

This is an E-linear dependence among $x_1, \ldots, x_n$. Therefore, it is trivial, i.e. for every i

$$\sum_{j=1}^{m} \gamma_{i,j} y_j = 0.$$

This is an F-linear dependence among $y_1, \ldots, y_m$. Thus, $\gamma_{i,j} = 0$ for every i, j. ■

Since $|\{x_i, y_j\}_{\substack{1 \le i \le n \\ 1 \le j \le m}}| = |\{x_i\}_{1 \le i \le n}||\{y_i\}_{1 \le i \le m}|$, the result follows directly from the claim. ■

Theorem. K/F is an extension and E is an intermediate field ($F \subset E \subset K$)

Corollary 4.0.1. Then $[E : F]$ and $[K : E]$ divide $[K : F]$.

Corollary 4.0.2. If the degree of K over F is prime then the only intermediate fields are K and F.

Example. $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Let $E = \mathbb{Q}(\sqrt{2})$. Therefore,

$$[K : \mathbb{Q}] = [K : E][E : \mathbb{Q}].$$

Note that $K = E(\sqrt{3})$. Easy to see that $1, \sqrt{3}$ spac K as an E-vector space. If $[K : E] \le 2$ then $[K : E] = 1$ or 2. If $[K : E] = 1$ then $K = E$ and $\mathbb{Q}(\sqrt{2})$ would contain $\sqrt{3}$. Thus, $[K : E] = 2$ and $[K : \mathbb{Q}] = 4$.

Proposition 4.0.3. Suppose that E/F is an extension and $\alpha \in E$ is algebraic over F. Then $F(\alpha)/F$ is a finite extension.

Proof. Put $F[\alpha]$ = smallest subring of E containing F and $\alpha = F\text{-span}(1, \alpha, \alpha^2, \ldots)$.

Claim. $F[\alpha]$ is finite dimensional over F.

Proof. We know $f(\alpha) = 0$ for some $f \in F[x]$ if $\deg(f) = n$ then $F[\alpha]$ is spanned by $1, \alpha, \ldots, \alpha^{n-1}$. ■

Claim. $F[\alpha]$ is actually a field and $F[\alpha] = F(\alpha)$.

Proof. Given $\beta \in F[\alpha]$. Once again, we have that $1, \beta, \beta^2, \ldots \in F[\alpha]$ must be F-linearly dependent. Therefore,

$$\beta^n + c_{n-1}\beta^{n-1} + \cdots + c_0 = 0.$$

Then

$$\frac{1}{c_0}(\beta^{n-1} + c_{n-1}\beta^{n-2} + \cdots + c_0) + \frac{1}{\beta} = 0.$$

Thus, $\frac{1}{\beta} \in F[\alpha]$. ■

■

Proposition 4.0.4. Given E/F and $\alpha_1, \ldots, \alpha_n \in E$ that are algebraic over F, the extension $F(\alpha_1, \ldots, \alpha_n)/F$ is finite.

Proof. Consider $F(\alpha_1, \alpha_2) = F(\alpha_1)(\alpha_2)$ If we continue, each iteration is finite by the previous claim. Then the whole thing is finite because degree is transitive. ■

Proposition 4.0.5. For any extension E/F, E/F is finite if and only if it is algebraic and finitely generated.

Proposition 4.0.6. For any extension E/F, the elements of E that are algebraic over F form a subfield.

Proof. If $\alpha, \beta \in E$ are algebraic over F then $F(\alpha, \beta)/F$ is finite. Therefore, it is algebraic. So $\alpha + \beta, \alpha\beta, \frac{\alpha}{\beta} \in F(\alpha, \beta)$ are algebraic over F. ■

Lecture 22: Basic Properties of Field Extensions

4.1 Characterstic

6 Feb. 02:00

Let F be a field. Then $\exists!$ ring homomorphism ϕ from $\mathbb{Z} \to F$ defined by $\phi(1) = 1 \in F$. There are two cases,

(1) ϕ is injective. Then $\mathbb{Z} \subset F$ and $\mathbb{Q} \subset F$. F has "characteristic 0"

(2) $\ker(\phi) \neq 0$. Then

$$\mathrm{im}(\phi) \cong \mathbb{Z}/\ker(\phi).$$

This is a domain because it is a subring of F. Therefore, $\ker(\phi)$ is a prime ideal such that $\ker(\phi) = (p)$ for some prime p. Thus, ϕ induces a field homomorphism

$$\underbrace{\mathbb{F}_p}_{\mathbb{Z}\,/\,p\mathbb{Z}} \to F.$$

Then F has "characteristic p".

Remark. If $F \to K$ is any field homomorphism then $\operatorname{char}(F) = \operatorname{char}(K)$.

4.2 Adjoining Elements

Suppose $E\,/\,F$ is a field extension and let $a \in E$ be algebraic over F. Then $\exists!$ ring homomorphism

$$\begin{aligned} \phi : F[x] &\longrightarrow E \\ h(x) &\longmapsto h(a). \end{aligned}$$

The $\ker(\phi)$ is a non-zero prime ideal ($\operatorname{im}(\phi)$ is a domain). Since $F[x]$ is a PID, $\ker(\phi) = ((f(x)))$ for some f. In fact, $\exists!$ monic $f(x)$ that generates $\ker(\phi)$.

Definition 4.2.1. This is called the minimal polynomial of a.

Remark. The minimal polynomial $f(x)$ of a is irreducible and has the following properties:

- If $g(x) \in F[x]$ such that $g(a) = 0$ then $f(x)|g(x)$.
  - The reason for this is that $g(a) = 0 \Rightarrow g \in \ker(\phi) = (f(x))$.

Example. We have the following examples:

- $E = \mathbb{C}$, $F = \mathbb{R}$, $a = i$. Then $f(x) = x^2 + 1$.
- $E = \mathbb{C}$, $F = \mathbb{Q}$, $a = \sqrt{2} + \sqrt{3}$. Then $f(x)$ is some degree 4 polynomial.
- $E = \mathbb{C}$, $F = \mathbb{Q}(\sqrt{2})$, $a = \sqrt{2} + \sqrt{3}$. Then $f(x) = (x - \sqrt{2})^2 - 3$.

Proposition 4.2.1. Let E/F and $a \in E$ be as above, let $f(x) \in F[x]$ be the minimal polynomial of a. Then

$$F[x] \big/ (f(x)) \cong F[a].$$

Proof. Recall

$$\begin{aligned} \phi : F[x] &\longrightarrow E \\ h(x) &\longmapsto h(a). \end{aligned}$$

Then $\operatorname{im}(\phi) = F[a] = F(a)$. By 1st Isomorphism Theorem,

$$F[x] \big/ \ker(\phi) \cong \operatorname{im}(\phi) = F(a).$$

Since $\ker(\phi) = (f(x))$, we are done. ■

Definition 4.2.2. Let $E\,/\,F$ and $K\,/\,F$ be two extensions of F. An F-homomorphism (or F-embedding) is a field homomorphism $E \xrightarrow{\gamma} K$ that is the identity on F.

More carefully, $E\,/\,F$ is really a field homomorphism $\alpha : F \to E$ and $K\,/\,F$ is $\beta : F \to K$. Then

γ is a field homomoprhism such that $\gamma \circ \alpha = \beta$.

Example. Let $\tau : \mathbb{C} \to \mathbb{C}$ be complex conjugation. Then τ is an $\mathbb{R}$-automorphism of $\mathbb{C}$.

Definition 4.2.3 (See Milne's Notes). Let F be a field, and let $f(x) \in F$ be an irreducible polynomial. A stem field for f is a pair $(E \,/\, F, a)$ for $a \in E$, such that $f(a) = 0$ and $E = F(a)$.

Note. f is the minimal polynomial of a.

Theorem 4.2.1. Let $f(x) \in F[x]$ be an irreducible polynomial.

(a) A stem field for f exists.

(b) Stem fields are unique in the following way: if $(E \,/\, F, a)$ and $(E' \,/\, F, a')$ are two stem fields then $\exists!$ F-isomorphism $\sigma : E \to E'$ such that $\sigma(a) = a'$.

Proof of (a). We have $E = F[x] \,/\, (f(x))$. This is a field because $f(x)$ is irreducible. Additionally, $\exists$ natural homomorphism $F \to E$, so E is an extension of F. Then let $a =$ img of x in E. Then $f(a) = 0$ and $(E \,/\, F, a)$ is a stem field. ■

Proof of (b). Let $(E \,/\, F, a)$ be as in part (a). Let $(E' \,/\, F, a')$ be a second stem field. Then $\exists!$ map $\phi : F[x] \to E'$ that is the identity on F and maps x to a'. We know that ϕ is surjective because $a' \in \operatorname{im}(\phi)$ and $E' = F(a')$. Then ϕ induces an isomorphism $\sigma : \underbrace{E}_{=F[x] \,/\, \ker(\phi)} \to E'$. Since $\phi(x) = a'$, we get $\sigma(a) = a'$.

Now we must show that σ is unique. Suppose that $\tau : E \to E'$ is an F-isomorphism such that $\tau(a) = a'$. Suppose $x \in E$. Then $x = \sum_{i=1}^{n} c_i \cdot a^i$ for $c_i \in F$. Then

$$\sigma(x) = \sum_{i=1}^{n} c_i \sigma(a)^i$$
$$\tau(x) = \sum_{i=1}^{n} c_i \tau(a)^i.$$

These are the same because $\tau(a) = \sigma(a) = a'$. ■

Remark. Suppose that $E \,/\, F$ and $K \,/\, F$ are two extensions and $\sigma : E \to K$ is a field homomorphism. Then σ being an F-homomorphism is the same as σ being an F-linear map.

Example. $(\mathbb{C} \,/\, \mathbb{R}, i)$ is a stem field for $x^2 + 1$ but $\tau : \mathbb{C} \to \mathbb{C}$ is an $\mathbb{R}$-isomorphism such that $\tau(i) = -i$. Therefore, the isomorphism is only unique in the sense that it must map the generator to the generator.

Example. $\alpha = 2^{\frac{3}{2}} \in \mathbb{R}$, $\beta = e^{2\pi i/3}(2^{\frac{3}{2}})$. Then $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are different subfields of $\mathbb{C}$. But, $\mathbb{Q}(\alpha) \,/\, \mathbb{Q}, \alpha)$ and $(\mathbb{Q}(\beta) \,/\, \mathbb{Q}, \beta)$ are both stem fields for $x^3 - 2$. From the theorem, $\exists!$ isomorphism $\sigma : \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$ such that $\sigma(\alpha) = \beta$.

Proposition 4.2.2. Let $(E \,/\, F, a)$ be a stem field for $f(x)$. Then $[E : F] = \deg f(x)$.

Proof. $E \cong F[x] \,/\, (f(x))$. If $f(x)$ has degree d then $1, x, \ldots x^{d-1}$ are an F-basis of E. ■

Lecture 23: Finite Fields

10 Mar. 02:00

Example. $F = \mathbb{Q}$, $E = \mathbb{Q}(2^{3/2})$, $f(x) = x^3 - 2$, $a = 2^{3/2}$. Then a is the only root of $f(x)$ in E because $E \subset \mathbb{R}$ and the other roots of f are complex.

Definition 4.2.4. Given any polynomial $f(x) \in F[x]$. A splitting field for f is a field extension E/F such that $f(x)$ factors into linear factors over E and E is generated by the roots of f.

Proposition 4.2.3. Splitting fields exist and are unique up to F-isomorphism.

Proof. To show they exist, we essentially iteratively create stem fields.

- Pick an irreducible factor $g(x)$ of $f(x)$
- $(E_0/F, a)$ be a stem field for g.
- Write $f(x) = (x-a)f_0(x)$ for $f_0(x) \in E_0[x]$
- Let E be an extension of E_0 (exists by induction on degree)
- E is splitting field for f.

To show uniqueness, Say E and E' are two splitting fields for f. Let $g(x)$ be an irreducible factor of $f(x)$. Since $g|f$ and f factors into degree 1 pieces, so does g. Therefore, $\exists$ root $a \in E$ and $a' \in E'$ of g. Let $E_0 = F(a) \subset E$ and $E_0' = F(a') \subset E'$

Note. E_0 and E_0' are stem fields for g. Therefore, $\exists\ !F$-isomorphism $E_0 \to E$ defined by $a \mapsto a'$.

Let $f(x) = (x-a)f_0(x) \in E_0[x] = (x-a')f_0(x) \in E_0'[x]$. Then E and E' are splitting fields for f_0 (rel to E_0). By induction on degree, $\exists E_0$-isomorphism from $E \to E'$. ■

Remark. If E and E' are splitting fields for f there will typically be many F-isomorphism $E \to E'$. When $E = E'$ there are typically non-trivial F-automorphisms from $E \to E$.

Example. $\mathbb{C}\,/\,\mathbb{R}$ is splitting field of x^2+1. $\mathbb{C}$ has two $\mathbb{R}$-automorphisms (id, complex conjugation).

Definition 4.2.5. Say f has no multiple roots. A marked splitting field is $(E\,/\,F, \alpha_1, \ldots, \alpha_n)$ such that $f(x) = \prod_{i=1}^n (x - \alpha_i)$ and $E = F(\alpha_1, \ldots, \alpha_n)$.

Now if $(E'\,/\,F, \alpha_1', \ldots, \alpha_n')$ is a second one. There must exist at most one F-isomorphism $\sigma : E \to E'$ such that $\sigma(\alpha_i) = \alpha_i'$.

However, σ does not have to exist in general.

Example. $F = \mathbb{Q}$, $f(x) = x^4 - 1$. $E = \mathbb{Q}(i)$ is a splitting field. $(E\,/\,\mathbb{Q}, 1, i, -1, -i)$, $(E\,/\,\mathbb{Q}, i, -i, 1, -1)$ are not isomorphic as marked splitting fields.

Example. $F = \mathbb{Q}$, $f(x) = \frac{x^5-1}{x-1}$ (roots are 5th roots of unity). $\zeta = e^{2\pi i/5}$. $E = \mathbb{Q}(\zeta)$. $(E\,/\,\mathbb{Q}, \zeta, \zeta^2, \zeta^3, \zeta^4)$, $(E\,/\,\mathbb{Q}, \zeta, \zeta^3, \zeta^4, \zeta^2)$ are not isomorphic as marked splitting fields.

4.3 Finite Fields

Definition 4.3.1. A finite field is a field with finitely many elements.

Say F is a finite field. Certainly, $\mathbb{Q} \not\subset F$. Therefore, $\text{char}(F) = p$ for some prime p and $\mathbb{F}_p \subset F$. Since F is finite, it is finite dimensional as an $\mathbb{F}_p$-vector space. Threfore, $F \cong \mathbb{F}_p^n$ as a vector space such that $\#F = p^n$.

Proposition 4.3.1. If F is a finite field then $F^\times$ is cyclic. More generally, if E is any field then any finite subgroup of $E^\times$ is cyclic.

Proof. Say $G \subset E^\times$ is finite. Write $G[n] = \{x \in G \mid x^n = 1\}$. Since the polynomimal $T^n - 1$ has $\leq n$ roots in E, it must be the case that $\#G[n] \leq n$.

Lemma 4.3.1. If G is a finite abelian group such that $\#G[n] \leq n$ then G is cyclic.

Proof. By structure theorem, $G \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots$, where $m_2 | m_1, m_3 | m_2, \ldots$

$$G[m_2] \supset \left({}^{\mathbb{Z}}\big/_{m_1\mathbb{Z}}\right)[m_2] \times {}^{\mathbb{Z}}\big/_{m_2\mathbb{Z}}.$$

Therefore, $\#G[m_2] \geq m_2^2$ so $m_2 = 1$. ■

Thus, the result follows directly from the lemma. ■

Definition 4.3.2. An integer a is called a primitive root mod p if a generates $F_p^\times$

Example. Some examples:

- 2 is a primitive root mod 5
- 3 is a primitive root mod 7
  - But 2 is not!

Remark (Artin's Conjecture)**.** An interesting conjecture: If a is an integer that is not a square and not -1, then a is a primitive root mod p for infinitely many p. At most 2 prime a's do not work i.e. true for at least one of $2, 3, 5$.

Remark (Discrete log problem)**.** Given a primitive root a mod p and some $b \in \mathbb{F}_p^\times$, find i such that $b = a^i$. $(i = \log_a b)$

Lecture 24: Classifying Finite Fields

As previously seen. If F is a finite field then F has characteristic $p > 0$. Therefore, $\mathbb{F}_p \subset F$. If $n = [F : \mathbb{F}_p]$ then $\#F = p^n$. 13 Mar. 02:00

Theorem 4.3.1. Given a prime p and $n \geq 1$, $\exists!$ finite field up to isomorphism with p^n elements.

Remark. If $q = p^n$, we write $\mathbb{F}_q$ for the field with q elements.

Note. $\mathbb{F}_q \neq \mathbb{Z}/q\mathbb{Z}$ unless q is prime.

Proof. We will start with a lemma.

Lemma 4.3.2. If $\#F = q$ then $a^q = a$ for every $a \in F$, so

$$x^q - x = \prod_{a \in \mathbb{F}_q} (x - a).$$

Proof. $F^\times$ is a group of order $q - 1$, so $\forall a \in F^\times$, we have $a^{q-1} = 1$ so $a^q = a$. If $a = 0$ then $a^q = a$ too. Each $a \in F$ is a root of $x^q - x$. Since $\#F = \deg(x^q - x)$ that gives this factorization. ■

Corollary 4.3.1. F is a splitting field of $x^q - x \in \mathbb{F}_p[x]$

Proof. We know that $x^q - x$ factors into linear pieces over F. The roots of $x^q - x \in \mathbb{F}$ generate F because every element of F is a root of this polynomial. ■

Corollary 4.3.2. If F_1 and F_2 are finite fields with q elements then they are isomorphic.

Proof. Splitting fields are unique. ■

Therefore, all that is left to show is that such a finite field exists. Let $q = p^n$ be given. Let F be a splitting field of $x^q - x$.

Claim. $\#F = q$.

Proof. First, we will show that $\#F \leq q$. Consider the mapping

$$\begin{aligned} \phi : F &\longrightarrow F \\ x &\longmapsto x^q. \end{aligned}$$

This is a field isomorphism. Since ϕ is a field isomorphism

$$\{x \in F \mid \phi(x) = x\} \text{ is a subfield of } F.$$

This field must be all of F because it contains the roots of $x^q - x$ and these generate F. Therefore, for every $x \in F$ we have that $\phi(x) = x$ i.e. $x^q - x = 0$. Since this polynomial has $\leq q$ roots, we have that $\#F \leq q$.

Now we must show the reverse inequality. Since $f(x) = x^q - x$ splits into linear factors over F. Therefore, $\#F \geq \#$ distinct roots of f. Note that if a is a multiple root of f then $f'(a) = 0$. However, $f'(x) = qx^{q-1} - 1 = -1$ because $q = 0$ in F. Thus, f has q distinct roots and $\#F \geq q$.

Remark. Let K be any field $f(x) \in K[x]$ such that

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad a_i \in K.$$

Then $f'(x) = \sum_{i=0}^{n} i a_i x^{i-1}$.

■

Thus, F is our desired field. ■

Problem 4.3.1. What is the "best" way to construct $\mathbb{F}_{p^2}$?

Answer. If -1 is not a square in $\mathbb{F}_p$ (p-odd). Then $x^2 + 1$ is an irreducible polynomial over $\mathbb{F}_p$.

Then

$$\mathbb{F}_p[x] \Big/ (x^2+1) \text{ ``='' } \mathbb{F}_p[i]$$

is a field of degree 2 over $\mathbb{F}_p$. If $-1 = a^2$ in $\mathbb{F}_p$ then $x^2+1 = (x-a)(x+a)$. By CRT,

$$\mathbb{F}_p[x] \Big/ (x^2+1) \cong \mathbb{F}_p[a] \times \mathbb{F}_p[a].$$

Remark. -1 is a square in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 4$.

In general ($p \neq 2$), if $a \in \mathbb{F}_p$ is not a square, then $x^2 - a$ is irreducible. Therefore,

$$\mathbb{F}_p[x] \Big/ (x^2-a) \text{ ``='' } \mathbb{F}_p[\sqrt{a}].$$

If $p = 2$, $\mathbb{F}_2[x] / (x^2+x+1)$ is a field with 4 elements. ⊛

Proposition 4.3.2. For $n, m \geq 1$, $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ if and only if $n|m$.

Proof. If $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ then

$$\underbrace{[\mathbb{F}_{p^m} : \mathbb{F}]}_{=m} = [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}] \underbrace{[\mathbb{F}_{p^n} : \mathbb{F}]}_{=n}.$$

Now suppose that $n|m$.

Claim. $x^{p^n} - x$ factors into linear factors over $\mathbb{F}_{p^m}$ (splits).

Proof. Let $m = rn$ for some r. Then $p^n - 1 | p^m - 1$ because

$$\frac{p^m-1}{p^n-1} = \frac{p^r n - 1}{p^n - 1}.$$

This is a geometric series. The same logic applies to see that $x^{p^n-1} - 1 | x^{p^m-1} - 1$. ■

Since $x^{p^m-1} - 1$ splits in $\mathbb{F}_{p^m}$ ($x^{p^m} - x = x(x^{p^m-1} - 1)$), $x^{p^m-1} - 1$ and consequently $x^{p^n} - x$ split. So $\mathbb{F}_{p^m}$ contains a splitting field for $x^{p^n} - x$ ($\cong \mathbb{F}_{p^n}$) ■

4.4 Algebraic Closure

Definition 4.4.1. A field Ω is algebraically closed if every polynomial $f(x) \in \Omega[x]$ has a root in Ω.

Example. $\mathbb{C}$ is algebraically closed (fundamental theorem of algebra).

Proposition 4.4.1. Ω is algebraically closed if and only if any algebraic extension of Ω is trivial (degree 1).

Proof. Suppose that Ω is algebraically closed and K/Ω is an algebraic extension. Pick $a \in K$ and consider its minimal polynomimal $f(x) \in \Omega[x]$. Since $f(x)$ is irreducible and has a root in Ω, it must be degree 1. Therefore, $f(x) = x - a$ and $a \in \Omega$. Thus, $K = \Omega$.

Now suppose that every algebraic extension of Ω is trivial. Let $f(x)$ be a given non constant polynomial. Then we need to show $f(x)$ has a root in Ω. Let K be the splitting field of F. This is an algebraic extension. Therefore, $K = \Omega$. Thus, f already splits over Ω. ■

Definition 4.4.2. Let F be any field. Then an algebraic closure of F is an algebraic field extension Ω/F with Ω algebraically closed.

Example. $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$.

Example (Non-example)**.** $\mathbb{C}$ is not an algebraic closure of $\mathbb{Q}$.

Lecture 25: Twenty-Fifth Lecture

Theorem 4.4.1. Given any F $\exists$ an algebraic closure Ω/F. If Ω'/F is another algebraic closure of F then $\exists F$-isomorphism $\Omega \to \Omega'$. 15 Mar. 02:00

Lemma 4.4.1. Let $\{E_i \,/\, F\}_{i\in I}$ be a family of algebraic extensions. Then there exists an algebraic extension $K \,/\, F$ such that each E_i admits an F-embedding $E_i \to K$.

Proof. Suppose each $E_i \,/\, F$ is finite. Let $x_{i_1}, \ldots, x_{i_{n(i)}}$ be generators for E_i as an extension of F. Consider the map

$$\begin{aligned} F[T_{i_1}, \ldots, T_{i_{n(i)}}] &\longrightarrow E_i \\ T_{i_j} &\longmapsto x_{i_j}. \end{aligned}$$

Let Q_i be the kernel. Now let $R = F[T_{i_j}]_{\substack{i\in I \\ 1\le j\le n(i)}}$ and $Q =$ ideal of R generated by Q_i's. Note

$$E_i = {}^{F[T_{i_1}, \ldots, T_{i_{n(i)}}]}\big/_{Q_i} \longrightarrow {}^{R}\big/_{Q}$$

is injective. Let Q' be a max ideal containg Q. Then we get a map $E_i \longrightarrow R \,/\, Q'$ and $R \,/\, Q'$ is a field.

Remark. $R \,/\, Q \cong \bigotimes_{i\in I} E_i$ (tensor product over F).

To see $R \,/\, Q'$ is an algebraic extension of F, note that the T_{i_j}'s generate and they are the image of the x_{i_j}'s, which are algebraic. Thus, extension generated by algebraic elements is algebraic and $K = R \,/\, Q'$. ■

Example. Consider $E_1 = E_2 = \mathbb{C}$. Then $R = \mathbb{R}[T_1, T_2]$ and $Q = \langle T_1^2 + 1, T_2^2 + 1\rangle$. Thus, Q' becomes either $\langle T_1^2 + 1\rangle$ or $\langle T_2^2 + 1\rangle$.

Construction of Closure. Now we must construct the closure from Theorem. Let $\{f_i\}_{i\in I}$ be the set of all polynomials with coefficients in F. Let $E_i =$ splitting field for f_i. Let F_1 be an algebraic extension of F such that each E_i embeds into F_1 via an F-embedding. Define F_2 by the same procedure starting with F_1 i.e.

$$F \subset F_1 \subset F_2 \subset \cdots.$$

Thus, $\bigcup_{n\ge 1} F_n$ is an algebraic closure of F. ■

Remark. Actually, F_1 is already closed and $F_i = F_1$ for every $i \ge 1$. This is less obvious.

Example. Algebraic closure of $\mathbb{F}_p$. Consider

$$\mathbb{F}_p \subset \mathbb{F}_{p^{2!}} \subset \mathbb{F}_{p^{3!}} \subset \cdots.$$

The union of this chain is an algebraic closure of $\mathbb{F}_p$.

Proposition 4.4.2. Let Ω be an algebraic closure of F and let $E \,/\, F$ be any algebraic extension. Then $\exists$ an F-embedding $E \to \Omega$.

Proof. Consider the simplest case: $E = F(a)$. Let f be the minimal polynomial of a. Then there exists a root a' of f in Ω. By stem fields, $\exists!$ F-embedding $E \to \Omega$ defined by $a \mapsto a'$.

Now consider the case $E = F(a_1, \ldots, a_n)$. We can extend inductively from the previous case.

In the general case, use Zorn's lemma i.e. order them via F-embeddings from one to the other. Then the algebraic closure will be the maximal element. ■

Corollary 4.4.1. If Ω and Ω' are two algebraic closures then they are F-isomorphic.

Proof. By the proposition, $\exists F$-embedding $\Omega' \to \Omega$. Therefore, $\Omega \,/\, \Omega'$ is algebraic extension. Thus, $\Omega = \Omega'$ because Ω' is algebraically closed. ■

4.5 Transcendental Extensions

Definition 4.5.1. If $E \,/\, F$ is an extension, an element a is transcendental over F if it is not algebraic.

Proposition 4.5.1. Suppose $a \in E$ is transcendental over F. Then $\exists F$-isomorphism $F(a) \cong F(x)$, where $F(a) =$ subfield generated by a and $F(x) =$ field of rational functions.

Proof. Consider the ring homomorphsim

$$\begin{aligned} \phi : F[x] &\longrightarrow E \\ f &\longmapsto f(a). \end{aligned}$$

ϕ is injective because if not then a would be algebraic. ϕ induces an injection $\mathrm{Frac}(F[x]) \to E$ whose image is exactly $F(a)$. ■

Problem 4.5.1. Is $F(a, b) \cong F(x, y)$?

Answer. No, could have $a = b$. ⊛

Problem 4.5.2. What if we say $b \not\subset F(a)$?

Answer. Still not neccessarily true. Consider $F = \mathbb{Q}$, $a = \pi^{1/2}$, $b = \pi^{1/3}$. ⊛

Definition 4.5.2. Elements $a_1, \ldots, a_n \in E$ are algebraically independent over F if there is no non trivial algebraic relation i.e. if $\Phi(a_1, \ldots, a_n) = 0$ for some $\Phi \in F[T_1, \ldots T_n]$ then $\Phi = 0$.

Lecture 26: Transcendental Extensions + Exam Review

17 Mar. 02:00

Remark. More generally, a set S of elements of E is algebraically independent if every finite subset is.

Example. $F = \mathbb{C}$, $E = \mathbb{C}(x, y)$. Then x, y are algebraically independent.

Note. If $a_1, \ldots, a_n \in E$ are algebraically independent then

$$F(a_1, \ldots, a_n) \cong F(T_1, \ldots, T_n).$$

Example. There exists an infinite subset of $\mathbb{C}$ that is algebraically independent over $\mathbb{Q}$. We can construct this by induction. Suppose we have $a_1, \ldots, a_n \in \mathbb{C}$ that are algebraically independent over $\mathbb{Q}$. Consider all elements of $\mathbb{C}$ that are algebraic over $\mathbb{Q}(a_1, \ldots, a_n)$. Note that this is a countable subfield of $\mathbb{C}$. Because $\mathbb{C}$ is uncountable, $\exists a_{n+1} \in \mathbb{C}$ that is transcendental over $\mathbb{Q}(a_1, \ldots, a_n)$. Thus, $a_1, \ldots, a_{n+1}$ is algebraically independent.

Definition 4.5.3. A transcendence base for $E \,/\, F$ is a maximal algebraically independent set.

Note (Fact)**.** If S is a transcendence base for $E \,/\, F$ then $E \,/\, F(S)$ is algebraic.

Note (Fact)**.** Any extension has a transcendence base (proof uses Zorn's lemma).

Theorem 4.5.1. Any two transcendence bases of $E \,/\, F$ have the same cardinality.

Definition 4.5.4. The transcendence degree of $E \,/\, F$, denoted tr $\deg(E \,/\, F)$ is the cardinality of any transcendence base.

Example. We have the following examples:

(1) tr $\deg(E \,/\, F) = 0 \Leftrightarrow E \,/\, F$ is algebraic.

(2) tr $\deg \mathbb{C}(T_1, \ldots, T_n) = n$

(3) Given $E \,/\, F$ and $K \,/\, E$ then tr $\deg(K \,/\, F) =$ tr $\deg(K \,/\, E) +$ tr $\deg(E \,/\, F)$

(4) $F = \mathbb{C}$, $E = \mathrm{Frac}\left(\frac{\mathbb{C}[x,y]}{(y^2 - x^3 - x)}\right)$. Then tr $\deg(E \,/\, F) = 1$. A transcendence base is any element of E not in F i.e. x or y or xy.

- Degree is not well defined i.e. $E \,/\, \mathbb{C}(y) = 3$ but $E \,/\, \mathbb{C}(x) = 2$ since $y = \sqrt{x^3 + x}$ is minimal polynomial of y and x is the degree three counterpart.

Example. $F = \mathbb{C}$, $E = \mathrm{Frac}\left(\frac{\mathbb{C}[x,y]}{(y^2 - x^3 - x)}\right)$. Set

$$X = \{(x, y) \in \mathbb{C}^2 \mid y^2 = x^3 + x\}.$$

E is the function field for X. Consider the maps $X \to \mathbb{C}$ defined by $(x, y) \mapsto x$ and $X \to \mathbb{C}$ defined by $(x, y) \to y$. These correspond to the degree 2 and 3 extensions respectively because they are two to one and three to one functions respectively.

4.5.1 Application to algebraic geometry

Suppose we have a ring $R = \mathbb{C}[x_1, \ldots, x_n] \,/\, (f_1, \ldots, f_n)$. Assume R is a domain. Geometrically, $R \leftrightarrow$ Zero locus of $f_1, \ldots, f_n$ in $\mathbb{C}^n$. The zero locus is an "algebraic variety" X.

Definition 4.5.5. $\dim(X) =$ tr $\deg\left(\mathrm{Frac}(R) \,/\, \mathbb{C}\right)$

Write $\mathbb{C}(X) = \mathrm{Frac}(R)$ (function field of X). Say $f : X \to Y$ is a map of varieties. This gives a field extension $\mathbb{C}(Y) \subset \mathbb{C}(X)$

Remark. If f is generally d to 1 then $[\mathbb{C}(X) : \mathbb{C}(Y)] = d$.

4.5.2 Application of tr deg

Theorem 4.5.2. Say $E\,/\,F$ is a finitely generated extension. Then any intermediate field is finitely generated over F.

Corollary 4.5.1. Let $\overline{F} = \{a \in E \mid a \text{ is algebraic over } F\}$. Then $\overline{F}$ is a finite extension of F.

Definition 4.5.6. $E\,/\,F$ is purely transcendental if $E = F(a_1, \ldots, a_n)$ with $a_1, \ldots, a_n$ algebraically independent.

Problem 4.5.3. Is every subextension of a purely transcendental extension purely transcendental? (For F algebraically closed)

Answer. Yes if $n = 1$ (Luroth's thm). Maybe true still for $n = 2$ in characteristic 0. But $n \geq 3$ it is not ture. ⊛

4.6 Exam Review

The exam will consist of mainly two topics: module theory and field theory.

4.6.1 Module Theory

- General definitions: (module, homo, ker, coker)
- Exact sequences.
- Free modules
  - What they are.
  - Bases.
  - Mapping property.
- Presentation of a module, presentation matrix.
- Structure theory for $\mathbb{Z}$-modules, or more generally R-modules, where R is a PID.
  - Polynomial ring over 1 variable. All submodules.
  - Application: $\mathbb{C}[t]$-modules are vector spaces with a linear operator.
- Do not need to know injective or projective modules.
- Do not need localization.
- Hilbert basis theorem.

4.6.2 Field Theory

- Characterisitic of a field $\big\{ F$ has characteristic $0 \Leftrightarrow \mathbb{Q} \subset F$ F has characteristic $p \Leftrightarrow \mathbb{F}_p \subset F$
- Field extension $E\,/\,F$, E is an F-vector space.
  - $[E : F] = \dim_F(E)$
- Transitivity of degree

  - $[K : F] = [K : E][E : F]$
- Algebraic elements / extensions, minimal polynomial.
  - If a is algebraic over F, then $[F(a) : F] =$ degree of minimal polynomial of a
- Stem / splitting fields: existence + uniqueness.
- Finite fields: classification, construction
- Multiplicative group is cyclic.

Chapter 5

Galois Theory

Lecture 27: Galois Theory Introduction

22 Mar. 02:00

Remark. From now on all fields are characteristic 0.

Definition 5.0.1. Let $E\,/\,F$ be a finite field extension. Then the Galois group

$$\mathrm{Gal}({}^{E}\!/_{F}) = \text{group of all } F\text{-automorphisms of } E.$$

As previously seen. An F-automorphism of E is a field automorphism $\sigma : E \to E$ that is constant on F.

Example. For $\mathbb{C}\,/\,\mathbb{R}$,

$$\mathrm{Gal}({}^{\mathbb{C}}\!/_{\mathbb{R}}) = \{1, \underbrace{\tau}_{\text{cmplx conjugation}}\}.$$

If σ is an arbitrary $\mathbb{R}$-automorphism of $\mathbb{C}$, then

$$\sigma(i) = \pm i, \quad \sigma(a+bi) = a + b\sigma(i).$$

Example. $E = F(\sqrt{d})$, $d \neq \square$ in F. $\exists F$-automorphism $\tau : E \to E$ such that $\tau(\sqrt{d}) = -\sqrt{d}$. This follows from stem fields minimal polynomial of $\sqrt{d}$ is $x^2 - d$. Its two roots are $\pm\sqrt{d}$. Then $\mathrm{Gal}(E\,/\,F) = \{1, \tau\}$.

Example. $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. By previous example, $\exists\mathbb{Q}(\sqrt{2})$-automorphism $\sigma : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \mathbb{Q}(\sqrt{2}, \sqrt{3})$ such that $\sigma(\sqrt{3}) = -\sqrt{3}$. This is also a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Therefore, $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$. Also $\exists\tau \in \mathrm{Gal}$ such that $\tau(\sqrt{3}) = \sqrt{3}$ and $\tau(\sqrt{2}) = -\sqrt{2}$. Also have $\sigma \circ \tau$. In fact,

$$\mathrm{Gal}\left({}^{\mathbb{Q}(\sqrt{2},\sqrt{3})}\!/_{\mathbb{Q}}\right) = \{i, \sigma, \tau, \sigma\tau\} \cong {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}.$$

Why is this all? Say $\theta \in \mathrm{Gal}$. We know that $\theta(\sqrt{2})^2 = 2 \Rightarrow \theta(\sqrt{2}) = \pm\sqrt{2}$ and the same for $\sqrt{3}$.

Example. $\mathrm{Gal}(\mathbb{Q}(2^{1/3})/\mathbb{Q})$. If $\theta \in \mathrm{Gal}$ then

$$\theta(2^{1/3})^3 = 2 \Rightarrow \theta(2^{1/3}) = 2^{1/3}.$$

Thus, Gal $= \{1\}$.

Theorem 5.0.1. If $E\,/\,F$ is a finite extension then

$$\#\mathrm{Gal}(E/F) \mid [E:F].$$

Definition 5.0.2. $E\,/\,F$ is a Galois extension if

$$\#\mathrm{Gal}(E/F) = [E:F].$$

Example. The following are examples of Galois extensions:

- A quadratic extension is Galois.
- $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ is Galois.
- $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ is not Galois.

Definition 5.0.3. Given E/F and a subgroup $H \subset \mathrm{Gal}(E/F)$ define

$$E^H := \{a \in E \mid \sigma(a) = a \ \forall \sigma \in H\}.$$

Example. $E/F = \mathbb{C}/\mathbb{R}$, $H = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Then

$$E^H = \{a \in \mathbb{C} \mid \bar{a} = a\} = \mathbb{R}.$$

Remark. E^H is a subfield of E and $F \subset E^H$.

Proposition 5.0.1. Say E/F is Galois and $G = \mathrm{Gal}(E/F)$ then $E^G = F$.

Proof. Since G fixes everything in E^G,

$$G \subset \mathrm{Gal}(E^G/E).$$

Therefore,

$$\#G = [E:F] \leq [E:E^G] = \frac{[E:F]}{[E^G:F]}.$$

Thus, $[E^G:F] = 1$. ∎

Example. We have the following application. If E/F is Galois with group G. Given any $a \in E$ then $\prod_{\sigma\in G}\sigma(a)$ is fixed by G. Therefore, it belongs to F i.e. if $\tau \in G$ then

$$\tau(b) = \prod_{\sigma\in G}\tau(\sigma(a)) = \prod_{\sigma'\in G}\sigma'(a) = b$$

with $\sigma' = \tau\sigma$.

Theorem 5.0.2. If $f(x) \in F[x]$ is any polynomial then the splitting field of f is a Galois extension of F. Conversely, if E/F is Galois then E is the splitting field of some $f(x) \in F[x]$.

Example. Say E is the splitting field of $f(x)$.

Observation 1: $G = \text{Gal}(E/F)$ permutes the roots of F.

If $\sigma \in G$ and $\alpha \in E$ is a root of f then $0 = \sigma(f(a)) = f(\sigma\alpha)$.

Observation 2: The action of G on the roots is faithful.

This is because if we know how $\sigma \in G$ acts on roots we know σ because the roots generate E.

Say $f(x) = (x - \alpha_1)\cdots(x - \alpha_n)$. Then $G \subset S_n =$ Group of permutations of $\{\alpha_1, \ldots, \alpha_n\}$.

Theorem 5.0.3. The action of G on the roots is transitive if and only if f is irreducible.

Proof. If $f(x) = g(x)h(x)$ then G maps roots of g to roots of g and similarly for h. Therefore, G is not transitive. Now suppose that f is irreducible. Say α is a root of f. Say $\alpha_1, \ldots, \alpha_m$ is the G-orbit of α_1. Consider $g(x) = (x - \alpha_1)\cdots(x - \alpha_m)$. We know that $g(x)|f(x)$. G fixes the coefficients of g. Therefore, $g(x) \in F[x]$. Since $g|f$ and f is irreducible, $g = f$ and the action is transitive. ∎

Alternative Proof. $\exists F$-isomorphism τ such that $\tau(\alpha_1) = \alpha_i$ by stem field. Consider the algebraic closure Ω. Then we can embed $E = F(\alpha_1, \ldots, \alpha_n)$ into Ω because E is an algebraic extension over $F(\alpha_1)$. Since E is a stem field, the image of E over our embedding must be E because splitting fields are unique. ∎

Lecture 28: Galois Theory cont.

24 Mar. 02:00

Corollary 5.0.1. Given any finite extension E / F, $\exists$ Galois extension M / F and an F-embedding from $E \to M$.

Proof. $E = F(a_1, \ldots a_n)$. Let f_i be the minimal polynomila of a_i. Consider

$$f(x) = f_1(x)\cdots f_n(x).$$

Let M be the splitting field of f. ∎

Remark. A few remarks:

(1) $\exists$ "minimal" M, this is called the Galois closure of E.

(2) The above corollary is false in positive characteristic.

Corollary 5.0.2. Say we have a Galois extension E / F and an intermediate field K. Then E / K is Galois.

Proof. Since E is Galois over F, E is the splitting field over F of some $f(x) \in F[x]$. E is still the splitting field of $f(x) \in K[x]$. ∎

As previously seen. If E / F is an extension and $H\text{Gal}(E / F)$, the fixed field of H is

$$E^H := \{a \in E \mid \sigma(a) = a \ \forall \sigma \in H\}.$$

This is an intermediate field to E / F.

Theorem 5.0.4 (Main Theorem of Galois Theory). Suppose E / F is a Galois extension.

- There is a bijective correspondence between
$$\{\text{subgroups of } \mathrm{Gal}({}^{E}\!/_{F})\} \longleftrightarrow \{\text{intermediate fields}\}$$
$$H \longmapsto E^H$$
$$\mathrm{Gal}({}^{E}\!/_{K}) \longleftarrow K.$$
- Say $H \longleftrightarrow K = E^H$. Then $[E : K] = \#H$ and $[K : F] = [G : H]$.
- If $H \longleftrightarrow K = E^H$ then H is a normal subgroup of $\mathrm{Gal}(E \,/\, F)$ iff $K \,/\, F$ is a Galois extension
- The correspondence is order-reversing i.e. if H_1 and H_2 are subgroups then $H_1 \subset H_2$ iff $E^{H_1} \supset E^{H_2}$

Remark. An application of the final point: $H_1 \cap H_2$ is the largest subgroup contained in H_1 and H_2. Then $E^{H_1 \cap H_2}$ is smallest field that contains both H_1 and H_2. This fixed field is the compositum of E^{H_1} and E^{H_2}.

Example. $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then $[E : F] = 4$. $\mathrm{Gal}(E \,/\, F) = \{1, \sigma, \tau, \sigma\tau\} \cong \mathbb{Z}\,/\,2 \times \mathbb{Z}\,/\,2$. Where $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = \sqrt{3}$, $\tau(\sqrt{2}) = \sqrt{2}$, and $\tau(\sqrt{3}) = -\sqrt{3}$.

Subgroups	Intermediate fields
1	$\mathbb{Q}(\sqrt{2}, \sqrt{3})$
$\{1, \sigma\}$	$\mathbb{Q}(\sqrt{3})$
$\{1, \tau\}$	$\mathbb{Q}(\sqrt{2})$
$\{1, \sigma\tau\}$	$\mathbb{Q}(\sqrt{6})$
$\{1, \sigma, \tau, \sigma\tau\}$	$\mathbb{Q}$

Example. $F = \mathbb{Q}$, $E =$ splitting field of $x^3 - 2$, $E = \mathbb{Q}(2^{1/3}, \zeta)$ with $\zeta = e^{2\pi i/3}$. Then $[E : F] = 6$ and $\mathrm{Gal}(E \,/\, F) = S_3$. Label the 3 roots as 1, 2, and 3.

Subgroups	Intermediate fields
1	E
$\{1, (12)\}$	$\mathbb{Q}(2^{1/3}\zeta^2)$
$\{1, (13)\}$	$\mathbb{Q}(2^{1/3}\zeta)$
$\{1, (23)\}$	$\mathbb{Q}(2^{1/3})$
$\{1, (123), (132)\}$	$\mathbb{Q}(\zeta)$
S_6	$\mathbb{Q}$

Then the 1st, 5th, and 6th are normal subgroups.

Corollary 5.0.3. If $E \,/\, F$ is a finite extension, then there only exists finitely many intermediate fields.

Proof. Choose $E \subset M$ such that $M \,/\, F$ is Galois. Then the intermediate fields of $M \,/\, F$ are in bijection with subgroups of the Galois group. Since this is a finite group, there are finitely many subgroups. ■

Remark. This is actually false in positive characteristic.

5.1 Cubic Polynomials

Say $f(x) \in F[x]$ is an irreducible cubic polynomial. Let E/F be its splitting field, $G = \mathrm{Gal}(E \,/\, F)$. We know $G \subset S_3$ and it acts transitively. Therefore, it must be the case that $G = A_3$ or S_3.

Problem 5.1.1. How do we tell which one?

Answer. The discriminant. ⊛

Write $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$. $\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$. $D = \delta^2$ (discriminant). For $\sigma \in S_3$, $\sigma\delta = \operatorname{sgn}(\sigma)\delta$. Therefore, $\sigma D = D$. If D is fixed by $\operatorname{Gal}(E / F)$ then $D \in F$.

In fact, can express D as a polynomial in coefficients of f.

Example. If $f(x) = x^3 + px + q$. Then $D = -4p^3 - 27q^2$.

Proposition 5.1.1. $G = A_3$ iff D is a square in F.

Proof. If G is A_3 then G fixes δ. Therefore, $\delta \in F$ and D is a square. Conversely, if D is a square in F, then $\delta \in F$ so G must be A_3. ■

Lecture 29: Main Theorems of Galois Theory

Remark. We will always be in characteristic 0 today. 27 Mar. 02:00

Theorem 5.1.1. Ω / F is an algebraic closure. K / F is a finite extension. Then the number of F-embeddings $K \to \Omega$ is $[K : F]$.

Proof. First suppose (K, a) is a stem field for the irreducible polynomial $f(x) \in F[x]$. Then

$$[K : F] = \deg f(x).$$

By stem field theory, giving an F-embedding $K \to \Omega$ is equivalent to choosing a root of $f(x)$ in Ω. The number of distinct roots is $\deg f(x)$ because Ω is algebraically closed and $f(x)$ has no repeated roots (irreducible polynomials are separable in characteristic 0).

In the general case, let K_0 be an intermediate field to K / F that is a stem field over F. Pick an F-embedding $\sigma : K_0 \to \Omega$. Then Ω is an algebraic closure of K_0 via σ. By induction on degree, the number of K_0-embeddings of K into Ω is $[K : K_0]$.

Problem 5.1.2. What is a K_0-embedding $K \to \Omega$?

Answer. This is a field homomorphism $\tau : K \to \Omega$ such that $\tau|_{K_0} = \sigma$. Therefore, τ is an F-embedding because σ is an F-embedding. ⊛

Rephrasing, each F-embedding $\sigma : K_0 \to \Omega$ admits exactly $[K : K_0]$ extensions to an F-embedding $K \to \Omega$. Therefore, the number of F-embeddings $K \to \Omega$ is the number of F-embeddings $K_0 \to \Omega$ multiplied by the number of ways of extending each of these to K i.e.

$$\#\ F\text{-embeddings } K \to \Omega = [K_0 : F][K : K_0] = [K : F].$$

■

Corollary 5.1.1. $\#\operatorname{Gal}(K / F) \le [K : F]$.

Proof. Fix an F-embedding $\sigma : K \to \Omega$. If $\tau \in \operatorname{Gal}(K / F)$ then $\sigma\tau : K \xrightarrow{\tau} K \xrightarrow{\sigma} \Omega$ is another F-embedding. Therefore, we have an injection

$$\operatorname{Gal}(K / F) \to \{F\text{-embeds } K \to \Omega\}.$$

■

Corollary 5.1.2. Say K / F is the splitting field of $f(x) \in F[x]$. Then K / F is a Galois extension.

Proof. Without loss of generality, assume $K \subset \Omega$. Suppose $\sigma : K \to \Omega$ is an F-embedding.

Claim. $\sigma(K) = K$.

Proof. If $a_1, \ldots, a_n$ are the roots of $f(x)$ in K. Then $\sigma(a_1), \ldots, \sigma(a_n)$ are the roots of $f(x)$ in K. Then

$$K = F(a_1, \ldots, a_n), \quad \sigma(K) = F(\sigma(a_1), \ldots, \sigma(a_n)) = K.$$

■

Therefore, each F-embedding $K \to \Omega$ is an automorphism of K and

$$\#\mathrm{Gal}({}^{K}\big/_{F}) = \#F\text{-embedding } K \to \Omega = [K : F].$$

Thus, K / F is Galois. ■

Remark. From the proof, we have that if K/F is a splitting field and $\sigma, \tau : K \to \Omega$ are two F-embeddings then $\sigma(K) = \tau(K)$. In fact, converse is true: an extension K / F with with property is a splitting field.

Theorem 5.1.2. Let K be a field and let G be a finite group of automorphisms of K. Put $F = K^G$. Then K / F is Galois and $\mathrm{Gal}(K / F) = G$.

Proof. We know $G \subset \mathrm{Gal}(K / F) \Rightarrow [K : F] \geq \#G$. It is enough to prove $[K : F] \leq \#G$. Put $m = \#G$. Then we want to show that $[K : F] \leq m$. We will show that if $n > m$ and $\alpha_1, \ldots, \alpha_n \in K$ then $\alpha_1, \ldots, \alpha_n$ are F-linearly dependent. For notation,

$$G = \{\underbrace{\sigma_1}_{=\mathrm{id}}, \ldots, \sigma_m\}.$$

Consider the following system of equations:

$$\begin{aligned} \sigma_1(x_1)\alpha_1 + \cdots + \sigma_1(x_n)\alpha_n &= 0 \\ &\vdots \\ \sigma_m(x_1)\alpha_1 + \cdots + \sigma_m(x_n)\alpha_n &= 0 \end{aligned} .$$

We know that $\exists$ non-trivial solution in K because $n > m$. To get an F-linear dependence we want a non-trivial solution in F. Consider a non-trivial solution of this system $(c_1, \ldots, c_n) \in K^n$. Choose this to have as many 0's as possible. Without loss of generality, $c_1 = 1$.

Claim. $(c_1, \ldots, c_n) \in F^n$.

Proof. Suppose not. Then $\exists i$ such that $c_i \notin F$. So c_i is not fixed by G i.e. $\exists \sigma \in G$ such that $\sigma c_i \neq c_i$. Note that $(\sigma c_1, \ldots, \sigma c_n)$ is still a solution to the system. Then

$$(c_1, \ldots, c_n) - (\sigma c_1, \ldots, \sigma c_n)$$

is also a solution. Since $\sigma c_1 = \sigma(1) = 1$, we have that

$$(c_1, \ldots, c_n) - (\sigma c_1, \ldots, \sigma c_n) = (0, ?, \ldots, \underbrace{c_i - \sigma c_i}_{\neq 0}, ?, \ldots, ?).$$

Therefore, this is a solution with fewer zeros, contradicting the maximal number of zeroes of our original solution. ■

From the claim, $(c_1, \ldots, c_n) \in F$ and

$$c_1\alpha_1 + \cdots + c_n\alpha_n = 0.$$

Thus, α's are F-linearly dependent. ■

Example. $K = \mathbb{C}(x_1, \ldots, x_n)$. Let S_n act on K by permuting variables. Then

$$F = K^{S_n} \Rightarrow {}^{K}\big/_{F} \text{ is a Galois extension with group } S_n \text{, degree } n!.$$

Write $\prod_{i=1}^n (t - x_i) = \sum_{i=0}^n \underbrace{c_i(x_1, \ldots, x_n)}_{S_n \text{ invariant}} t^i$. Then we have the following fact: $F = \mathbb{C}(c_0, \ldots, c_{n-1})$.

Remark. If G is any finite group then $G \subset S_n$ for some n. If $K = \mathbb{C}(x_1, \ldots, x_n)$, $F = K^G$ then $K \,/\, F$ is a Galois extension with group G.

Lecture 30: Main Theorem of Galois Theory

29 Mar. 02:00

Proposition 5.1.2. If $E \,/\, F$ is a finite extension then the following are equivalent

(a) $E \,/\, F$ is Galois,

(b) $E \,/\, F$ is a splitting field,

(c) If $f(x) \in F[x]$ is irreducible and has one root in E then all roots of f are in E.

Proof. We already proved last time that (b) $\Rightarrow$ (a). First we will show that (a) $\Rightarrow$ (c). Let $f(x) \in F[x]$ be irreducible. Suppose $\exists a \in E$ such that $f(a) = 0$. If $\sigma \in \mathrm{Gal}(E \,/\, F)$ then $\sigma(a)$ is also a root of f. Let $a_1, \ldots, a_n$ be the orbit of a under the $\mathrm{Gal}(E \,/\, F)$. Consider $g(x) = \prod_{i=1}^n (x - a_i)$

Note (Key point)**.** The coefficients of $g(x)$ are symmetric polynomials in $a_1, \ldots, a_n$. Therefore, the coefficients of $g(x)$ are fixed by $\mathrm{Gal}(E \,/\, F)$.

From the key point, we must have that the coefficients are in $E^{\mathrm{Gal}(E \,/\, F)} = F$. Therefore, $g(x) \in F[x]$ and $g(x) | f(x)$. Then it must be the case that $g(x) = f(x)$. Thus, the a_i's are all the roots of $f(x)$ and are in E.

Lastly, we must show that (c) $\Rightarrow$ (b). Since $E \,/\, F$ is finite, $E = F(a_1, \ldots, a_n)$. Let $f_i(x)$ be the minimal polynomial of a_i. By (c), $f_i(x)$ factors into linear pieces over E. Therefore, the same is true for $f(x) = f_1(x) \cdots f_n(x)$. Thus, E is the splitting field of F. ■

Remark. Looking at orbit of root under Galois group is a very important method.

Corollary 5.1.3. If $E \,/\, F$ is Galois and K is an intermediate field then $E \,/\, K$ is Galois.

Proof. We know that E is the splitting field of some $f(x) \in F[x]$. Therefore, it is also the splitting field of $f(x) \in K[x]$. Thus, $E \,/\, K$ is Galois. ■

Example. $K \,/\, F$ is not necessarily Galois. Consider $\mathbb{Q}(2^{1/3}, e^{2\pi i/3})$. Then $\mathbb{Q}(2^{1/3}) \,/\, \mathbb{Q}$ is not Galois.

Proof of main theorem. Let $E \,/\, F$ be a Galois extension and $G = \mathrm{Gal}(E \,/\, F)$. We want a bijective correspondence between subgroups of G and intermediate fields of $E \,/\, F$:

$$\{\text{subgroups of } G\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \{\text{intermediate fields of } {}^{E}\big/_{F}\},$$

where $\Phi(H) = E^H$ and $\Psi(K) = \mathrm{Gal}(E \,/\, K)$. Therefore, we want to show Φ and Ψ are inverses.

Suppose $H \subset G$. We want to show that $\Psi(\underbrace{\Phi(H)}_{\mathrm{Gal}(E \,/\, E^H)}) = H$. This follows from a previous theorem. Now say that K is an intermediate field. Then we want to show that $\Phi(\underbrace{\Psi(K)}_{E^{\mathrm{Gal}(E \,/\, K)}}) = K$. This is true because $E \,/\, K$ is Galois, so the fixed field of $\mathrm{Gal}(E \,/\, K)$ is K.

Another part of the main theorem is that this correspondence is order reversing i.e. if $H_1 \subset H_2 \subset G$ then $\underbrace{\Phi(H_2)}_{E^{H_2}} \subset \underbrace{\Phi(H_1)}_{E^{H_1}}$. This is clear because we are simply requiring that the elements must be fixed by more things. Similarly, if $F \subset K_1 \subset K_2 \subset E$ then $\underbrace{\Psi(K_2)}_{\mathrm{Gal}(E \,/\, K_2)} \subset \underbrace{\Psi(K_1)}_{\mathrm{Gal}(E \,/\, K_1)}$.

Lastly, let $H \subset G$, $K = \Phi(H) = E^H$. Then we want to show that H is a normal subgroup if and only if $K \,/\, F$ is Galois. Suppose that H is normal.

Claim. Every element of G maps $K = E^H$ into itself.

Proof. Say $x \in E^H$ and $\sigma \in G$. Then we want to show that $\sigma x \in E^H$. Let $\tau \in H$. Then

$$\tau\sigma x = \sigma \underbrace{\sigma^{-1}\tau\sigma}_{\in H} x = \sigma x.$$

This is because $x \in E^H$. Thus, $\sigma x \in K = E^H$. ∎

Now show that $K \,/\, F$ is Galois. Say $f(x) \in F[x]$ is irreducible and it has a root $a \in K$. We know if $a_1, \ldots, a_n$ is the G-orbit of a that these are all the roots of f. Since $a \in K$ and G maps K to itself each $a_i \in K \Rightarrow f(x)$ splits over K. So $K \,/\, F$ is Galois.

Suppose $K \,/\, F$ is Galois. Then we want to show that $H = \mathrm{Gal}(E \,/\, K)$ is normal.

Claim. It is once again true that K is mapped to itself by elements of G

Proof. Since $K \,/\, F$ is Galois, K is the splitting field of some $f(x)$. Note that K is the unique splitting field of $f(x)$ contained in E. If $\sigma \in G$ then σK is still a splitting field of f in E. Thus, $\sigma K = K$ ∎

Note that we have the map

$$\begin{aligned} \mathrm{Gal}({}^{E}\!/_{F}) &\longrightarrow \mathrm{Gal}({}^{K}\!/_{F}) \\ \sigma &\longmapsto \sigma|_K. \end{aligned}$$

The kernel of this is $\mathrm{Gal}(E \,/\, K) = H$. Thus, H is normal.

Note. This mapping is actually surjective

$$1 \longrightarrow \mathrm{Gal}({}^{E}\!/_{K}) \longrightarrow \mathrm{Gal}({}^{E}\!/_{F}) \longrightarrow \mathrm{Gal}({}^{K}\!/_{F}) \longrightarrow 1.$$

This is an exact sequence of groups.

∎

Lecture 31: Galois Theory of Finite Fields

Say $q = p^r$ and consider $\mathbb{F}_q \,/\, \mathbb{F}_p$ - this is a Galois extension. Define 29 Mar. 02:00

$$\begin{aligned} \phi : \mathbb{F}_q &\longrightarrow \mathbb{F}_q \\ x &\longmapsto \phi(x) = x^p. \end{aligned}$$

This is a field automorphism and $\phi \in \mathrm{Gal}(\mathbb{F}_q \,/\, \mathbb{F}_p)$. We know that $x^q = x$ holds for every $x \in \mathbb{F}_q$. Therefore, $\phi^r = 1$ in $\mathrm{Gal}(\mathbb{F}_q \,/\, \mathbb{F}_p)$. This gives us that the order of the Galois group divides r.

Note. $\phi^k = \phi \circ \cdots \circ \phi$ such that $\phi^k(x) = x^{p^k}$.

We cannot have that $\phi^k = 1$ for $k < r$ because this would say that $x^{p^k} = x$ for every $x \in \mathbb{F}_q$ but this polynomial only has $p^k < q$ roots. This gives us that ϕ has order r. On the other hand, $[\mathbb{F}_q : \mathbb{F}_r] \leq r$ such that $\#\mathrm{Gal}(\mathbb{F}_q \,/\, \mathbb{F}_p)$. Thus, $\mathrm{Gal}(\mathbb{F}_q \,/\, \mathbb{F}_p) = \langle \phi \rangle$.

Subgroups of $\langle \phi \rangle$ correspond to divisors of r. (If $d | r$ then the subgroups is $\langle \phi^d \rangle$. Main theorem of Galois theory implies subfields of $\mathbb{F}_q$ correspond to divisors of r. Explicitly, $d \longleftrightarrow$ fixed field of $\phi^d \cong \mathbb{F}_{p^d}$.

Note. If $\langle \phi \rangle$ is abelian then all subgroups are normal. Therefore, all extensions of finite fields are Galois.

Let F be a field of characteristic 0, $\zeta = p$th root of 1

Claim. $F(\zeta)$ is a Galois extension of F.

Proof. $F(\zeta)$ is the splitting field of $x^p - 1$.

$$x^p - 1 = \prod_{a \in \mathbb{F}_p} (x - \zeta^a), \quad \zeta^a \in F(\zeta).$$

■

Define $\chi : \mathrm{Gal}(F(\zeta) \,/\, F \to \mathbb{F}_p^\times$ as follows. Say $\sigma \in \mathrm{Gal}(F(\zeta) \,/\, F)$, where σ is a prime pth root of 1. Then $\sigma(\zeta) = \zeta^a$ for $a \in \mathbb{F}_p^\times$. Define $\chi(\sigma) = a$. An observation is that this is actually independent of choic of ζ. To see this, say ω is a second prime pth root of 1. Then $\omega = \zeta^b$ for some $b \in \mathbb{F}_p^\times$. Therefore,

$$\sigma(\omega) = \sigma(\zeta)^b = (\zeta^a)^b = (\zeta^b)^a = \omega^a.$$

This gives us that χ is actually well defined. Now we observe that χ is a group homomorphism. To see this, say $\sigma, \tau \in \mathrm{Gal}(F(\zeta) \,/\, F)$. Then

$$\zeta^{\chi(\sigma\tau)} = \sigma\tau(\zeta) = \sigma(\zeta^{\chi(\tau)}) = \sigma(\zeta)^{\chi(\tau)} = \left(\zeta^{\chi(\sigma)}\right)^{\chi(\tau)} = \zeta^{\chi(\sigma)\chi(\tau)}.$$

Thus, $\chi(\sigma\tau) = \chi(\sigma) \cdot \chi(\tau)$.

Lastly, we see that χ is injective. To see this, say $\sigma, \tau \in \mathrm{Gal}(F(\zeta) \,/\, F)$. If $\chi(\sigma) = \chi(\tau)$ then $\sigma(\zeta) = \tau(\zeta)$. Thus, $\zeta = \tau$ because ζ generates the extension.

Proposition 5.1.3. For any F of characteristic 0, $\exists$ canonical injective group homomorphism:

$$\chi : \mathrm{Gal}({}^{F(\zeta)}\!\big/\!{}_{F}) \longrightarrow \mathbb{F}_p^\times.$$

In particular, $\mathrm{Gal}(F(\zeta) \,/\, F)$ is cyclic of order dividing $p - 1$.

Remark. χ is not bijective in general i.e. F could already contain ζ, in which case $F(\zeta) = F$.

Proposition 5.1.4. If $F = \mathbb{Q}$ then χ is a bijection.

Proof. ζ is a root of $\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1$, which is irreducible over $\mathbb{Q}$. Therefore, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$. Thus, $\#\mathrm{Gal}(\mathbb{Q}(\zeta) \,/\, \mathbb{Q}) = p - 1$. ■

Problem 5.1.3. Now we have that $\mathrm{Gal}(\mathbb{Q}(\zeta) \,/\, \mathbb{Q}) \cong \mathbb{F}_p^\times$. What is the subfield E of $\mathbb{Q}(\zeta)$ correspond to the subgroup $\langle -1 \rangle \subset \mathbb{F}_p^\times$?

Answer. Let $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta) / \mathbb{Q})$ be complex conjugation. Then $\tau \neq 1$ but $\tau^1 = 1$. So τ is the unique element of order 2, such that $\chi(\tau) = -1$. Therefore, E is the fixed field under complex conjugation. Namely, $E = \mathbb{Q}(\underbrace{\zeta + \overline{\zeta}}_{2\cos(2\pi/p)})$. To see inclusion, we have that $\zeta + \overline{\zeta}$ is fixed by τ. Then we have that

$$(x - \zeta)(x - \overline{\zeta}) = x^2 - (\zeta + \overline{\zeta})x + 1 \in \mathbb{Q}(\zeta + \overline{\zeta}).$$

Therefore, $\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \overline{\zeta}) \leq 2$. Since these fields are not equal, this extension is exactly 2. Thus, we have equality. ⊛

Problem 5.1.4. $(\mathbb{F}_p^\times)^2 \subset \mathbb{F}_p^\times$ has index 2. Let F be the fixed field of $(\mathbb{F}_p^\times)^2$. Then what is F?

Answer. Consider $g' = \sum_{a \in \mathbb{F}_p^\times} \zeta^{a^2}$. This is the "average" of ζ over $(\mathbb{F}_p^\times)$. Automatic that $g' \in F$. Consider

$$g = 1 + g' = \sum_{a \in \mathbb{F}_p} \zeta^{a^2}.$$

This is analagous to $I = \int_{-\infty}^{\infty} e^{-x^2} \mathrm{d}x$. Then

$$\begin{aligned} I^2 &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} e^{-(x^2+y^2)} \mathrm{d}x\mathrm{d}y \\ &= \int_0^{\infty} \int_0^{2\pi} e^{-r^2} r \mathrm{d}\theta \mathrm{d}r \\ &= \pi. \end{aligned}$$

Thus, $I = \sqrt{\pi}$. Now we will see the analagous p case, where $p = 1 \bmod 4$. Then

$$g^2 = \sum_{a,b \in \mathbb{F}_p} \zeta^{a^2+b^2}.$$

Since $p = 1 \bmod 4$, we have that $\exists i \in \mathbb{F}_p$ such that $i^2 = -1$. Then

$$a^2 + b^2 = a^2 - (ib)^2 = \underbrace{(a + ib)}_{u} \underbrace{(a - ib)}_{v}.$$

This gives us that

$$g^2 = \sum_{u,v \in \mathbb{F}_p} \zeta^{uv} = \sum_{u \neq 0} \underbrace{\sum_{v \in \mathbb{F}_p} \zeta^{uv}}_{=0}.$$

Therefore, $g^2 = p$ and $g = \sqrt{p}$. ⊛

Lecture 32: Adjoining Roots + Galois Closure

5.2 Adjoining roots

3 Apr. 02:00

We know that $\mathbb{Q}(2^{1/3})$ is not a Galois extension of $\mathbb{Q}$. Say F is a field of characteristic 0 and F contains all pth roots of 1.

Proposition 5.2.1. For any $a \in F$ ($a \neq p$th power). $F(a^{1/p})$ is a Galois extension of F with Galois group $\cong \mathbb{Z} / p\mathbb{Z}$.

Proof. $a^{\frac{1}{p}}$ is a root of $f(t) = t^p - a = \prod_{i=1}^{p}(t - \zeta^i a^{\frac{1}{p}})$. By assumpotino $\zeta^i \in F$ for every i. Therefore, all roots of $f(t)$ belong to $F(a^{1/p})$. Thus, $F(a^{1/p})$ is the splitting field of F. Let $\mu_p = \{\omega \in F \mid \omega^p = 1\} \cong \mathbb{Z}/p\mathbb{Z}$. We have a function $\phi : \mathrm{Gal}(F(a^{1/p})/F) \to \mu_p$ defined by $\phi(\sigma) = \sigma(a^{1/p})/a^{1/p}$.

Note. $\sigma(a^{1/p})$ this is another p th root of a. Therefore, it is of the form $\zeta^i a^{1/p}$, $\phi(\sigma) = \zeta^i$.

Now we must show that ϕ is a group homomorphism.

$$\begin{aligned}\sigma\tau(a^{1/p}) &= \phi(\sigma\tau) \cdot a^{1/p} \\ &= \sigma(\phi(\tau)a^{1/p}) && = \sigma(\phi(\tau))\sigma(a^{1/p}).\end{aligned}$$

Since $\phi(\tau) \in F$ by assumption, it is fixed by σ. Therefore,

$$\sigma(\phi(\tau))\sigma(a^{1/p}) = \phi(\tau) \cdot \phi(\sigma) \cdot a^{1/p}.$$

We know that ϕ is injective because any σ is determined by $\sigma(a^{1/p})$. We also know that ϕ is surjective because $\mathrm{im}\phi$ is a subgroup of $\mathbb{Z}/p\mathbb{Z}$. Since a is not a pth power, $F(a^{1/p})$ is not a trivial extension. Therefore, $\mathrm{im}\phi$ is not trival and must be $\mu_p \cong \mathbb{Z}/p\mathbb{Z}$. ■

Proposition 5.2.2. Suppose that $\mu_p \subset F$. Let E/F be a Galois extension with Galois group $\mathbb{Z}/p\mathbb{Z}$. Then $E \cong F(a^{1/p})$ for some $a \in F$.

Proof. Let σ generate $\mathrm{Gal}(E/F)$. Consider σ as an F-linear operator on $E \to E$. We know that $\sigma^p = 1$. Therefore, eigenvalues of σ are pth roots of 1 (They are all in F). Therefore, we can diagonalize σ over F because σ has finite order. We know that $\sigma \neq 1$. Therefore, $\exists$ eigenvalue $\omega \in \mu_p$ of σ such that $\omega \neq 1$. Say $b \in E$ is an eigenvector $\sigma(b) = \omega b$. Therefore,

$$\sigma(b^p) = \sigma(b)^p = \omega^p b^p = b^p.$$

This gives us that $b^p \in F$ because b^p is fixed by σ and σ generates $\mathrm{Gal}(E/F)$. However, $b \notin F$ because $\sigma(b) \neq b$. Thus, $E = F(b)$ because $[E : F] = p$ such that there are no proper intermediate fields. ■

Remark. More generally, say n is a positive integer and $\mu_n \subset F$. Then $F(a^{1/n})$ is a Galois extension of F and $\mathrm{Gal}(F(a^{1/n})/F) \subset \mu_n$. The converse is also true.

5.3 Galois Closure

Proposition 5.3.1. Let E/F be a finite extension. $\exists$ a Galois extension M/F and an F-embedding $E \to M$ such that if M'/F is a Galois extension with an F-embedding $E \to M'$ then $\exists M \to M'$. Moreover, M is unique up to F-isomorphism.

Definition 5.3.1. Such an M is called the Galois closure of E/F.

Proof. Let Ω/F be an algebraic closure. Choose an F-embedding $E \to \Omega$, such that $E = F(a_1, \ldots, a_n)$. Let $f_i(x)$ be the minimal polynomial of a_i. Let $M \subset \Omega$ be generated over F by all the roots of the f_i's. M is a splitting field for $f(x) = f_1(x)\cdots f_n(x)$. Therefore, M/F is Galois.

Now we must show that M is minimal. Let M' be given. Choose an E-embedding $M' \to \Omega$. Since M'/F is Galois and $f_i(x)$ has one root in M', M' must have all the roots of f. Thus, $M \subset M'$. ■

Example. Suppose we have Galois extensions $F(\sqrt{d})/F$ with Galois group $\mathbb{Z}/2\mathbb{Z}$ and $F(\sqrt{a+b\sqrt{d}})/F(\sqrt{d})$

with Galois group $\mathbb{Z}/2\mathbb{Z}$. If $E = F(\sqrt{a+b\sqrt{d}})$ then E/F is not necessarily Galois.

Suppose that E/F is Galois. Let $\sigma \in \mathrm{Gal}(E/F)$ be an element such that $\sigma(\sqrt{d}) = -\sqrt{d}$. Put $x = \sqrt{a+b\sqrt{d}}$. Consider $x^2 = a + b\sqrt{d}$. Then

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

Therefore, if E/F is Galois then $a - b\sqrt{d}$ is a square in E. (In fact, converse is true).

If E/F is not Galois its closure is $M = F(\sqrt{a+b\sqrt{d}}, \sqrt{a-b\sqrt{d}})$. Then $\mathrm{Gal}(M/F(\sqrt{d})) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.

Remark. If E/F is Galois then $\mathrm{Gal}(E/F) = \mathbb{Z}/4$. $F(\sqrt{d})$ sits inside a $\mathbb{Z}/4$ extension if and only if d is the sum of two squares in the base field.

Lecture 33: TBD

5 Apr. 02:00

Definition 5.3.2. Let G be a finite group. A composition series for G is a chain of subgroups

$$1 = H_0 \subset H_1 \subset \cdots \subset H_n = G,$$

such that H_i is normal in H_{i+1} and maximal among normal subgroups.

Remark. These exist because G is finite. For H_{i-1}, just take maximal proper subgroup of H_i.

Remark. Composition series are not unique i.e.

$$1 \subset \mathbb{Z}/2 \subset \mathbb{Z}/6$$

and

$$1 \subset \mathbb{Z}/3 \subset \mathbb{Z}/6.$$

Remark. In a composition series H_i/H_{i-1} is a simple group (no normal subgroups except trival and whole group).

Theorem 5.3.1 (Jordan-Holder Theorem)**.** Let $1 = H_0 \subset \cdots \subset H_n = G$ and $1 = H'_0 \subset \cdots \subset H'_m$ be two composition series. Then $n = m$ and $\exists \sigma \in S_n$ such that

$$H_i / H_{i-1} \cong H'_{\sigma(i)} / H'_{\sigma(i)-1}.$$

Definition 5.3.3. The groups H_i/H_{i-1} are the J-H constituents of G and n is the J-H length of G.

Example. We have the following examples:

1. If G is a simple group then its J-H constituents are only G and J-H length 1.
2. If $G = S_5$ then the J-H constituents are A_5 and $\mathbb{Z}/2$ and it is of J-H length 2.
3. $G = S_3$ is J-H length 2 with constituents A_3 and $\mathbb{Z}/2$.
4. $G = S_4$, we have the $V = \{1, (12)(34), (14)(23)\}$ which is a normal subgroup of A_4. Therefore,

a composition series is

$$1 \subset \mathbb{Z}/_{2} \subset V \subset A_4 \subset S_4.$$

This gives us constitutients $\mathbb{Z}/2$, $\mathbb{Z}/2$, $\mathbb{Z}/3$, and $\mathbb{Z}/2$ with length 4.

Definition 5.3.4. G is solvable if its J-H constituents are all $\mathbb{Z}/p\mathbb{Z}$'s for varying primes p.

Example. S_2, S_3, S_4 are solvable but S_5 is not solvable.

Proposition 5.3.2 (Permance props of solvability)**.** We have the following:

(a) A sub or quotient of a solvable group is solvable.

(b) An extension of solvable groups is solvable i.e. if G has a normal subgroup N such that N and G/N are solvable then G is solvable.

(c) A product of solvable groups is solvable.

Proof of (a). Suppose that G is solvable and G surjects onto G'. Let $1 = H_0 \subset \cdots \subset H_n = G$. Then we can define $H_i' = \text{img of } H_i$ in G'. This is a chain of subgroups. However, the chain is not necessarily strict, so we must delete duplicates. We have that

$$H_i/_{H_{i-1}} \longrightarrow \underbrace{H_i'/_{H_{i-1}'}}_{\mathbb{Z}/p\mathbb{Z} \text{ or trivial}}.$$

■

Proof of (b). Suppose N and G/N are solvable. Consider $1 = H_0 \subset \cdots \subset H_r = N$ and $1 = \overline{H}_r \subset \cdots \subset \overline{H}_s \subset G/N$. Let $H_i = $ inverse image of $\overline{H}_i$ in G. Then this is a composition series in G. ■

Proof of (c). Follows from (b). ■

Definition 5.3.5. Let F be a field, $\Omega =$ algebraic closure of F, and $a \in \Omega$. Then a can be expressed with radicals if there exists a tower of field $F \subset F_1 \subset F_2 \cdots \subset F_r \subset \Omega$ such that $F_1 = F(\text{roots of } 1)$, $F_i = F_{i-1}(n\text{th root of something in } F_{i-1})$, where n can vary such that $a \in F_r$.

Definition 5.3.6. A polynomial $f \in F[x]$ is solvable by radicals if its roots can be expressed by radicals.

Theorem 5.3.2. Let $f \in F[x]$ be a polynomial with Galois group G i.e. $G =$ Galois group of splitting field of f. Then the following are equivalent:

(a) f is solvable by radicals.

(b) G is a solvable group.

Proof of (b) $\Rightarrow$ (a). Let E/F be the splitting field of f. Then this is a Galois extension with group G, where G is a solvable group. Let $F' = F(\text{all } n\text{th roots of } 1 \text{ with } n|\#G$. Let $F' \cdot E$ be the compositum i.e. subfield of Ω generated by F' and E. Then $F' \cdot E$ is a Galois extension of F (also of F'). We have a group homomorphsim

$$\begin{aligned} \mathrm{Gal}(F' \cdot E/_{F}) &\longrightarrow \mathrm{Gal}(F'/_{F}) \times \mathrm{Gal}(E/_{F}) \\ \sigma &\longmapsto (\sigma|_{F'}, \sigma|_{E}). \end{aligned}$$

This is injective because F' and E generate $F' \cdot E$. Then

$$\mathrm{Gal}(F' \cdot E \,/\, F') = \ker(\mathrm{Gal}(E \cdot F' \,/\, F) \longrightarrow \mathrm{Gal}(F' \,/\, F)$$

Therefore, $\mathrm{Gal}(F' \cdot E \,/\, F')$ is isomorphic to a subgroup of $\mathrm{Gal}(E \,/\, F)$. Then $\mathrm{Gal}(F' \cdot E \,/\, F')$ is a subgroup of a solvable group and therefore solvable.

> **Note.** $F' \cdot E =$ splitting field of $f(x)$ over F'

We may as well relable now and assume that our F contains all the nth roots of unity with $n | \#G$. Since G is solvable, there exists a normal subgroup N such that $G \,/\, N$ is of the form $\mathbb{Z} \,/\, p\mathbb{Z}$. Then we have the tower

$$F \longrightarrow E^N \longrightarrow E$$

with $\mathrm{Gal}(E^N \,/\, F) = \mathbb{Z} \,/\, p$, $\mathrm{Gal}(E \,/\, E^n) = N$ and $\mathrm{Gal}(E \,/\, F) = G$. By last time, $E^N = F(a^{1/p})$ for some $a \in F$. By induction, everything in E is expressed with radicals over E^N. Since $E^N = F(a^{1/p})$, same is true for $E \,/\, F$. ■

Lecture 34: TBD

7 Apr. 02:00

Proof of (a) $\Rightarrow$ (b). We know that there exists some tower $F \subset K_1 \subset K_2 \subset \cdots \subset K_n$ such that $K_1 = F(\text{roots of } 1)$, $K_n = K_{n-1}(\text{a root from } K_{n-1})$, where $E \subset K_n$.

> **Note.** The idea is that we want to enlarge K_n to get some $K_n \subset L_n$ such that L_n/F is Galois. Then we have a surjection $\mathrm{Gal}(L_n/F) \to G$. Since $\mathrm{Gal}(L_n/F)$ is solvable, this will give us that G is solvable.

Let $L_1 = F(\text{roots of } 1)$. Namely, use all appearing in K_1 and d th roots of 1 for every d of the form $[K_i : K_{i-1}]$. Then $K_1 \subset L_1$. Recall $K_2 = K_1(a^{1/d})$ for $a \in K_1$. Then define L_2 to be the Galois closure of $L_1(a^{1/d})$ over F. Then we have that $K_2 \subset L_2$ and L_2/F is Galois. Since K_1/F is Galois, $L_2 = L_1((\sigma a)^{1/d})$ as σ varies in $\mathrm{Gal}(K/F)$.

> **Remark.** Say F is a field containing all d th roots of 1. Then if $E = F(a_1^{1/d}, \ldots, a_n^{1/d})$ then E/F is Galois and
>
> $$\mathrm{Gal}(E/F) \subset \left(\mathbb{Z}/d\mathbb{Z}\right)^n.$$

Therefore,

$$\mathrm{Gal}(L_2/L_1) \subset \prod_{\sigma \in \mathrm{Gal}(K/F)} \mathbb{Z}/d\mathbb{Z}.$$

Then we have a short exact sequence

$$1 \longrightarrow \underbrace{\mathrm{Gal}(L_2/L_1)}_{\text{abelian}} \longrightarrow \mathrm{Gal}(L_2/F) \longrightarrow \underbrace{\mathrm{Gal}(L_1/F)}_{\text{abelian}} \longrightarrow 1.$$

Therefore, $\mathrm{Gal}(L_2/F)$ is solvable. Now keep going. $K_3 = K_2(b^{1/e})$. Then define L_3 to be the Galois closure of $L_2(b^{1/e})$ over F. Then

$$L_3 = L_2((\sigma b)^{1/e}), \qquad \text{for } \sigma \in \mathrm{Gal}(L_2/F).$$

Then once again we have that

$$1 \longrightarrow \underbrace{\mathrm{Gal}(L_3/L_2)}_{\text{abelian}} \longrightarrow \mathrm{Gal}(L_3/F) \longrightarrow \underbrace{\mathrm{Gal}(L_2/F)}_{\text{solvable}} \longrightarrow 1.$$

In the end, we get that L_n/F such that

(1) $E \subset K_n \subset L_n$,

(2) L_n/F is Galois,

(3) $\mathrm{Gal}(L_n/F)$ is solvable.

Therefore, $\mathrm{Gal}(L_n/F) \to \mathrm{Gal}(E/F) = G$. Thus, G is solvable. ■

Theorem 5.3.3 (Abel-Rufini Theorem)**.** There does not exist a quintic formula.

Proof. Let $E = \mathbb{C}(\alpha_1, \dots, \alpha_5)$ be a rational function field. Then S_5 acts on E by permuting the roots. Define $F = E^{S_5} = \mathbb{C}(a_0, \dots, a_4)$, where

$$f(t) = \prod_{i=1}^{5}(t - \alpha_i) = t^5 + a_4t^4 + \cdots + a_0.$$

Then $\mathrm{Gal}(E/F) = S_5$, which is not solvable. Therefore, f is not solvable by radicals i.e. cannot express α_i in terms of coefficients just using radicals. ■

Example. There exists fields F such that every irreducible quintic over F is solvable by radicals.

- $F = \mathbb{C}, \mathbb{R}$ (no irreducible quintics).
- $F = \mathbb{F}_q$ every extension is Galois with abelian Galois group.
- Every Galois extension of $\mathbb{Q}_p$ has solvable Galois group.

Example. Over $\mathbb{Q}$ there exists irreducible quintics not solvable by radicals

Lemma 5.3.1. Let $f \in \mathbb{Q}[x]$ be an irreducible quintic with Galois group G. Suppose f has exactly 3 real roots. Then $G = S_5$.

Proof. We know that $G \subset S_5$ and is transitive. By Orbit-stabilizer, we have that $5|G$, so G must contain a 5-cycle. Let E be the splitting field in $\mathbb{C}$. Then complex conjugation restricts to an element $\tau \in \mathrm{Gal}(E/\mathbb{Q})$, such that τ fixes the three real roots, and switches the other 2. Therefore, τ is a transposition. A transposition and a 5-cycle generate S_5. Thus, $G = S_5$. ■

Example. Consider $f(x) = x^5 - 16x + 2$. This is an irreducible polynomial with 3 real roots. Therefore, f is not solvable by radicals.

Corollary 5.3.1. There exists a cubic formula and a quartic formula.

Cubic case. Consider $E = \mathbb{C}(\alpha_1, \alpha_2, \alpha_3)$ and $F = E^{S_3} = \mathbb{C}(a_0, a_1, a_2)$, where

$$f(t) = \prod_{i=1}^{3} t^3 + a_2t^2 + a_1t + a_0.$$

Then $\mathrm{Gal}(E/F) = S_3$ is a solvable group. Therefore, there is an expression for α_1 in terms of a_0, a_1, a_2 using radicals. ■

Example. We have an SES

$$1 \longrightarrow A_3 \longrightarrow S_3 \longrightarrow {}^{\mathbb{Z}}\big/_{2} \longrightarrow 1.$$

Then this gives us a tower of fields $F \subset K \subset E$, where $K = F(\delta) = F^{A_3}$.

Lecture 35: Infinite Galois Theory

5.4 Infinite Galois Theory

10 Apr. 02:00

Problem 5.4.1. Find intermediate fields between $\mathbb{F}_p$ and $\overline{\mathbb{F}}_p$.

Answer. If we consider the chain

$$\mathbb{F}_p \subset \mathbb{F}_{p^2} \subset \mathbb{F}_{p^4} \subset \mathbb{F}_{p^8} \subset \cdots .$$

The union of this chain will be an intermediate field between $\mathbb{F}_p$ and $\overline{\mathbb{F}}_p$. Not all of $\overline{\mathbb{F}}_p$ because it does not contain $\mathbb{F}_{p^3}$. Similarly, we can do

$$\bigcup_{n=1}^{\infty} \mathbb{F}_{p^{3\cdot 2^n}} .$$

If we let $q_1, q_2, \ldots$ be primes such that $q_i \equiv 1 \bmod 4$ then

$$\bigcup_{n=1}^{\infty} \mathbb{F}_{p^{q_1 \cdots q_n}} .$$

⊛

Answer. Consider a formal product

$$n = \prod_{\text{all primes } q} q^{e(q)},$$

where $e(q) \in \mathbb{N} \cup \{\infty\}$. Given $m \in \mathbb{N}$ we say $m|n$ if the power of q in m is $\leq e(q)$ for every prime q. Then

$$\mathbb{F}_{p^n} = \bigcup_{m|n} \mathbb{F}_{p^m} .$$

⊛

Problem 5.4.2. What is $\mathrm{Gal}(\overline{\mathbb{F}}_p \,/\, \mathbb{F}_q)$?

Answer. We have the tower $\mathbb{F}_q \subset \mathbb{F}_{p^n} \subset \overline{\mathbb{F}}_p$. Therefore, we have the restriction map

$$\begin{aligned} \phi : \mathrm{Gal}\left({}^{\overline{\mathbb{F}}_p}\big/_{\mathbb{F}_q}\right) &\longrightarrow \mathrm{Gal}({}^{\mathbb{F}_{p^n}}\big/_{\mathbb{F}_p}) \cong {}^{\mathbb{Z}}\big/_{n} \\ \sigma &\longmapsto \phi(\sigma) = \sigma|_{\mathbb{F}_{p^n}} . \end{aligned}$$

This is a surjective group homomorphism. Fix a prime q. Then we have the tower

$$\mathbb{F}_p \subset \mathbb{F}_{p^q} \subset \mathbb{F}_{p^{q^2}} \subset \cdots ,$$

which gives us a chain of restriction maps, such that we somehow end up with a group homomorphism from

$$\operatorname{Gal}\left({}^{\overline{\mathbb{F}}_p}\Big/_{\mathbb{F}_p}\right) \to \varprojlim \operatorname{Gal}\left({}^{\mathbb{F}_{p^{q^n}}}\Big/_{\mathbb{F}_p}\right) \cong \mathbb{Z}_q.$$

Similarly,

$$\operatorname{Gal}\left({}^{\overline{\mathbb{F}}_p}\Big/_{\mathbb{F}_p}\right) \to \varprojlim \operatorname{Gal}\left({}^{\mathbb{F}_{p^n}}\Big/_{\mathbb{F}_p}\right) \cong \varprojlim {}^{\mathbb{Z}}\Big/_{n\mathbb{Z}} = \hat{\mathbb{Z}}.$$

For $n = \prod_p p^{\mathrm{val}_p(n)}$, we have that

$$\begin{aligned}\hat{\mathbb{Z}} &= \varprojlim {}^{\mathbb{Z}}\Big/_{n\mathbb{Z}} \\ &= \varprojlim \prod_p {}^{\mathbb{Z}}\Big/_{p^{\mathrm{val}_p(n)}\mathbb{Z}} \\ &\cong \prod_p \mathbb{Z}_p.\end{aligned}$$

⊛

Remark. $\mathbb{Z}_q$ has a topology. Closed subgroups are just $0 =$ "$q^\infty \mathbb{Z}_q$" and $q^n\mathbb{Z}_q$ for $n \in \mathbb{N}$.

We have now observed a bijection

$$\left\{\text{Closed subgroups of Gal}\left({}^{\overline{\mathbb{F}}_p}\Big/_{\mathbb{F}_p}\right)\right\} \longleftrightarrow \left\{\text{intermediate fields to } {}^{\overline{\mathbb{F}}_p}\Big/_{\mathbb{F}_p}\right\}.$$

Definition 5.4.1. Suppose K characteristic 0. Then the absolute Galois group of K is $\operatorname{Gal}(\overline{K}/K)$. This is often denoted G_K.

Suppose K is countable. Let $\{g_n\}_{n\geq 1}$ be a sequence in G_K and let $h \in G_K$. We say $\{g_n\}$ converges to h if $\overline{K} = \bigcup_{n\geq 1} L_n$ for $L_n \,/\, K$ finite Galois with

$$L_1 \subset L_2 \subset \cdots$$

such that $g_n|_{L_n} = h|_{L_n}$.

For each finite Galois extension $L \,/\, K$ $(L \subset \overline{K})$, we have a surjection

$$G_K \xrightarrow{\pi_K} \operatorname{Gal}\left({}^{L}\Big/_{K}\right).$$

Then $\ker(\pi_K)$ is an open subgroup of G_K (Krull topology). Groups with tons of open subgroups are profinite i.e.

$$G_K \cong \varprojlim_L \operatorname{Gal}\left({}^{L}\Big/_{K}\right).$$

Theorem 5.4.1. This gives us the previous observation.

$$\{\text{Closed subgroups of } G_K\} \longleftrightarrow \left\{\text{intermediate fields to } {}^{\overline{K}}\Big/_{K}\right\}$$

and

$$\{\text{Open subgroups of } G_K\} \longleftrightarrow \{\text{intermediate fields finite over } K\}$$

5.4.1 Application-ish

Consider $\overline{\mathbb{Q}} / \mathbb{Q}$ and $G_{\mathbb{Q}}$. Fix prime p. $\zeta_{p^n} = e^{2\pi i/p^n}$. Then we have a tower

$$\mathbb{Q} \subset \mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \cdots .$$

This gives us the map

$$G_{\mathbb{Q}} \to \operatorname{Gal}\left(\mathbb{Q}(\zeta_n) \big/ \mathbb{Q}\right) = \left(\mathbb{Z} \big/ p^n\mathbb{Z}\right)^{\times}.$$

This is compatible as n varies, go we get a homomorphism

$$\chi_p : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_p^{\times}.$$

This is known as the cyclotomic character. If $\zeta \in \overline{\mathbb{Q}}$ is a p-power root of 1 and $\sigma \in G_{\mathbb{Q}}$ then $\sigma\zeta = \zeta^{\chi_p(\sigma)}$.

Lecture 36: Elements of $G_{\mathbb{Q}}$

Let $\overline{\mathbb{Q}}$ be an abstract algebraic closure of $\mathbb{Q}$. Then $\exists$ an embedding 12 Apr. 02:00

$$i : \overline{\mathbb{Q}} \longmapsto \mathbb{C},$$

such that $i(\overline{\mathbb{Q}})$ is stable by complex conjugation c i.e. $i^{-1} \circ c \circ i \in G_{\mathbb{Q}}$.

Now say $j : \overline{\mathbb{Q}} \to \mathbb{C}$ is a second embedding. Then $i(\overline{\mathbb{Q}}) = j(\overline{\mathbb{Q}})$ i.e. $\sigma = j^{-1} \circ i \in G_{\mathbb{Q}}$.

$$j^{-1}cj = \underbrace{\sigma^{-1}(i^{-1}ci)\sigma}_{\text{conjugate to } i^{-1}ci \text{ in } G_{\mathbb{Q}}}.$$

The upshot is that there exists a conjugacy class in $G_{\mathbb{Q}}$ corresponding to complex conjugation. Similarly, there exists an embedding

$$i : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p.$$

We get a homorphism

$$\begin{aligned} G_{\mathbb{Q}_p} &\longrightarrow G_{\mathbb{Q}} \\ \sigma &\longmapsto i^{-1}\sigma i. \end{aligned}$$

Remark. There is some class of extensions of $\mathbb{Q}_p$ known as the "unramified" extensions that bijectively correspond to Galois extensions of $\mathbb{F}_p$.

The maximal unramified extension of $\mathbb{Q}_p$: $\mathbb{Q}_p^{\text{un}}$, corresponds the algebraic closure of $\mathbb{F}_p$. The extension from $\mathbb{Q}_p^{\text{un}}$ to $\overline{\mathbb{Q}}_p$ is Galois with Galois group $I_p \subset G_{\mathbb{Q}_p}$ known as the "inertia subgroup". Additionally, the extension from $\mathbb{Q}_p$ to $\mathbb{Q}_p^{\text{un}}$ is Galois with group $\hat{\mathbb{Z}}$, where $\hat{\mathbb{Z}}$ is generated by Frob_p.

Suppose $K / \mathbb{Q}$ is a finite Galois extension. Then there exists a surjection $\pi : G_{\mathbb{Q}} \to \operatorname{Gal}(K / \mathbb{Q})$.

Remark. For all but finitely many p, $\pi(I_p) = 1$. We say that K is unramified at p if $\pi(I_p) = 1$.

Example. $\mathbb{Q}(i)$.

- $2 = (1+i)^2$ (up to units)
- If $p \equiv 1 \bmod 4$, $p = \pi\overline{\pi}$ in $\mathbb{Z}[i]$.
- If $p \equiv 3 \bmod 4$, p remains prime in $\mathbb{Z}[i]$.

Then we are ramified at 2 and unramified at all odd p. For all odd p, we get a well-defined element

$\mathrm{Frob}_p \in \mathrm{Gal}(\mathbb{Q}(i) / \mathbb{Q}) \cong \mathbb{Z} / 2$, where

$$\mathrm{Frob}_p = \begin{cases} 1, & \text{if } p = 1 \bmod 4 \\ \neq 1, & \text{if } p = 3 \bmod 4 \end{cases}.$$

Fix a finite set Σ of primes. There exists a maximal algebraic extension $\overline{\mathbb{Q}}^{\Sigma}$ of $\mathbb{Q}$ such that $\forall p \notin \Sigma$, p is unramified in $\overline{\mathbb{Q}}^{\Sigma}$. Let $G_{\mathbb{Q},\Sigma} = \mathrm{Gal}(\overline{\mathbb{Q}}^{\Sigma}/\mathbb{Q})$ i.e.

$$G_{\mathbb{Q},\Sigma} = {}^{G_{\mathbb{Q}}}\Big/_{(\text{normal subgroup generated by } I_p \text{ with } p \in \Sigma)}.$$

For $p \notin \Sigma$, there exists a well-defined conjugacy class of elements $\mathrm{Frob}_p \in G_{\mathbb{Q},\Sigma}$. Also have complex conjugation $c \in G_{\mathbb{Q},\Sigma}$.

Theorem 5.4.2 (Chebotarev density theorem). We have the following two equivalent formulations:

(1) The Frob_p's are dense in $G_{\mathbb{Q},\Sigma}$ for $p \notin \Sigma$.

(2) If $K / \mathbb{Q}$ is a finite Galois extension then every element of $\mathrm{Gal}(K / \mathbb{Q})$ is of the form Frob_p for some prime p.

Let $K / \mathbb{Q}$ be a finite Galois extension, unramified outside of Σ. Consider a representation

$$\rho : \underbrace{\mathrm{Gal}({}^{K}\big/_{\mathbb{Q}})}_{\text{finite group}} \to \mathrm{GL}_n(\mathbb{C}).$$

For $\rho \notin \Sigma$, we have a conjugacy class Frob_p in $\mathrm{Gal}(K / \mathbb{Q})$. Then from the character we get a complex number $\chi_\rho(\mathrm{Frob}_p) \in \mathbb{C}$.

For some fixed prime ℓ, now consider a continuous representation

$$\rho : G_{\mathbb{Q},\Sigma} \longrightarrow \mathrm{GL}_n(\mathbb{Q}_\ell).$$

For $p \notin \Sigma$, can consider $\chi_\rho(\mathrm{Frob}_p) \in \overline{\mathbb{Q}}_p$.

Example. Recall we have the cyclotomic character

$$\chi_\ell : G_{\mathbb{Q},\{\ell\}} \longrightarrow \mathbb{Z}_\ell^\times,$$

where

$$\sigma(\zeta) = \zeta^{\chi_\ell(\sigma}.$$

for an ℓ-power root of 1, ζ. We can think of χ_ℓ as a 1-d ℓ-adic representation

$$\chi_\ell(\mathrm{Frob}_p) = p.$$

Given $\rho : G_{\mathbb{Q},\Sigma} \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$, there exists a modular form f such that the numbers $\chi_\rho(\mathrm{Frob}_p)$ are the coefficients of f.

Example. $\Delta(q) = q\prod_{n\geq 1}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n$ for $q = e^{2\pi i z}$, $z \in h$. Then there exists a represenation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ such that $\operatorname{tr}\rho(\mathrm{Frob}_\rho) = \tau(p)$ and $\det\rho(\mathrm{Frob}_p) = p^{11}$.

Lecture 37: Final Exam Review

Will focus on stuff since the second midterm. Will be 6 questions choose 5. 17 Apr. 02:00

5.5 Finite Fields

- If F is a finite field then F contains $\mathbb{F}_p$ for some prime p.

- We say that F has characteristic p and $\#F = p^n$ because F is a finite dimensional $\mathbb{F}_p$-vector space i.e. $[F : \mathbb{F}_p] = n$.
- Given $q = p^n$ there exists a finite field $\mathbb{F}_q$ with q elements that is unique up to isomorphism.
$$\mathbb{F}_q = \text{ splitting field of } x^q - x.$$
- $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ iff $n|m$.
- $\mathbb{F}_q^\times$ is a cyclic group of order $q-1$.
- Concrete construction of $\mathbb{F}_{p^2}$.

  For $p \neq 2$, pick $a \in \mathbb{F}_p$ that is not a square. Then
$$\mathbb{F}_p[\sqrt{a}] = \frac{\mathbb{F}_p[x]}{(x^2 - a)} \text{ is a field with } p^2 \text{ elements.}$$
  For $p = 2$,
$$\mathbb{F}_4 = \frac{\mathbb{F}_2[x]}{(x^2 + x + 1)}.$$
- For $q = p^n$, $\phi : \mathbb{F}_q \to \mathbb{F}_q$ defined by $x \mapsto x^p$ is a field automorphism called the Frovenius map. ϕ generates $\mathrm{Aut}(\mathbb{F}_q) \cong \mathbb{Z} / n\mathbb{Z}$.

5.6 Galois Theory

There will be no infinite Galois theory on the exam.

- E / F - finite extension. Then
$$\mathrm{Gal}({}^{E}\big/{}_{F}) = \{\text{field automorphism } \sigma \text{ of } E \text{ such that } \sigma|_F = \mathrm{id}\}.$$
- E / F is a Galois extension if $\# \mathrm{Gal}(E / F) = [E : F]$.
- E / F is Galois if and only if E is the splitting field of some polynomial in $F[x]$.
- Important observation: if $\sigma \in \mathrm{Gal}(E / F)$ and $a \in E$ is a root of $f(x) \in F[x]$ then σa is also a root of $f(x)$.
- If E is the splitting field of $f(x) \in F[x]$ then $\mathrm{Gal}(E / F) \subset S_n$, where $n = \deg f$ i.e. the elements of the Galois group permute the n roots of $f(x)$.
  - If $f(x)$ is irreducible then this action is transitive.
  - If $a \in E$ and $a_1, \ldots, a_r$ is the Galois orbit of a then
$$h(x) = \prod_{i=1}^{r} (x - a_i) \in F[x].$$
    If f is irreducible and a is a root of f then $h|f$, such that $h = f$. Thus, the action is transitive.
- **Artin's theorem**. E is any field, $G \subset \mathrm{Aut}(E)$ is a finite group, $F = E^G$ then E / F is a Galois extension with group G.
  - $E = \mathbb{C}(x_1, \ldots, x_n)$, $G = S_n$ permuting variables. $F = E^{S_n}$. E / F is Galois with group S_n.
  - Write $\prod_{i=1}^n (t - x_i) = \sum_{i=1}^n a_i t^i$. $F = \mathbb{C}(a_0, \ldots, a_{n-1})$.
- **Main Theorem of Galois Theory**. Suppose E / F is a Galois extension with group G

- There is a bijective correspondence

$$\begin{aligned}\{\text{intermediate fields to } {}^{E}\big/_{F}\} &\longleftrightarrow \{\text{subgroups of } G\}\\ E^H &\longleftarrow H\\ K &\longmapsto \operatorname{Gal}({}^{E}\big/_{K}).\end{aligned}$$

- If $K = E^H$ then $K \,/\, F$ is Galois if and only if H is normal in G. Then $\operatorname{Gal}(K \,/\, F) = G \,/\, H$.
  * Assuming $K \,/\, F$ is Galois, every element of G maps K to itself.
  * We get a restriction map

$$\begin{aligned}\operatorname{Gal}({}^{E}\big/_{F}) &\longrightarrow \operatorname{Gal}({}^{K}\big/_{F})\\ \sigma &\longmapsto \sigma|_K.\end{aligned}$$

    This map is surjective with kernel H.
- The Galois correspondence is order-reversing i.e. if

$$\begin{aligned}H_1 &\longleftrightarrow K_1 = E^{H_1}\\ H_2 &\longleftrightarrow K_2 = E^{H_2}\end{aligned}$$

  then $H_1 \subset H_2$ iff $K_1 \supset K_2$.

- If E is the splitting field of f of $\deg n$ and $G = \operatorname{Gal}(E \,/\, F) \subset S_n$ then $G \subset A_n$ iff $\operatorname{disc}(f)$ is a square in F.
  - If $f(x) = x^3 + px + q$ is irreducible. Then

$$G = \begin{cases} S_3, & \text{if } \operatorname{disc}(f) \neq \square \\ A_3, & \text{if } \operatorname{disc}(f) = \square \end{cases},$$

    where $\operatorname{disc}(f) = -4p^3 - 27q^2$. This is because these are the only transitive subgroups of S_3.

- Important Examples:
  (a) If ζ_n = primitive nth root of 1. Then $F(\zeta_n)/F$ is Galois and $\operatorname{Gal}(F(\zeta_n) \,/\, F) \subset (\mathbb{Z} \,/\, n\mathbb{Z})^\times$. They are the same if $F = \mathbb{Q}$.
  (b) If $\zeta_n \in F$ and $a \in F$ then $F(a^{1/n})/F$ is Galois and $\operatorname{Gal}(F(a^{1/n}) \,/\, F) \subset \mathbb{Z} \,/\, n\mathbb{Z}$. Equality if a is not an nth power or some power dividing n.
  (c) We have the converse to (b). If $\zeta_n \in F$ and $E \,/\, F$ is a Galois extension with group $\mathbb{Z} \,/\, n\mathbb{Z}$ then $E = F(a^{1/n})$ for some $a \in F$.

- Useful trick: If $f(x) \in \mathbb{Q}[x]$ and E is the splitting field of f. Then complex conjugation is an element in $\operatorname{Gal}(E \,/\, \mathbb{Q})$. It will be non-trivial if ≥ 1 non-real root of f.

- Solvable groups **NOT** on final.