Algebra

Nathaniel D. Hoffman

December 18, 2020

Contents

Lecture 1: Algebra

Monday, August 31, 2020

Topics in this course:

- Groups
- Rings/modules

- Fields/Galois theory
- Algebraic geometry
- Representation theory

Office hours: Thursday 3pm or by appointment. Zoom link is on the website (no in-person office hours).

0.1 Recap of Group Theory

Group homomorphisms (groups G, H) $\varphi\colon G \to H$ preserve $\forall g_1, g_2 \quad \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$, $\varphi(g^{-1}) = \varphi(g)^{-1}$, and $\varphi(I_G) = I_H$. A group action of G on a set X is a homomorphism $G \to S_X$, where S_X is the symmetric group on X, set of bijections from X onto itself.

The usual notation for the group action is

$$\varphi(g)x \equiv g \cdot x$$

For example

(1) S_X acting on X: $S_x \xrightarrow{\text{id}} S_X$

(2) S_X acting on $\binom{X}{2} \equiv \{\{x_1, x_2\}\colon x_1, x_2 \in X\}$: $\pi \cdot \{x_1, x_2\} = \{\pi x_1, \pi x_2\}$

(2') S_X acting on $\binom{X}{k}$ or 2^X

(3) $\mathrm{GL}_n(F)$ being the set of n-by-n matrices M with coefficients in a field F where $\det(M) \neq 0$ ($\mathrm{GL}(F) \curvearrowright F^n$)

(4) We can also have the action of a subgroup if $G \curvearrowright X$ and $H \leq G$, $H \curvearrowright X$

(5) $\mathbb{Z}$-action on a metric space M given a homeomorphism $T\colon M \to M$ by $n \cdot x = T^{(n)}(x) = \underbrace{T(T(\cdots(x)))}_{n}$.

(6) G-actions on G

   (a) $g \cdot a = ga$

   (b) $g \cdot b = ag^{-1}$

   (c) Conjugation: $g \cdot a = gag^{-1}$. If $ag = ga$ then $gag^{-1} = a$

Let's examine the action $G \curvearrowright G$ on the left: $\varphi\colon G \to S_G$. We claim that $\ker\varphi = 1$. We can define the kernel by $\varphi(g) \cdot h = h \forall h \Leftrightarrow g \in \ker\varphi$. Hence, $gh = h \forall h \implies g = 1$.

Theorem 0.1.1 (Cayley)**.** *For all G, G is isomorphic to a subgroup of S_G.*

Proof: $G \simeq \frac{G}{\ker\varphi} \cong \varphi(G)$

Definition 0.1.1 (Orbits)**.** $G \curvearrowright X$, for $x \in X$ the set $G \cdot x = \{g \cdot x\colon g \in X\}$ is called the orbit of X under G.

The reason for this nomenclature is from the action of rotations in $\mathbb{R} \curvearrowright \mathbb{R}^2$. If we consider $\alpha \cdot v$ as the rotations of v by α, the orbit of $\mathbb{R}^2$ under $\mathbb{R}$ is the set of all rotations of v (an orbit of the magnitude of the vector about its origin).

LECTURE 2:
Wednesday, September 02, 2020

A final note on orbits: they are equivalence classes. We can prove this through the following propositions:

Proposition: If $y \in G \cdot x$ then $x \in G \cdot y$

Proof: $y = g \cdot x$ then $g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = id \cdot x = x$

Proposition: If X is finite and $G \curvearrowright X$, then $|G \cdot x| = |G|/|G_x|$ where $G_x := \{g \in G \mid gx = x\}$ (stabilizer of x)

Proof: $\varphi : G \to G \cdot x$, $g \mapsto g \cdot x$

Note

$h \in G_x =: H$ implies $\varphi(gh) = \varphi(g)$ since $ghx = gx$. φ is constant on the left cosets of H, i.e. sets of the form gH.

G/H is the set of left cosets. We can make maps $\pi(g) = gH$ and $\psi(gH) = \varphi(g)$. $\varphi = \psi\pi$ and $|G/H| = |G|/|H|$. We claim ψ is a bijection, and if we prove it, we prove the proposition. First, we can say its a surjection because ψ is a surjection. Suppose $\psi(g_1H) = \psi(g_2H)$. This is equivalent to $\varphi(g_1) = \varphi(g_2)$.

$$\begin{aligned} g_1 \cdot x = g_2 \cdot x &\Leftrightarrow g_1^{-1}g_2 \cdot x = x \\ &\Leftrightarrow g_1^{-1}g_2 \in G_x = H \\ &\Leftrightarrow g_2 \in g_1 H \\ &\Leftrightarrow g_2 H = g_1 H \end{aligned}$$

which proves injectivity.

0.1.1 Fixed Points

Definition 0.1.2. An orbit of size 1 is called a *fixed point*.

Definition 0.1.3. The orbit of $G \curvearrowright G$ by conjugation—the orbit of this action is a conjugacy class. The *centralizer* is the stabilizer for this action: $C_G(x) = \{g \in G \mid gxg^{-1} = x\}$.

Definition 0.1.4. We can also look at mappings like $G \curvearrowright 2^G$. If we look at subgroups $H \leq G$, the stabilizer of H is called the *normalizer*: $N_G(H) = \{g \mid gHg^{-1} = H\}$.

Definition 0.1.5. The *center* of G is $Z(G) = \{h \in G \mid g^{-1}hg = h \quad \forall g \in G\}$.

If G is finite,

$$G = Z(G) \cup G \cdot x_1 \cup \cdots \cup G \cdot x_r$$

where $x_1 \cdots x_r$ are representations of non-central conjugacy classes. Additionally,

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G \colon C_G(x_i)]$$

0.2 P-Groups

Definition 0.2.1. A group G is a *p-group* if $|G| = p^m$ where p is prime.

The reason these are important in group theory is that most finite groups are p-groups.

Definition 0.2.2. For finite groups G, if p divides $|G|$ and p^m divides $|G|$ but p^{m+1} does not divide $|G|$ and $H \leq G$ of order $|H| = p^m$, we call H the *p-Sylow subgroup* of G.

We will use the notation $a \mid b$ sometimes for a "divides" b.

Theorem 0.2.1 (Sylow I)**.** *If $p \mid |G|$, then G contains a p-Sylow subgroup.*

Lemma 0.2.2. *If G is abelian, $p \mid |G|$ then G contains a subgroup of order p.*

Proof. A number n is an *exponent* of G if $g^n = 1 \quad \forall g \in G$. We claim if n is an exponent of an abelian group G, then $|G| \mid n^m \quad \exists m$. We can prove this by induction on $|G|$: $b \in G$ and $b \neq 1$, we can define a subgroup $H =< b >$, the powers of b. Therefore, $b^{|H|} = 1 \implies |H| \mid n$. Because n is an exponent of G, n is also an exponent of G/H: $(gH)^n = g^n H$. By induction, $\exists m$ such that $|G/H| \mid n^m$: $|G| = |G/H| \cdot |H|$ and $n^m \cdot n = n^{m+1}$.

Consider $n = \prod_{g \in G} |g|$. n is an exponent of G. Therefore, we know that $p \mid |G|$ and $|G| \mid n^m$, so $p \mid |g|$ for some $g \in G$. $h = g^{|g|/p}$, so $|h| = p$. □

Let's now use this lemma to prove the first Sylow theorem:

Proof. Proof by induction on $|G|$. Let's assume $|G| = p^m n$ where $p \not| n$. If $H < G$ and $p^m \mid |H|$, then a p-Sylow subgroup of H is a p-Sylow subgroup of G.

For all $H < G$, assume the largest power of p dividing $|H|$ is $p^{l(H)}$ with $l < m$. This is equivalent to $p \mid [G\colon H]$. Recall that we can say

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G\colon C_G(x_i)]$$

We know that $p \mid |G|$ and $p \mid [G\colon C_G(x_i)]$, so $p \mid |Z(G)|$. By the lemma we just proved, $\exists H \leq Z(G)$ such that $|H| = p$.

$Z(G) \triangleleft G$ (normal subgroup) and even $H \triangleleft G$. Consider $G' = G/H$. We want to use induction to find P', the p-Sylow subgroup in G'.

$G \xrightarrow{\pi} G/H = G' \geq P'$. We are going to pull back $P = \pi^{-1}(P')$. $|P| = p \cdot |P'|$, so P is a subgroup. □

Lecture 3: The Sylow Theorems

Friday, September 04, 2020

Theorem 0.2.3 (Sylow)**.** *Let G be finite, prime $p \mid |G|$, P is p-Sylow:*

1. *If H is a p-subgroup of G, then a conjugate of H is in P.*
2. *All p-Sylow subgroups of G are conjugate.*
3. *The number of p-Sylow subgroups is $1(\mod p)$.*

Lemma 0.2.4. *If G is a p-group and $G \curvearrowright X$, then the number of fixed points is $|X|(\mod p)$.*

Proof.

$$|X| = \sum_{i=1}^{r} |G \cdot x_i| = \sum_{i=1}^{r} [G : G_{x_i}]$$

We can write this as the number of fixed points plus the sum of powers of p. Taking everything mod-p, we get the desired result. □

Lemma 0.2.5. *If $H \leq G$ is a p-subgroup, P is p-Sylow and $H \leq N_G(P)$, then $H \leq P$.*

Note that $P \subseteq N_G(P) = \{g \mid gPg^{-1} = P\}$.

Proof. Consider HP. $HP \leq G$. This is not necessarily true for two subgroups, but this works because $h_1p_1h_2p_2 = h_1h_2h_2^{-1}p_1h_2p_2 = h_1h_2p_1p_2$ because H is in the normalizer of P.

The second isomorphism theorem says that $(HP)/P \cong H/(H \cap P)$. The proof of this is that we can make a projection map $H \xrightarrow{\pi} HP/P$ which maps $h \mapsto hP$ surjectively. $\ker\pi = H \cap P$ so by the first isomorphism theory this is proven.

$$[HP : P] = [H : H \cap P]$$

If $H \not\leq P$ then HP is strictly larger than P. Hence, HP is a larger p-group than P. This is a contradiction. □

Proof. Finally we will prove all the Sylow theorems. Consider S to be the set of all p-Sylow subgroups of G. Let's examine the conjugation action $G \curvearrowright S$. $P \leq N_G(P)$, the stabilizer of this action, so

$$p \not| [G : N_G(P)] = \frac{|G|}{|N_G(P)|} = \frac{|G|}{|P|}\frac{|P|}{|N_G(P)|}$$

Therefore,

$$|G \cdot P| = \frac{|G|}{|N_G(P)|} \neq 0(\mod p)$$

on the other hand, consider the action of $H \curvearrowright G \cdot P$. The number of fixed points is $|G \cdot P| \neq 0(\mod p)$.

Suppose $Q \in G \cdot P$ is a fixed point. This means $H \leq N_G(Q)$ by definition. By the second lemma we proved, $H \leq Q = gPg^{-1}$. This proves the first part of the Sylow theorem. For the second part, take H to be the p-Sylow subgroup and apply (1). By (1), $H \subseteq gPg^{-1}$.

For part (3), we know that $G \cdot P = S$ by part (2). By part (2), the number of fixed points is equal to the number of p-Sylow subgroups containing H. □

Example. If $|G| = 35$, and G is abelian, $S_5 \leq G \mod 5$, and $S_7 \leq G \mod 7$.

The number of 5-Sylow subgroups is $1(\mod 5) = \frac{|G|}{|N_G(S_5)|}$, so S_5 is the only 5-Sylow subgroup of G. Similarly with S_7, so S_5 and S_7 are normal in G. ◇

Proposition: If $|G|$ is finite, p is the smallest prime dividing $|G|$, and $[G : H] = p$, then H is normal.

Lecture 4:
Wednesday, September 09, 2020

If $X \subseteq G$, the group generated by X, denoted by, $\langle X \rangle$ is the smallest group containing X:

$$\langle X \rangle = \bigcap_{H \subseteq G,\ X \subseteq H} H$$

Equivalently,

$$\langle X \rangle = \{x_1^{\epsilon_1}x_2^{\epsilon_2} \cdots x_n^{\epsilon_n} \mid \epsilon \in \{\pm 1\},\ n \in \mathbb{Z} \geq 0\}$$

Definition 0.2.3. If S is a set, the *free group* on S, $F(S)$, "consists of" all formal expressions of the form $x_1^{\epsilon_1}x_2^{\epsilon_2}\cdots x_n^{\epsilon_n}$ with multiplication being the concatenation. This is not yet a group, but rather a monoid (no inverses). We also need to define equivalence classes of "words" in the obvious way, namely you can cancel adjacent pairs of elements and their inverses and insert these pairs arbitrarily.

Conjugation Notation

We don't want to write things like $b^{-1}ab$ all the time so we will just call it a^b. Additionally, we can write things like

$$(a^b)^c = a^{bc} = c^{-1}(b^{-1}ab)c$$

Additionally, $1^a = 1$ and $a^1 = a$ by definition.

Definition 0.2.4. The *commutator* of a and b is denoted by $[a,b] = a^{-1}b^{-1}ab$. By this definition, $[a,b] = 1 \iff ab = ba$ or equivalently $ab = ba[a,b]$.

$$[a,bc] = [a,c][a,b][a,b,c]$$

and

$$[ab,c] = [a,c][a,c,b][b,c]$$

where $[a,b,c] \equiv [[a,b],c]$. More generally,

$$[a,b,c,\cdots,z] = [[\cdots[a,b],\cdots],z]$$

Additionally,

$$[a,b,c^a][c,a,b^c][b,c,a^b] = 1 \qquad \text{(Hall's Identity)}$$

If $A, B \triangleleft G$, we can define

$$[A,B] \equiv \langle [a,b] \mid a \in A,\ b \in B \rangle$$

and this group, $A \cap B$, and AB are all normal in G.

$$[A,B] \subseteq A \cap B$$

Why? $[a,b] = a^{-1}b^{-1}ab = a^{-1}a^b \in A = (b^{-1})^a b \in B$.

If we define $[A,B,C] = [[A,B],C]$, we claim that $[A,B,C] = \langle [a,b,c] \mid a \in A,\ b \in B,\ c \in C \rangle = H$.

Proof.

$$[a,b,c] \in [A,B,C]$$

$$[\prod_{i=1}^{n}[a_i,b_i]^{\epsilon_i},c] = \underbrace{[[a_1,b_1]^{\epsilon_1},c]}_{\in H} \underbrace{[[a_1,b_1]^{\epsilon_1},c_1\prod_{i=2}^{n}[a_i,b_i]^{\epsilon_i}]}_{[[a,b,c],\prod[a_i,b_i]^{\epsilon_i}\in H \text{ since } [a,b,c]\in H} \underbrace{[\prod_{i=2}^{n}[a_i,b_i],c]}_{\in H}$$

□

Definition 0.2.5. Nilpotent Groups: Take a series of subgroups $\gamma_0(G) = G$, $\gamma_i(G) = [\gamma_{i-1}(G), G]$, etc. It is clear from this definition that $\gamma_0 \supseteq \gamma_1 \supseteq \gamma_2 \cdots$. All of these subgroups are normal in G ($\gamma_i \triangleleft G$).

We say G is nilpotent of step s if $\gamma^{s+1}(G) = 1$ yet $\gamma^s(G) \neq 1$.

Lecture 5:
Friday, September 11, 2020

Aside

In the last class, there was a question about the inverse of commutators in this derivation. We want to show that

$$\left[[a,b]^{-1},c\right] = [[b,a],c] \in [A,B,C]$$

Let's examine

$$\begin{aligned}
[[b,a],c]^{b^{-1}} &= \left[[b,a]^{b^{-1}}, c^{b^{-1}}\right] \\
&= \left[b(b^{-1}a^{-1}ba)b^{-1}, c^{b^{-1}}\right] \\
&= \left[a^{-1}bab^{-1}, c^{b^{-1}}\right] \\
&= \left[\left[a, \underbrace{b^{-1}}_{\in B}\right], \underbrace{c^{b^{-1}}}_{\in C}\right] \in [A,B,C]
\end{aligned}$$

Back to nilpotent groups. When we say that $a \equiv b \pmod H$, we mean $H \triangleleft G$, $aH = bH$ for $a = b \in G/H$.

$$ab = ba \mod \gamma_1$$

Claim.

$$[A,B,C] \subseteq [C,A,B][B,C,A]$$

Claim. If $a \in \gamma_i$, $b \in \gamma_j$, then $[a,b] \in \gamma_{i+j}$. In particular, $ab \equiv ba \mod \gamma_{i+j}$.

Proof. We will prove this by induction on $\min(i,j)$. If $j = 1$, we are done by definition. Let's then take $a \in \gamma_{i-1}$, $b \in \gamma_{j+1}$.

$$[\gamma_{i-1}, \gamma_{j+1}] = [\gamma_{i-1}, [\gamma_j, G]]$$

(proof unfinished) □

Examples of nilpotent groups

(0) Abelian groups are nilpotent of rank 0.

(1) If G is nilpotent, $G/Z(G)$ is nilpotent because $\gamma_i(G/Z(G)) = \frac{\gamma_i(G)Z}{Z}$. Elements of γ_i are generated by nested commutators with $i-1$ bracket pairs. $[g_1Z, g_2Z] = [g_1,g_2]Z$.

In particular, if G is nilpotent of step s, then $G/Z(G)$ is nilpotent of step $s-1$ because $\gamma_s \neq 1$ and $1 = [\gamma_s, G]$ implies $\gamma_s \subseteq Z(G)$.

(2) p-groups have non-trivial center. By induction on $|G|$, you can prove that p-groups are nilpotent.

If G/Z is nilpotent, say $\gamma_s(G/Z) = 1$, then $\gamma_{s+1}(G) \subseteq Z$ which implies $\gamma_{s+2}(G) = 1$.

Definition 0.2.6. A *subring* R of a ring with a unit is nilpotent of step s if the product of any $s+1$ elements is 0.

Claim. The set $1_R + R$ (the unit plus the elements of the subring) is a nilpotent group.

Example.

$$R = \begin{pmatrix} 0 & a & b & \cdots \\ \vdots & \ddots & c & \cdots \end{pmatrix}_{n\times n}$$

is nilpotent of step $n-1$. ◇

(back to claim) For $r \in R$,

$$(1-r)^{-1} = 1 + r + r^2 + \cdots r^s$$
$$(1-r)(1+r+\cdots+r^s) = 1 - r^{s+1} = 1$$

Claim. If $r \in R^k$, $r' \in R$,

$$[1-r, 1-r'] \in 1 + R^{k+1}$$

where $R^k = \text{span}\{r_1 r_2 \dots r_k\}$ or $R^k = \{\sum_{i=1}^m \prod_{j=1}^k r_{ij} \mid r_{ij} \in R,\ m \in \mathbb{Z} \geq 0\}$, so for example, $R^2 = \{r_1 r_2 + r_3 r_4 + \dots + r_{99} r_{100}, \dots\}$.

Proof.

$$\begin{aligned}
(1 + \overbrace{r + r^2 + \dots + r^s}^{\#1})(1 + \overbrace{r' + r'^2 + \dots + r'^s}^{\#2})(1 - \overbrace{r}^{\#3})(1 - \overbrace{r'}^{\#4}) \\
&= \overbrace{(1 + r' + \dots + r'^s)(1 - r')}^{=1} + \overbrace{\#1}^{\in R^k}(\#2 + \#3 \dots) \\
&+ \#2\#3\#4 + \#1 \cdot 1 + \#3 \cdot 1 \\
&\in 1 + rR + RrR + rR + (r + r^2 + \dots + r^s - r) \\
&\in 1 + R^{k+1}
\end{aligned}$$

□

Lecture 6:
Monday, September 14, 2020

Claim.

$$[A, B, C] \subseteq [C, B, A][B, C, A]$$

Proof.

$$[a, b, c^a][c, a, b^c][b, c, a^b] = 1$$

□

Claim.

$$[\gamma_i, \gamma_j] \subseteq \gamma_{i+j}$$

Proof. Induction on $\min(i, j)$: For $j = 1$, this is the definition.

$$\begin{aligned}
[\gamma_i, \gamma_j] &= [\gamma_i, [\gamma_{j-1}, G]] \\
&= [G, \gamma_{j-1}, \gamma_i] \\
&\subseteq [[\gamma_i, G], \gamma_{j-1}][\gamma_{j-1}, \gamma_i, G] && \subseteq \gamma_{i+j}\gamma_{i+j}
\end{aligned}$$

□

(3) Heisenberg group expressions of the form $a^l b^m c^n$

$ac = ca$, $cb = bc$, $ab = bac$, so $a^l b^m c^n \mapsto \begin{pmatrix} 1 & l & n \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix}$

Nilpotent groups are examples of corner central series: $\gamma_1 \lhd \gamma_2 \lhd \gamma_3 \lhd \cdots$.

We can also have upper central series: $Z_0 = 1$, Z_{i+1} consists of elements of G that commute with all G mod (Z_i):

$$g \in Z_{i+1} \iff [g, h] \in Z_i\ \forall h \in G \iff [gZ_i, hZ_i] = 1 \text{ in } G/Z_i$$

By definition, $gZ_i \in Z(G/Z_i)$ (the center of G), so Z_{i+1} is the image under the $G \to G/Z_i$ projection of $Z(G/Z_i)$.

Claim. If G is nilpotent of step s (i.e. $\gamma_{s+1} = 1$), iff $Z_s = G$, and in this case, $\gamma_i \subseteq Z_{s-i+1}$.

Proof. Suppose $\gamma_{s+1} = 1$. This implies $\gamma_s \subseteq Z(G)$.

Assume $\gamma_{i+1} \subseteq Z_{s-i}$. We know that γ_i commute with $G \mod \gamma_{i+1}$. This means that γ_i commute with $G \mod Z_{s-i}$. But this also means (by definition of Z_i) that $\gamma_i \subseteq Z_{s-i+1}$.

Since $\gamma_1 = G$, then $Z_s = \gamma_1 = G$ so $Z_s = G$. Elements of Z_{s-i+2} commute with $G \mod Z_{s-i+1}$ so $\gamma_i = [\gamma_{i-1}, G] \subseteq Z_{s-i+1}$. □

In general, central series are sequences of normal subgroups: $1 = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots$. The minimal length central series have the same length and satisfy

$$\begin{array}{rccccc} 1 = & Z_0 \triangleleft \cdots \triangleleft & & Z_1 \triangleleft \cdots \triangleleft & Z_s = G \\ & \triangledown & & \triangledown & \triangledown \\ 1 = & G_0 \triangleleft \cdots \triangleleft & & G_1 \triangleleft \cdots \triangleleft & G_s = G \\ & \triangledown & & \triangledown & \triangledown \\ 1 = & \gamma_{s+1} \triangleleft \cdots \triangleleft & \gamma_{s-i+1} & \triangleleft \cdots \triangleleft & \gamma_1 = G \end{array}$$

Theorem 0.2.6. *Finite G is nilpotent iff it is a product of Sylow subgroups. Say $P_1, \cdots, P_l$ are Sylow subgroups for primes $p_1, \cdots, p_l$. Then $G = p_1 p_2 \cdots p_l \cong P_1 \times \cdots \times P_l$*

Proof. Claim 1: If $H \leq G$, then $H \leq N_G(H)$.

Proof of 1: We can prove this by induction on $|G|$. First, we know that $Z(G) \leq N_G(H)$. If $Z(G) \nsubseteq H$, we are done. Otherwise, we know that $H/Z(G) < G/Z(G)$, so by induction, $H/Z < N_{G/Z}(H/Z) = N$. Pull back any element of N.

Claim 1 implies that if P is Sylow, then $N_G(P) = P$. □

Lecture 7:
Wednesday, September 16, 2020

We will continue with the proof from the last lecture. We ended with the claim that if $H < G$, then $N_G(H) > H$. Next, we claim that every Sylow subgroup is normal in G.

Proof. P is p-Sylow in G. Consider the normalizer $N = N_G(P)$. We can trivially say that $P \triangleleft N$.

Now consider the normalizer of the normalizer, $H = N_G(N)$. For $h \in H$, $P^h \subseteq N^h = N$. P^h is a subgroup of size $|P|$. Since all p-Sylow subgroups are conjugate. This means that P is the only p-Sylow subgroup of N.

$P^h = P$ and hence $P \triangleleft N_G(N)$. That means that $N_G(N) \subseteq N$. Therefore, $N_G(N) = N$. Therefore, by our first claim, $N = G$. □

The final step in the original proof is by induction.

Claim.

$$P_1 P_2 \cdots P_s \cong P_1 \times P_2 \times \cdots \times P_s$$

Proof. For $s = 1$, this is trivial. Now suppose $H = P_1 P_2 \cdots P_s \triangleleft G$. Let's look at $H \cap P_{s+1}$. $|H \cap P_{s+1}|$ divides both $|H|$ and $|P_{s+1}|$. The order of H is the power of primes up to s while the order of P_{s+1} is a power of that prime, so $H \cap P_{s+1} = 1$.

Recall $[H, P_{s+1}] \subseteq H \cap P_{s+1} = 1$, so these commute, and we have an isomorphism. □

0.3 Solvable Groups

Like nilpotent groups, we can describe another kind of series, called a derived series:

$$G^{(0)} = G \qquad G^{(1)} = [G, G] \qquad G^{(i+1)} = \left[G^{(i)}, G^{(i)}\right]$$

Definition 0.3.1. A group G is *solvable* if $G^{(s)} = 1$ for some s. The smallest such s is called the *solvable length.*

Lemma 0.3.1. *If $N \triangleleft G$, then $[G/N, G/N] = \frac{[G,G]N}{N}$.*

Proof.

$$[g_1N, g_2N] = [g_1, g_2]N$$

If we now take a group generated by this commutator, we see that

$$\langle [g_1N, g_2N] \rangle = \langle [g_1, g_2] \rangle N = [G, G]N$$

□

Claim. If $N \triangleleft G$, then G is solvable iff both N and G/N are.

Proof. Suppose G is solvable. $N^{(i)} \subseteq G^{(i)}$ by induction on i. We know that $G^{(s)} = 1$ for some s, so $N^{(s)} = 1$ (it possibly has a shorter solvable length, but we don't care).

Now what about G/N? From our lemma, we know that

$$\left(\frac{G}{N}\right)^{(i)} = \frac{G^{(i)}N}{N} \implies \left(\frac{G}{N}\right)^{(s)} = \frac{N}{N} = 1_N$$

In the converse direction, assume N and G/N are solvable. This means that $\exists s$ such that $\left(\frac{G}{N}\right)^{(s)} = 1$ and $\exists t$ such that $N^{(t)} = 1$.

$$\begin{aligned} \frac{G^{(s)}N}{N} = \left(\frac{G}{N}\right)^{(s)} = 1_N &\implies G^{(s)} \leq N \\ &\implies G^{(s+i)} \leq N^{(i)} \quad \forall i \\ &\implies G^{(s+t)} \leq N^t = 1 \end{aligned}$$

□

Claim. A group G is solvable iff there is a series of subgroups $1 = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_s = G$ and $\frac{H_{i+1}}{H_i}$ are abelian for all i.

Proof. First, an observation. For $H \triangleleft G$, if G/H is abelian,

$$\frac{[G, G]H}{H} = \left[\frac{G}{H}, \frac{G}{H}\right] = 1$$

and so $[G, G] \subseteq H$.

Now suppose $H_0, H_1, \cdots, H_s$ exist. We claim that $G^{(i)} \subseteq H_{s-i}$ by induction. For $i = 0$ this is trivially true.

$$G^{(i+1)} = \left[G^{(i)}, G^{(i)}\right] \subseteq [H_{s-i}, H_{s-i}] \subseteq H_{s-i-1}$$

For the converse, set $H_i = G^{(s-i)}$. $\frac{H_{i+1}}{H_i}$ is abelian. □

0.4 Ring Morphisms

Rings are associative but not necessarily with 1.

Definition 0.4.1. A *ring morphism* is a morphism $\varphi\colon R \to S$ such that $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$.

Definition 0.4.2. The *ideal* is the kernel of a morphism.

LECTURE 8:
Friday, September 18, 2020

Definition 0.4.3. $a \neq 0$ is a *zero divisor* if $\exists b$ such that $ab = 0$ or $ba = 0$.

Definition 0.4.4. A ring R is an *integral domain* if R is commutative and has no zero divisors.

Definition 0.4.5. A *field* is a commutative ring where all nonzero elements have an inverse.

0.5 Polynomial Rings

R is a commutative ring with 1. X is a symbol. $R[X]$ consists of all formal expressions of the form

$$a_0 + a_1 x + \cdots + a_n x^n$$

with $n \in \mathbb{Z}_{\geq 0}$ and $n_i \in R$ with the usual addition and multiplication in the ring.

$$(a_0 + a_1 x + \cdots + axunx^n)(b_0 + b_1 x + \cdots + b_m x^m) = \sum_{t=0}^{\infty} x^t \sum_{i+j=t} a_i b_j$$

Formally, $R[X]$ consists of functions $f\colon \mathbb{Z}_{\geq 0} \to R$ with finite support ($f(i) \neq 0$ only at finitely many points).

0.5.1 Power Series and Laurent Series

A power series is an expression of the form $a_0 + a_1 x + \cdots + a_n x^n + \cdots$, usually denoted $R[[X]]$ (no finite support).

A Laurent series a power series that allows for negative powers:

$$a_{-m} x^{-m} + a_{-m+1} x^{-m+1} + \cdots + a_0 + a_1 x + \cdots$$

Notation

$$(R[X])[Y] \equiv R[X,Y] \cong R[Y,X]$$

and if

$$X = (X_1, X_2, \cdots, X_n)$$
$$R[X] = R[X_1, X_2, \cdots, X_n]$$

Fun Aside

We can construct ordered rings by adding some ordering operation $(R, <)$ with the usual rules. For example, $\mathbb{R}[X]$ with the ordering $p < q \iff LC(q-p) > 0$ where $LC(p)$ is the leading coefficient of p.
This ordering is a way to define the statement

$$\lim_{x\to\infty}(q-p)(x) > 0$$

Another example is $q > p$ if the least significant nonzero coefficient of $q - p$ is > 0. Instead of $\mathbb{R}[X]$, we can think of instead $\mathbb{R}[\epsilon]$ where ϵ is "infinitesimal"

0.6 Group Rings

Definition 0.6.1. G is a group, R is a commutative ring with 1. The ring $R[G]$ consists of formal expressions of the form $a_1g_1 + a_2g_2 + \cdots + a_ng_n$ where $n \in \mathbb{Z}_{\geq 0}$, $a_i \in R$, and $g_i \in G$.

For example, if we look at $R[\mathbb{Z}]$, this is almost the same as $R[X]$. If we have $a_1n_1 + a_2n_2 + \cdots + a_mn_m$, this is equivalent to writing $a_1x^{n_1} + a_2x^{n_2} + \cdots + a_mx^{n_m}$.

Formally, we define group rings as functions $f\colon G \to R$ with finite support and

$$(f+g)(x) = f(x) + g(x) \qquad (fg)(x) = \sum_{y,z=x} f(y)g(z)$$

Polynomial Functions

$f \in R[X]$ induces a function $R \to R$: $x \in R \mapsto a_0 + a_1x + \cdots + a_nx^n$.

Example.

$$R = \mathbb{Z}/2\mathbb{Z}$$
$$x \in \mathbb{Z}/2\mathbb{Z}[X]$$

and

$$x^2 \in \mathbb{Z}/2\mathbb{Z}[X]$$

induce the same functions, since $0^2 = 0$ and $1^2 = 1$. ◇

0.7 Ideals

Recall $I \subseteq R$ is an ideal if I is a subring of R and $ab \in I$ if either a or b is in I. This is equivalent to saying $I = \ker\varphi$ for some morphism φ: $\varphi\colon R \to R/I$.

Example. The main example is $n\mathbb{Z} \subseteq \mathbb{Z} \quad \forall n$. ◇

0.7.1 Generation

For a ring R, if $A \subseteq R$, (A) is the ideal generated by A:

$$(A) = \Cap_{I \supseteq A} I$$

where I is ideal.

If $R \subseteq S$ and $A \subseteq S$, the notation $R[A]$ is the subring of S generated by $R \cup A$.

For example, $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}\colon a, b \in \mathbb{Z}\}$.

Notation

Say F is a field and $F \subset G$, another field. $A \subseteq G$ is a set, and $F(A)$ is the field generated by $F \cup A$.

Definition 0.7.1. Ideal $M \subset R$ is *maximal* if $M \neq R$ and there is no ideal I such that $M \subset I \subset R$.

Definition 0.7.2. An ideal $P \subset R$ is *prime* if $\forall a, b$, $ab \in P$ then either $a \in P$ or $b \in P$.

Example. $n\mathbb{Z}$ is prime in $\mathbb{Z}$ iff n is prime or negative prime. ◇

Properties of commutative R:

- $M \subseteq R$ is maximal iff R/M is a field
- $P \subset R$ is prime iff R/P is an integral domain (no zero divisors)

Proof. Fun observation: if $I \subseteq R$ is ideal, then $I = R \iff 1 \in I$. □

LECTURE 9:
Monday, September 21, 2020

0.8 Factorization

Definition 0.8.1. Suppose R is an integral domain. Then $N \colon R \to \mathbb{Z}_{\geq 0}$ is a *norm* that makes R into a *Euclidean domain* if $\forall a \in R$, $\forall q \neq 0$, $\exists b, r$ such that $a = qb + r$ such that $N(r) \geq N(q)$.

Example. In $\mathbb{Z}$, $N(a) = |a|$. ◇

Example. In a field $\mathbb{F}$, $f \in \mathbb{F}[x]$, $N(f) = \deg(f) + 1$ and $N(0) = 0$. ◇

Definition 0.8.2. A *principal ideal domain* is an integral domain all of whose ideals are principal (they are generated by a single element).

Claim. Euclidean domains are principal ideal domains.

Proof. Consider ideal $I \subset R$. Say that $m = \min\{N(a) \colon a \in I - 0\}$ and pick $a \in I$ such that $N(a) = m$. We claim that $I = (a)$ (I is generated by a). $(a) \subseteq I$, so for $b \in I$, $\exists c, r$ such that $b = ac + r$. $N(r) < N(a) = m$, and $r \in (a, b) \subseteq I$. □

Recall that a prime ideal $P \subseteq R$ is an ideal such that $ab \in P$ implies $a \in P$ or $b \in P$.

Definition 0.8.3. A *prime element* is a $p \in R$ such that (p) is prime and $a \in (p) \iff \exists b, a = bp$.

Definition 0.8.4. An *irreducible* element a is an element such that when $a = bc$ then either b or c is a unit invertible.

Claim. If $p \in R$ is prime, then p is irreducible.

Proof. We want to show that if $p = ab$ then either $p \mid a$ or $p \mid b$. Say $a = cp$. Then $p = (cp)b \implies cb$ is irreducible. □

The reverse is not true (not all irreducibles are prime):

Example.

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$$

Now $6 = 2 \cdot 3 \in \mathbb{Z}[\sqrt{-5}]$, and 2 and 3 are irreducible. Consider the mapping $x \mapsto |x|^2$, so $N(a+b\sqrt{-5}) = a^2 + 5b^2$. There are other ways to factor 6:

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

2 and 3 are irreducible but neither divides $1 \pm \sqrt{-5}$. ◇

0.8.1 Uniqueness of Factorization into Ideals

This is true for many rings, and for example, consider the ring we just used, $\mathbb{Z}[\sqrt{-5}]$.

$$(2) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}) = (4, 2 \pm 2\sqrt{-5}, 6) = (2, 2 \pm 2\sqrt{-5})$$

which is ideal.

Definition 0.8.5. An integral domain R is a *unique factorization domain* (UFD) if every $x \in R$ can be written $x = ur_1r_2 \cdots r_s$ where r_i are irreducible, u is a unit, and this is unique up to permuting r's and replacing them by associates (i.e. replace $r \to ru$).

Claim. Prime ideal domains are unique factorization domains (converse is not true).

Proof. Let S be the set of all elements in PID R such that they cannot be factored into irreducibles (we want to show this set is empty). Consider chains of ideals

$$(a_1) \subset (a_2) \subset \cdots$$

where $a_i \in S$.

$$I = \bigcup_{i=1}^{\infty} (a_i)$$

is an ideal. A PID implies that $\exists a \in R$ such that $I = (a)$. $a \in I \implies a \in (a_i)$ for some i. This implies $(a_i) \subseteq I = (a) \subseteq (a_i)$, so the chain must be finite. Let the last element be (a_n). a_n is not irreducible since it is in S, therefore it can be factored:

$$\exists b, c \qquad bc = a_n$$

where b, c are not units. In this case, we can extend the chain: If both b and c are not in S, then they have factorizations, so multiplying those factorizations gives a factorization of a_n. If $b \in S$, $(a_n) \subset (b)$. Hence $S = \emptyset$.

Proving uniqueness is easier. Suppose $x = ur_1r_2 \cdots r_m$. We claim that in a PID, irreducibles are prime. For some irreducible p, $p \mid ab$, and we want to show it divides either a or b. Suppose p does not divide a. Consider (p, a). This is an ideal inside the PID. That means there is a way to generate it with a single element: $\exists c \in R$ such that $(p, a) = (c)$. This means that $c \mid p$, and since p is irreducible, c is a unit or c is p times some unit. If the second was the case, then $(c) = (p)$ which would imply $p \mid a$, a contradiction. Therefore, c is a unit, so $(c) = (1)$.

Therefore, $\exists x, y \in R$ such that $1 = xp + ya$. Multiplying both sides by b, we see that $b = bxp + yab$. $p \mid ab$, so $p \mid b$.

Now we know that the irreducibles in a PID are prime. $x = ur_1 \cdots r_n = u'y_1 \cdots y_m$. r_1 is prime implies $r_1 \mid y_i$ for some i. Say $r_1 \mid y_1$, so $y_1 = wr_1$. Then $ur_2 \cdots r_n = u'wy_2 \cdots y_m$. □

Lecture 10: Localization

Wednesday, September 23, 2020

0.9 Localization

R commutative, $D \subset R$ multiplicative subset (i.e. D is closed under multiplication and D has no 0 or zero-divisors). Informally, RD^{-1} or $R[D^{-1}]$ consists of "fractions" $\frac{a}{d}$ for $a \in R$, $d \in D$.

Formally, elements of $R[D^{-1}]$ are equivalence classes of pairs $(a, d),\ a \in R,\ d \in D$ under equivalence relation $(a, b) \sim (c, d)$ iff $ad - bc = 0$.

Notation

$\frac{a}{b}$ for equivalence class (a, b).

$$\frac{a}{b} + \frac{c}{d} \equiv \frac{ad + cb}{bd}$$

The ring $R[D^{-1}]$ is commutative with 1.

0.9.1 Universal Property

$$R \xrightarrow{i} R[D^{-1}]$$

If we have a map $R \xrightarrow{\varphi} S$ where $\varphi(d)$ is a unit for every $d \in D$, then $\exists R[D^{-1}] \xrightarrow{\psi} S$ such that $\psi = \varphi \circ i$.

Claim. Given R, D there is a unique ring satisfying this universal property.

Proof. Suppose there was some ring S which also had this property. We could then define a map $R[D^{-1}] \xrightarrow{a} S$ by that universal property, and a map $S \xrightarrow{b} R[D^{-1}]$ by the other universal property.

Clearly, $b \circ a \colon R[D^{-1}] \xrightarrow{c} R[D^{-1}]$, so $R[D^{-1}]$ is isomorphic to S. □

Example. Some examples of localization:

- $\mathbb{Z} \to \mathbb{Q}$
- $R = F[X]$, $D = R - \{0\}$, $F[X][D^{-1}]$ is the ring of rational functions denoted $F(X)$.

$$\frac{1}{x + x^2} \in F(x),\ F = \mathbb{Z}/2\mathbb{Z}$$

- R is an integral domain, $D = R - \{0\}$, $R[D^{-1}]$ is a field called the field of fractions.
- Suppose we have a prime ideal $P \subset R$ and let $D = R - P$. Recall that $a, b \in D \implies ab \in D$. If $ab \notin D$ then $ab \in P$ iff $a \in P$ or $b \in P$.

  Notation

  The ring $R[(R - P)^{-1}]$ is denoted by R_P.

  Properties:

  – R_P has a unique maximal ideal which is PR_P.

  Proof. PR_P consists of elements $\frac{a}{b}$ where $a \in P$ and $b \notin P$. Suppose $I \subsetneq PR_P$ ideal. Then $\exists \frac{a}{b} \in I - PR_P$ where $a, b \notin P$. Therefore, $\frac{b}{a} \in R_P \implies 1 = \frac{a}{b}\frac{b}{a} \in I$ so $I = R_P$. □

◇

Why do we call this localization? Take a compact metric space M (like $\{0,1\}^d$ or any compact subset of Euclidean space). Lets look at $R(M)$ as the set of continuous functions on M. R is a ring (adding and multiplying functions gives another function, inverses don't necessarily work so it isn't a field).

Say we have $S \subset M$ as a closed subset of M. How do the functions on this subset relate to functions on the whole space? Tietze extension theorem says that every $f\colon S \to \mathbb{R}$ extends to $\tilde{f}\colon M \to \mathbb{R}$, i.e. $\tilde{f}/S = f$.

Take $f, g \in R(M)$. These are equal on S if $f - g$ vanishes on S. This is equivalent to saying that $f - g \in I = \{h \in R(M),\ h\big|_S = 0\}$. I is an ideal in R which we will denote $I(S)$.

This means that $\frac{R(M)}{I(S)} \cong R(S)$. The quotient by ideal is equivalent to the ring on the smaller space.

Let's look at an ideal of a point $x \in M$:

Claim. $I(\{x\})$ is a maximal ideal.

Proof. $I(\{x\}) = \ker(f \in R \overset{\pi}{\mapsto} \{x\})$. By the first isomorphism theorem, $\frac{R}{I(\{x\})} \cong \mathrm{Im}(\pi) = R$, therefore $I(\{x\})$ is maximal. □

Claim. Every maximal ideal is of the form $I(\{x\})$.

Proof. Suppose I is ideal not contained in any $I(\{x\})$:

$\forall x \in M$, $\exists f_x \in I$ such that $f_x(x) \neq 0$. Since f_x is continuous, $\exists$open $U_x \ni x$ such that $f_x\big|_{U_x} \neq 0$.

If we look at the set of all such $\{U_x\}_{x \in M}$, M is compact so there is some finite subcover $U_{x_1} \cup \cdots \cup U_{x_n} = M$. $f = f_{x_1}^2 + f_{x_2}^2 + \cdots f_{x_n}^2$ is everywhere positive. $f^{-1} \in R(M)$, so $1 = f \cdot f^{-1} \in I$ so $I = R(M)$. □

On the space $M \to R(M)$, the points $x \in M$ correspond to the maximal ideals. In the next lecture, we will see that this works for spaces which don't necessarily have a metric, and there will be a similar correspondence with neighborhoods of points.

Lecture 11:
Friday, September 25, 2020

In the last lecture, we were talking about rings of functions on a compact metric space. We showed that maximal ideals correspond to points in that space. We did this with continuous functions, but this also works fine with differentiable functions, twice-differentiable functions, etc.

Polynomials are a common class of functions. Let's take a field F (think $\mathbb{R}$ or $\mathbb{C}$). Polynomials on a field are represented $F[x]$. We know that this is a principal ideal domain, so primes are irreducibles of the form f where f is an irreducible polynomial.

Theorem 0.9.1 (Fundamental Theorem of Algebra (Analysis?))**.** *In $\mathbb{C}$, every polynomial factors into a product of linear factors. Equivalently, every $f \in \mathbb{C}[x]$ has a root.*

Definition 0.9.1. A field F such that every non-constant polynomial in $F[x]$ has a root is called *algebraically closed.*

If F is algebraically closed, then prime ideals in $F[x]$ are $(x - a)$, $a \in F$. They are also maximal.

Let's localize such a field. Take $\mathbb{C}[x]_{(x-a)} = \{\frac{f}{g}\colon g \neq 0\}$ where the only maximal ideal is $(x-a)\mathbb{C}[x]_{(x-a)}$.

Example. Take $\mathbb{C}[x, y]$. $P = (x)$ is a prime ideal. $fg \in (x) \implies f \in (x)$ or $g \in (x)$, and $fg \in (x) \iff fg = xh \exists h \iff fg\big|_{x=0} = 0$. (x) is prime but not maximal, since $(x) \subseteq (x, y)$.

Maximal ideals of $F[x, y]$ for algebraically closed F are $(x-a, y-b)$ $a, b \in F$, which are $\{f\colon f\big|_{(a,b)} = 0\}$. ◇

Recall F is a field $\implies$ $F[x]$ is a UFD (unique factorization domain).

Theorem 0.9.2. *If R is a UFD, then $R[x]$ is a UFD.*

Proof. To prove this, we need to define something called the content of a function:

Definition 0.9.2. For $f \in R[x]$ with R UFD, let $\text{content}(f) \equiv \gcd(a_0, \cdots, a_n)$ where $f = a_0x^a + \cdots + a_nx^n$.

Lemma 0.9.3 (Gauss's Lemma)**.**

$$\textit{content}(fg) = \textit{content}(f) \cdot \textit{content}(g)$$

Proof. If $\text{content}(f) \neq 1$, then consider $f' = \frac{f}{\text{content}(f)} \in R[x]$. This is still in the ring because every coefficient is divisible by the content. $g' = \frac{g}{\text{content}(g)}$. It is now enough to show the content is multiplicative for f' and g'. Without loss of generality, $\text{content}(f) = \text{content}(g) = 1$. Now we want to show that this is equal to the content of the product.

Suppose p is irreducible in R and p divides $\text{content}(fg)$. Since p does not divide $\text{content}(f)$, let s be the smallest index such that p does not divide a_s (this exists). Similarly, p does not divide $\text{content}(g)$, so we can look at the smallest t such that p does not divide b_t (the coefficients of f and g are a_n and b_n respectively).

Now consider the coefficient of x^{s+t} in fg. It is

$$\sum_{i+j=s+t} a_ib_j = a_sb_t + \sum_{i+j=s+t,\ (i,j)\neq(s,t)} a_ib_j$$

This final term is divisible by p but the left side is also divisible by p, and this is a contradiction. □

Consider R is a UFD and F is a field of fractions (for example $R = \mathbb{Z}$, $F = \mathbb{Q}$). $f \in F[x]$, $f = \frac{f'}{d}$, $f' \in R[x]$, $d \in R$.

$$\text{content}(f) \equiv \frac{\text{content}(f')}{d}.$$

Gauss's lemma holds for this content:

$$\text{content}\left(\frac{f'}{c} \cdot \frac{g'}{d}\right) = \frac{\text{content}(f'g')}{cd}$$

A quick observation: $f \in F[x]$ and $\text{content}(f) \in R$ iff $f \in R[x]$.

Theorem 0.9.4. *If $f \in R[x]$ is irreducible in $R[x]$, then f is irreducible in $F[x]$.*

Proof. $f = gh$ where $g, h \in F[x]$. $\text{content}(f) = \text{content}(g) \cdot \text{content}(h) = \frac{a}{b}\frac{c}{d}$. This means b divides c and d divides a. We can consider a polynomial $f' = \frac{fb}{c}$ and $g' = \frac{gd}{b}$. $f', g' \in R[x]$. □

□

Lecture 12:
Monday, September 28, 2020

Proof. Proof continued from last lecture:

Lemma 0.9.5. *If R is a UFD and F is its field of functions, then $f \in R[x]$ is irreducible in $R[x]$ iff it is irreducible in $F[x]$.*

Proof. Without loss of generality, let content$(f) = 1$, $f = ab$ in $F[x]$. Define $a' = \frac{a}{\text{content}(a)}$ and $b' = \frac{b}{\text{content}(b)}$, so $f = a'b' \in R[x]$. □

Finally, we can prove the theorem. If $f \in R[x]$. By definition, $f = \text{content}(f)f'$ for some f'. We can factor content(f) in R.

Without loss of generality, suppose content$(f) = 1$. Then we can factor f inside $F[x]$ as $f = a_1 a_2 \cdots a_n$, where a_i are irreducible in $F[x]$.

Define $a_i' = \frac{a_i}{\text{content}(a_i)} \in R[x]$, since we have a mapping $\pi\text{content}(a_i) = \text{content}(f) = 1$. Therefore, $f = a_1' a_2' \dots a_n'$, and by the most recent lemma, a_i' are irreducible in $R[x]$. The proof of uniqueness is similar. □

0.9.2 Irreducibility Criteria

1. $x - a \mid f(x)$, $f \in F[x] \iff f(a) = 0$

2. If R is an integral domain, $f \in R[x]$, and $P \subset R$ is a proper prime ideal, then let $\bar{f}$ denote its image in $(R/P)[x]$. If $\bar{f}$ cannot be factored into polynomials of degree smaller than deg$f$, then f is irreducible in $R[x]$. (Proof: $f = ab \implies \bar{f} = \bar{a}\bar{b}$)

3. Eisensteins Criterion:
$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
Prime ideal P with $\forall i,\ a_i \in P$ and $a_0 \notin P^2$, then f is irreducible.

   Proof. $(R/P)[x]$, $f = bc$, $b = \sum_{i=0}^{s} b_i x^i$ and $c = \sum_{i=0}^{t} c_i x^i$. Note we cannot have $b_0, c_0 \in P$ because that would imply $a_0 = b_0 c_0 \in P^2$.

   Say $c_0 \notin P$. Let i be the least such that $b_i \notin P$. Then $a_i \in P = b_i c_0 + b_{i-1}c_1 + b_0 c_i$, where the last two terms are in P but the first is not. □

4. $F[x_1, \cdots, x_n = F[x]$. As notation, for $\alpha \in \mathbb{Z}^n_{\geq 0}$, write $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.
   We can write $f = \sum_{\alpha \in S} C_\alpha x^\alpha$.

   Definition 0.9.3. The *Newton polytope* for f is the set conv(S) which is the convex hull of S denoted by $N(f)$.

   Claim.
$$N(fg) = N(f) + N(g)$$

0.10 Noetherian Rings

Definition 0.10.1. A ring R is called *Noetherian* if R is commutative with 1 and every ideal is finitely generated (this is a generalized PID).

Theorem 0.10.1. *If R is Noetherian, then so is $R[x]$.*

Corollary 0.10.1.1. *If F is a field, then $F[x_1, \cdots, x_n]$ is Noetherian.*

0.10.1 Systems of Polynomial Equations over Fields

Take a field $F[X] = F[x_1, \cdots, x_n]$. We can look at a system of equations $f_1(X) = f_2(X) = \cdots = f_n(X) = 0$. A consequence of this system is that for some a_i, $a_1 f_1 + a_2 f_2 + \cdots + a_m f_m = 0$.

The set $\{a_1 f_1 + \cdots + a_m f_m : a_i \in F[x]\}$ is the ideal generated by the polynomials: $(f_1, \cdots, f_m)$. Therefore, we can think of a system of equations as an ideal.

If we have an infinite system of equations, we can do the same thing: $f_1 = f_2 = \cdots = 0$ can be defined as the ideal $(f_1, \cdots)$, but the consequence of Noetherian rings is that this can be written as some finitely generated set $(g_1, \cdots, g_t)$.

Warning

$x^2 - y = y = 0$. The ideal $(x^2 - y, y) = (x^2, y) \not\ni x$

Definition 0.10.2. The *radical* of an ideal is $\operatorname{rad}(I) = \{f : \exists m,\ f^m \in I\}$.

LECTURE 13:
Wednesday, September 30, 2020

Exam

Mid-semester Test: October 22-25 (take home, four hours of your choice)

Recall in the last lecture we were proving the following theorem:

Theorem 0.10.2 (Hilbert's Basis Theorem)**.** *If R is a Noetherean ring, then $R[x]$ is.*

Proof. Let I be ideal in $R[x]$. Consider $L = \{\mathrm{LC}(f) : f \in I\}$, the set of leading coefficients of polynomials in I.

Claim. L is an ideal in R.

Proof. We need to show that it is closed under addition and multiplication and also under multiplication with elements of R.

Say $a \in L$ and $b \in R$. We need to show that $ab \in L$, and a is the leading coefficient of some $f \in R[x]$. By definition, $ab = \mathrm{LC}(bf)$.

$a' = \mathrm{LC}(f')$, so $a + a' = \mathrm{LC}\left(x^{\deg f'} f + x^{\deg f} f'\right)$ if $a + a' \neq 0$. Otherwise, $a + a' = \mathrm{LC}(0)$.

Since R is Noetherean, L admits a finite set of generators, say

$$L = (a_1, a_2, \cdots, a_n)$$

Let $f_i \in I$ such that $a_i = \mathrm{LC}(f_i)$. Let $D = \max(\deg(f_i))$. For each $d \leq D$, let $L_d = \{\mathrm{LC}(f) : f \in I,\ \deg(f) = d\} \cup \{0\}$ (the zero being added to make it an ideal). L_d is an ideal, and the proof is similar (in fact, they have the same degree, so the step to prove $a + a'$ is in the set is much simpler). Because L_d is ideal, $L_d = (S_d)$ where S_d is finite. Say $S_d = \mathrm{LC}(F_d)$ where $F_d \subset I$ and finite.

Claim. $F = F_0 \cup F_1 \cup \cdots \cup F_D \cup \{f_1, \cdots, f_n\}$ generates I.

Proof. Suppose $f \in I$ which is not in (F) and assume f is the minimal degree among such polynomials.

Case 1: $\deg f > D$

In this case, $\mathrm{LC}(f) \in L$, so $\mathrm{LC}(f) \in (a_1, \cdots, a_n)$, say $\mathrm{LC}(f) = b_1 a_1 + \cdots b_n a_n$.

Consider $f' = f - b_1 f_1 x^{\deg f - \deg f_1} + b_2 f_2 x^{\deg f - \deg f_2} + \cdots \in I$. This is constructed to eliminate the leading term of f, so $\deg(f') < \deg(f)$. By minimality, $f' \in (F)$. Therefore, $f = f' +$ some linear combination of $f_1, \cdots, f_n \in (F)$. This is a contradiction.

Case 2: Let $\deg f \leq D$ and $d = \deg f$. Consider $\mathrm{LC}(f) \in L_d$.

$\mathrm{LC}(f) \in (S_d)$ so $\mathrm{LC}(f) = \sum b_i \mathrm{LC}(g_i)$ where $g_i \in F_d$. Consider $f' = f - \sum b_i g_i$, where $\deg f' < \deg f$, so we find a similar contradiction to Case 1.

□

□

□

Consider $F[x_1, \cdots, x_n] = F[x]$, where F is a field.

Definition 0.10.3. *Monomials* are things of the form x^α. This is in contrast to a *monomial term* $c_\alpha x^\alpha$, where c_α is called the *coefficient*

Definition 0.10.4. A linear ordering on monomials is a *monomial ordering* if it is a well-ordering such that $x^\alpha < x^\beta \implies x^{\alpha+\gamma} < x^{\beta+\gamma}$.

Example. Lexicographic ordering (lex-ordering): $x^\alpha < x^\beta$ if $\alpha_1 = \beta_1, \cdots, \alpha_i = \beta_i$ and $\alpha_{i+1} < \beta_{i+1}$. Basically, this is an ordering based on the first non-equal exponent. ◇

Example. Graded Lexicographic ordering (grlex): $x^\alpha < x^\beta$ if $\deg(x^\alpha) < \deg(x^\beta)$. If $\deg(x^\alpha) = \deg(x^\beta)$, then use lexicographic ordering. ◇

For a polynomial $f = \sum c_\alpha x^\alpha$, the leading term of f, $\mathrm{LT}(f)$, is the largest term in the monomial ordering. $\mathrm{LC}(f)$ is the coefficient of $\mathrm{LT}(f)$, and $\mathrm{LM}(f)$ is the monomial in $\mathrm{LT}(f)$.

0.10.2 Division Algorithm

Input: polynomial f and polynomials $g_1, \cdots, g_n$.

Outputs: $a_1, \cdots, a_m$ and m such that $f = a_1 g_1 + \cdots + a_m g_m + m$ and $\deg(a_i g_i) \leq \deg(f)$ and no term of r is divisible by $\mathrm{LT}(g_i)$.

Algorithm:

1. Start with $r = 0$ and $a_i = 0$. At each step, do:
2. Pick g_i such that $\mathrm{LT}(g_i)$ divides $\mathrm{LT}(f)$. $a_i \to a_i + \frac{\mathrm{LT}(f)}{\mathrm{LT}(g_i)}$ and $f \to f - g_i \frac{\mathrm{LT}(f)}{\mathrm{LT}(g_i)}$.
3. If no such g_i exists, then $r \to r + \mathrm{LT}(f)$ and $f \to f - \mathrm{LT}(f)$ (move it into the remainder).
4. Stop when $f = 0$.

Note that $\max \deg(f)$ decreases at every step.

LECTURE 14:
Friday, October 02, 2020

In the last lecture, we discussed a division algorithm which takes a polynomial $f \in F[X]$ in several variables and a finite set of polynomials $G \subset F[X]$ and outputs a way of writing f as $f = f' + r$ where f' is an $F[X]$-linear combination of polynomials in G (where the degree of every summand is no greater than the degree of f) and r is the remainder term: no term of r is divisible by any $LT(g)$ for $g \in G$.

Example. $G = \{x^2, x^2 - y\}$. $I = (G) = (x^2, y)$. ◇

Definition 0.10.5. G is a *Gröbner basis* for the ideal $I = (G)$ if $\mathrm{LT}(I) = (\mathrm{LT}(g) \colon g \in G)$.

Example. $G = \{x^2, x^2 - y\}$. It's clear that $\mathrm{LT}(I) = (x^2, y)$. On the other hand, the leading term of $x^2 - y$ is $\mathrm{LT}(x^2 - y) = x^2$ and $\mathrm{LT}(x^2) = x^2$. Therefore, this is not a Gröbner basis. ◇

Notation

The remainder r in the division algorithm is denoted $f \mod G$.

Claim. If $I = (x^\alpha \colon \alpha \in S)$ is a monomial ideal (ideal generated by monomials), then this ideal consists of polynomials f, each of whose terms is divisible by some x^α, $\alpha \in S$.

Proof. $f \in I$—we want to show that f is of this form. We will do this by induction on the number of terms in f. The zero step is trivial.

$$f = \sum c_\alpha x^\alpha$$

$\mathrm{LM}(f)$ is contained in some $c_\alpha x^\alpha$, yet the term in c_α^α is divisible by x^α. □

Claim. If $I = (G)$ and G is Gröbner, if $f \equiv f' (\mod I)$, then $f \mod G = f' \mod G$.

Proof. Let $r = f \mod G$ and $r' = f' \mod G$. Therefore $r - r' \equiv f - f' (\mod I)$.

Let's write $f = f_I + r$ and $f' = f'_I + r'$. We can then say that $r - r' = (f - f_I) - (f' - f'_I) \in I$.

$\mathrm{LT}(r - r') \in \mathrm{LT}(I)$. By definition of the Gröbner basis, $\mathrm{LT}(I) = (\mathrm{LT}(G))$. We just proved in the last proposition that $\mathrm{LT}(r - r')$ is therefore divisible by some $\mathrm{LT}(g)$ for some $g \in G$.

$\mathrm{LM}(r - r')$ is a monomial in either r or r'. Say it's r. This contradicts the guarantee made on the remainder by the division algorithm. The only way $\mathrm{LM}(r - r') = 0$ is if $r - r' = 0$. □

Corollary 0.10.2.1. *If $f \in (G)$ and G is Gröbner, then $f \mod G = 0$.*

Next, we want to talk about how to tell if something is a Gröbner basis and how we can make Gröbner bases out of things that aren't.

Definition 0.10.6. For polynomials $f, f' \in F[X]$, the S-polynomial (S for "syzygy") of f, f' is defined as

$$S(f, f') = \frac{M}{\mathrm{LT}(f)} f - \frac{M}{\mathrm{LT}(f')} f'$$

where $M = \mathrm{lcm}(\mathrm{LT}(f), \mathrm{LT}(f'))$.

Theorem 0.10.3 (Buchberger's Criterion)**.** *G is Gröbner iff $S(g, g') \mod G = 0$ $\forall g, g' \in G$.*

Lemma 0.10.4. *$f_1, \cdots, f_m \in F[X]$. $LM(f_i) = x^\alpha \leftrightarrow \partial(f_i) = \alpha$ and $\partial(a_1 f_1 + \cdots + a_m f_m) < \alpha$, $a_i \in F$, then*

$$a_1 f_1 + \cdots + a_m f_m = b_1 S(f_1, s_2) + b_2 S(f_2, f_3) + \cdots + b_{m-1} S(f_{m-1} f_m)$$

(note that ∂ here is shorthand for "degree")

Proof. $f_i = c_i f_i'$ where $c_i = \mathrm{LC}(f_i)$. $f = a_1c_1(f_1' - f_2') + (a_1c_1 + a_2c_2)(f_2' - f_3') + \cdots + (a_1c_1 + \cdots + a_mc_m)f_m'$. There are no more terms left to cancel the last term, but recall the $\mathrm{LM}(f) < \mathrm{LM}(f_m')$. We also know that $\mathrm{LM}(\underbrace{f_{i+1}' - f_i'}_{S(f_{i+1}, f_i)}) < \mathrm{LM}(f_m')$.

Comparing the leading coefficient of $\mathrm{LM}(f_m')$, we conclude that $a_1c_1 + \cdots + a_mc_m = 0$. □

Lecture 15:
Monday, October 05, 2020

Recall the Buchberger criterion, which says that G is Gröbner iff $S(g, g') \mod G = 0$, $\forall g, g' \in G$.

How does $S(x^{alpha}f, f')$ relate to $S(f, f')$? Clearly $\mathrm{LT}(x^\alpha f) = x^\alpha \mathrm{LT}(f)$. The new M will be $x^\beta M$ for some $x^\beta \mid x^\alpha$, so $S(x^\alpha f, f') = x^\beta(f, f')$.

Given $f \in (G)$, we want to show that $\mathrm{LT}(f) in (\mathrm{LT}(G))$. The S polynomials are the only ways to get cancellations between elements of the basis.

If we write $f = \sum h_i g_i$ where $h_i \in F[X]$, suppose $x^\alpha = \max(\mathrm{LM}(h_i g_i))$. Then

$$\begin{aligned} f = \sum_{\mathrm{LM}(h_i g_i)} &= x^\alpha h_i g_i + \sum_{\mathrm{LM}(h_i g_i) < x^\alpha} h_i g_i \\ &= \underbrace{\sum_{\mathrm{LM}(h_i g_i) = x^\alpha} \mathrm{LT}(h_i) g_i}_{\sum_1} + \underbrace{\sum_{\mathrm{LM}(h_i g_i) = x^\alpha} (h_i - \mathrm{LT}(h_i)) g_i}_{\sum_2} + \underbrace{\sum_{\mathrm{LM}(h_i g_i) < x^\alpha} h_i g_i}_{\sum_3} \end{aligned}$$

Suppose $\mathrm{LM}(f) < x^\alpha$. All polynomials in that first term have the same degree. Let's write $\mathrm{LT}(h_i) = \mathrm{LC}(h_i)\mathrm{LM}(h_i)$ and define $h_i' = \mathrm{LM}(h_i)$. By our lemma, the first sum can be written as

$$\sum_1 = \sum_i b_i S(h_i' g_i, h_{i+1}' g_{i+1})$$

since $S(h_i' g_i, h_{i+1}' g_{i+1})$ is a monomial multiple of $S(g_i, g_{i+1})$. We know that $S(g_i, g_{i+1}) \mod G = 0$, so it must be a linear combination of the form $\sum_{g_j \in G} q_j g_j$ and $\mathrm{LM}(q_j g_j) \le \mathrm{LM}(g_i, g_{i+1})$.

This means that $s = S(h_i' g_i, h_{i+1}' g_{i+1})$ are sums of the form $\sum q_j' g_j$ where $\mathrm{LM}(s) \le \mathrm{LM}(q_j g_j)$.

So suppose next that $\mathrm{LM}(f) \ge x^\alpha$. Since $f = \sum h_i g_i$, $\mathrm{LT}(f) = \sum_{\mathrm{LM}(h_i g_i) = x^\alpha} \mathrm{LT}(h_i g_i) = \sum \mathrm{LT}(h_i)\mathrm{LT}(g_i)$. This concludes the proof.

Now we have a practical way of determining if something is a Gröbner basis. Next, we want to find a way to generate one.

Input: some set G_0. Output: a set G such that $(G) = (G_0)$ and G is Gröbner.

If G_i is Gröbner, we are done. Else, $S(g, g') \mod G_i \neq 0$ for some $g, g' \in G_i$. Note that $g, g' \in (G_i) \implies S(g, g') \in (G_i)$ so $r \in (G_i)$. By the division algorithm, $\mathrm{LT}(r) \notin (\mathrm{LT}(G_i))$.

Define $G_{i+1} = G_i \cup \{r\}$. $(\mathrm{LT}(G_{i+1})) \supsetneq (\mathrm{LT}(G_i))$.
Claim. If R is Noetherian, then every sequence of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ stabilizes (i.e. $I_j = I_{j+1} = \cdots$ from some point on).

Proof. $I = \bigcup_{j=1}^\infty I_j$. Since it's Noetherian, $I = (g_1, \cdots, g_m)$. For each g_s, there is $I_{kj} \ni g_i$. $k = \max(k_1, \cdots, k_m) \implies I_k \ni g_1, \cdots, g_m$. Therefore, $I_k \supseteq I$ so $I_k = I$. □

This is enough to show that our algorithm will eventually end.

Suppose we have an ideal $I \subset F[x_1, \cdots, x_n]$. Look at $I_i = I \cap F[x_{i+1}, \cdots, x_n]$ is the ith elimination ideal.

Claim. With lex-ordering, if G is Gröbner for I, then $G_i = G \cap F[x_{i+1}, \cdots, x_n]$ is Gröbner for I_i.

Proof. Note $G_i \subset I_i$. We want to show that $(\mathrm{LT}(G_i)) = \mathrm{LT}(I_i)$. Say $f \in I_i$. Since G is Gröbner, $\mathrm{LT}(f) \in (\mathrm{LT}(G))$. By our lemma about monomial ideals, $\mathrm{LT}(f)$ is divisible by some $\mathrm{LT}(g)$ for $g \in G$.

Since $f \in I_i$, $\mathrm{LT}(f) \in F[x_{i+1}, \cdots, x_n]$, so $\mathrm{LT}(g) \in F[x_{i+1}, \cdots, x_n]$. By lex-ordering, all monomials in g are free of $x_1, \cdots x_i$, so $g \in I_i$. □

LECTURE 16: MODULES
Wednesday, October 07, 2020

0.11 Modules

Definition 0.11.1. Given a ring R which is not necessarily commutative (and not necessarily with 1), a left R-module is an abelian group M with an action of R on M. This is a map $R \times M \to M$. We will denote this map $(r, m) \mapsto \varphi(r, m)$ as $rm = \varphi(r, m)$.

$$r(m + m') = rm + rm'$$
$$(rr')m = r(r'm)$$
$$(r + r')m = rm + r'm$$

If $1 \in R$, then $1m = m$.

Example. If F is a field, F-module is the same as a vector space over F. ◇

Example. Take R to be any ring and $M = R$ with action being the ring multiplication. In this example, R-submodules of M are left ideals. ◇

Example. If $R = \mathbb{Z}$ then R-modules are abelian groups.

$$rm = \overbrace{1 + \cdots + 1}^{r} m = \overbrace{m + \cdots + m}^{r}.$$ ◇

Example. Let F be a field. Consider the ring of polynomials over F as $F[x]$-modules M. M is an F-module, since $F \subset F[x]$. Multiplication by x takes $m \mapsto xm$ and is a linear map— call it T. We now have a vector space V together with a linear map $T \colon V \to V$.

Say we have a polynomial $p(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$.

$$p(x)V \equiv (a_0 + a_1 T + \cdots + a_n T^n)V$$

An $F[x]$-submodule is a subspace invariant of V under T. ◇

Example. $F[x, g]$-modules would have two such linear maps, say T and S such that $TS = ST$. ◇

Example. Take a group G and field F. The group ring FG is $\{a_1 g + \cdots + a_n g_n \mid n \in \mathbb{Z}^+, a_i \in F\}$. The FG-module is given by an F-vector space together with linear maps $Tg \colon V \to V \ \forall g \in G$ such that $T_g T_{g'} = T_{gg'}$. ◇

0.11.1 Module morphisms

Module morphisms are maps $\varphi \colon M \to N$ (where M, N are left R-modules) such that

$$\varphi(r, m) = r\varphi(m)$$
$$\varphi(m + m') = \varphi(m) + \varphi(m')$$

$$M \times N = \{(m, n) \colon m \in M, n \in N\}$$

$r(m, n) = (rm, rn)$. Similarly, $\prod_{i \in I} M_i$ and $\bigoplus_{i \in I} M_i$ both operate as expected.

$$\mathrm{Hom}_R(M, N) = \{\text{homomorphisms from } M \to N\}$$

$\mathrm{Hom}_R(M, N)$ is an R-module:

$$\begin{aligned} \varphi, \psi &\in \mathrm{Hom}_R(M, N) \\ (\varphi + \psi)(m) &= \varphi(m) + \psi(m) \\ (r\varphi)(m) &= r(\varphi(m)) \end{aligned}$$

If A is a subset of an R-module M, $RA = \{r_1 a_1 + \cdots + r_n a_n \colon n \in \mathbb{Z}^+, a_i \in A, r_i \in R\}$.

0.12 Tensor Products

Digression on Universal Properties

Free groups on a set S of generators are defined as $F(S) = \{s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_m^{epxilon_m}\}$.
The universal property is satisfied as follows. If $\varphi \colon G \to S$ (for group G), then there exists a unique way to extend it as a mapping to the free group generated by S: $\exists! \Phi \colon G \to F(S)$ and conversely, any Φ gives a unique φ such that the diagram commutes.
Now take the free abelian group on S, $FA(S) = F(S)/\{x_1 x_2 x_1^{-1} x_2^{-1} \colon x_1, x_2 \in F(S)\} = F(S)/[F(S), F(S)]$. This satisfies a similar universal property.

Consider vector spaces V, W, U over F. The map $T \colon V \times W \to U$ is bilinear. $T(v, \cdot) \colon W \to U$ is linear $\forall V$ and $T(\cdot, w) \colon V \to U$ is linear $\forall w \in W$.

Lecture 17: Tensor Products
Friday, October 09, 2020

Definition 0.12.1. *Tensor products* are universal objects for bilinear maps. If we can define left R-modules rm and right R-modules mr, we can also define (R, S)-bimodules with the form rms.

In particular, we want to take a right R-module M and left R-module N and construct mrn through some map $\varphi \colon M \times N \to T$. Such a map is *$R$-balanced* if $\varphi(mr, n) = \varphi(m, rn)$ and is linear for each M and N.

Recall that if we have abelian groups A, B, and C and we look at maps $A/B \to C$, and these are the same as maps $\varphi \colon A \to C$ such that $\varphi(B) = 0$.

We can similarly construct R-balanced maps from $M \times N$ as maps from $M \otimes_R N$. Consider $\mathrm{FA}(M \times N)$, the free abelian group on $M \times N$. Let $B \subset A$ be generated $(mr, n) - (m, rn)$ and $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$ and so on. A is an abelian group, and we can define $M \otimes_R N \equiv A/B$.

If M is and (S, R)-bimodule, $M \otimes_R N$ is a left S-module. Similarly, if N is not a left R-module, it can be an (R, S)-bimodule.

Notation

The equivalence class of $(m, n) \in M \times N$ in $M \otimes_R N$ is denoted $m \otimes n$.

Example. $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} \cong 0$. Let's look at some element $a \otimes b$ (this is not the most general element, the general elements are linear combinations of such elements).

$$a \otimes b = 3a \otimes b = a \otimes 3b = a \otimes 0 = 0$$

since $x \otimes 0 = x \otimes 0 \cdot 0 = 0x \otimes 0 = 0 \otimes 0 = 0$. ◇

Example. $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$. T is generated by $1 \otimes 1$, since other products are trivial. Consider a bilinear map on $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$:

$$\varphi(a, b) = ab$$

$$1 \otimes 1 + 1 \otimes 1 = 2 \otimes 1 = 0 \otimes 1 = 0$$

◇

Example. In general, $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/\gcd(m, n)\mathbb{Z}$ ◇

Example. $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} \cong 0$:

$$\frac{a}{b} \otimes \frac{c}{d} = \frac{1}{d}\frac{a}{b} \otimes d\frac{c}{d} = \frac{a}{bd} \otimes c = \frac{a}{bd} \otimes 0 = 0$$

◇

Example. Say V, U are F-vector spaces. $U \otimes_F V$. Suppose $b_1, \cdots, b_n$ is a basis for U and $c_1, \cdots, c_n$ is a basis for V. Then the set $G = \{b_i \otimes c_j\}$ spans $U \otimes_F V$.

G is linearly independent. We want to show that $\sum a_{ij} b_i \otimes c_j = 0$, all a_{ij} must be 0. This is to say that for every bilinear $T\colon U \times V$, $\sum a_{ij} T(b_i, c_j) = 0$.

Define $T_{ij}\colon U \times V \to F$ by $T_{ij}(\sum_k \beta_k b_k, \sum_l \gamma_l c_l) \equiv \beta_i \gamma_j$. This map shows that $a_{ij} = 0$. ◇

Claim. $M \otimes_R (N \oplus N) cong (M \otimes_R N) \otimes (M \otimes_R N)$

Proof. $(m, (n, n')) \mapsto (m \otimes n, m \otimes n')$. The inverse mapping is defined as $(m \otimes n, m' \otimes n') \mapsto m \otimes (n, 0) + m' \otimes (0, n')$. □

Example. R is a subring of S. Think of S as an (S, R)-bimodule. Say M is a left R-module. Then $S \otimes_R M$ is a left S-module. ◇

Example. $S = \mathbb{C}$, $R = \mathbb{R}$. For a vector space V over $\mathbb{R}$, $V' = \mathbb{C} \otimes_{\mathbb{R}} V$ is a $\mathbb{C}$-vector space. If $v \in V$, then $1 \otimes v \in V'$. ◇

0.12.1 Tensors of Homomorphisms

$\varphi\colon M \to M'$ is a hom of right R-modules and $\psi\colon N \to N'$ is a hom of left R-modules. Define $\varphi \otimes \psi\colon M \otimes_R N \to M' \otimes_R N'$ by $(\varphi \otimes \psi)(m \otimes n) = \varphi(m) \otimes \psi(n)$.

If R is a field, the matrix of φ is $\begin{pmatrix} a_{11} & a_{12} & \cdots \\ a_{21} & \ddots & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$, and the matrix of ψ is A, matrix representations of $\varphi \otimes \psi$ are a block matrix $\begin{pmatrix} a_{11}A & a_{12}A & \cdots \\ a_{21}A & \ddots & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$.

LECTURE 18: TENSOR PRODUCTS, CONT.
Monday, October 12, 2020

Tensor products are *associative*. If we have three modules, M, N, and L which are right R-modules, (R,S)-bimodules, and left S-modules respectively, then

$$(M \otimes_R N) \otimes_S L \cong M \otimes_R (N \otimes_S L)$$

These are isomorphic because both the left and right-hand sides are in bijection with triply balanced maps $\varphi\colon M \times N \times L \to D$ such that φ is trilinear and $\varphi(mr, n, l) = \varphi(m, rn, l)$ and $\varphi(r, ns, l) = \varphi(r, n, sl)$.

Given such φ, we can define the map $(M \otimes_R N) \times L \to D$ by $(m \otimes n, l) \to \varphi(m, n, l)$. This map is bilinear. Linearity in the second coordinate follows from linearity of φ in the third coordinate. Linearity in the first coordinate follows from biliniarity of φ in the first and second coordinates.

Main Case: R commutative (R,R)-bimodule where left and right actions coincide. We then talk about trilinear maps where

$$\varphi(rm, n, l) = \varphi(m, rn, l) = \varphi(m, n, rl)$$

Write $M \otimes_R N \otimes_R L$.

Definition 0.12.2. For R commutative with 1, M is an R-algebra if M is a ring together with a map $\varphi\colon R \to Z(M)$. In other words, M is an (R,R)-bimodule (R-module) given by $rm = \varphi(r)m$.

Example. $\mathbb{R}$, $\mathbb{C}$, quaternions, etc. ◇

If A and B are R-algebras, then $A \otimes_R B$ is also an R-algebra under multiplication given by $(a \otimes b)(a' \otimes b') \mapsto aa' \otimes bb'$.

Think of $A \times B \times A \times B$ under the mapping $(a, b, a', b') \mapsto aa' \otimes bb'$. This is quadrilinear and introduces a map $(A \otimes_R B) \otimes_R (A \otimes_R B) \to A \otimes_R B$.

0.13 Tensor Algebras

Given an R-module V (when we say R-module you should really think "vector space"), we can look at the tensor product of V with itself:

$$V^{\otimes m} \equiv \underbrace{V \otimes V \otimes \cdots \otimes V}_{m}$$

If we now have some element $\alpha \in V^{\otimes i}$ and $\beta \in V^{\otimes j}$, then $\alpha \otimes \beta \in V^{\otimes i} \otimes V^{\otimes j}$.

Definition 0.13.1. $T(V) = \bigoplus_{m=0}^{\infty} V^{\otimes m}$ is a *tensor algebra*.

Given $\alpha, \beta \in T(V)$, their product in $T(V)$ is given by the tensor product. We can write any α as $\alpha = \alpha_0 \oplus \alpha_1 \oplus \cdots$ and $\beta = \beta_0 \oplus \beta_1 \oplus \cdots$ such that $\alpha\beta \equiv \alpha_0\beta_0 \oplus (\alpha_0 \otimes \beta_1 + \alpha_1 \otimes \beta_0) \oplus (\alpha_0 \otimes \beta_2 + \alpha_1 \otimes \beta_1 + \alpha_2 \otimes \beta_0) \oplus \cdots$.

Universal Property: For every R-module homomorphism $\varphi\colon V \to A$ there exists a unique R-algebra homomorphism $\Phi\colon T(M) \to A$ where A is an R-algebra such that $\Phi\big|_V = \varphi$.

$V^{\otimes i} \to A$ is given by $v_1 \otimes \cdots \otimes v_i \mapsto \varphi(v_1)\varphi(v_2)\cdots\varphi(v_i)$.

Definition 0.13.2. A bilinear map $T\colon V \times V \to D$. T is *symmetric* if $T(v, v') = T(v', v)$. There is an associated symmetric algebra $S(V) = T(V)/I(V)$ where $I(V)$ is an ideal generated by $(v \otimes v' - v' \otimes v\colon v, v' \in V)$.

Definition 0.13.3. A map $T\colon V \times V \to D$ is *alternating* if $T(v, v) = 0 \quad \forall v \in V$.

Definition 0.13.4. The *exterior algebra* is $\Lambda(V) = T(V)/A(V)$ where $A(V)$ is the ideal generated by $(v \otimes v \colon v \in V)$.

$A(V)$ contains, for example, $w \otimes v \otimes v \otimes u$ for some w and u.

In $\Lambda(V)$, $(a+b)\otimes(a+b)$ is 0. By distributivity, the is $a\otimes a + a\otimes b + b\otimes a + b\otimes b = a\otimes b + b\otimes a$ because of the $/A(V)$. Therefore, $a \otimes b = -b \otimes a$ in general, and we call this behavior *antisymmetric*. This is not entirely equivalent to being alternating. An alternating map is antisymmetric, but the converse is not necessarily true. Suppose $T(a,b) = -T(b,a) \quad \forall a, b$. This implies that $T(a,a) + T(a,a) = 0$. By bilinearity, this implies that $T(2a, a) = 0$. If R is a field such that $2 \neq 0$, then $T(a,a) = 0 \forall a$, so it is alternating. If this is not the case (say $R = \mathbb{Z}/2\mathbb{Z}$), then $(a,b) \mapsto ab$ is antisymmetric but not alternating $(1 \cdot 1 = 1 \neq 0)$.

We can also write the exterior algebra as a direct sum:

$$\Lambda(M) = R \oplus M \oplus \Lambda^2 M \oplus \cdots$$

where $\Lambda^k M = M^{\otimes k}/(A(M) \cap M^{\otimes k})$. This is an example of a graded algebra. Another example is

$$R[x] = R \oplus Rx \oplus Rx^2 \oplus \cdots$$

Lecture 19: Tensor Products, cont.

Wednesday, October 14, 2020

In the previous lecture, we discussed the exterior product

$$\Lambda(M) = R \oplus M \oplus \Lambda^2(M) \otimes \cdots$$

where $\Lambda^k(M)$ consist of k-tensors modulo all tensors: $v_1 \otimes v_2 \otimes \cdots \otimes v_k$ such that $v_i = v_j$ for some $i \pm j$. Equivalence of this definition to the one in our previous lecture can be shown by showing that every tensor of this form is in the ideal

$$A(M) = (v \otimes v \colon v \in V) \subseteq T(M)$$

The basic idea of the proof is that $v \otimes u = -u \otimes v \mod A(M)$, so $v_1 \otimes \cdots v_i \otimes v_{i+1} \otimes \cdots \otimes v_k \equiv -v_1 \otimes \cdots \otimes v_{i+1} \otimes v_i \otimes \cdots \otimes v_k$.

Say M is a finite-dimensional vector space over F with $\dim(M) = n$ and $\{v_1, \cdots, v_n\}$ is a basis for M.

$$\Lambda^{n+1}(M) = 0$$

because we can write all vectors in terms of our basis vectors. Suppose we have some $u_1 \otimes \cdots \otimes u_{n+1}$ with $u_i \in M$. Write each u_i in terms of the basis and expand using multilinearity. Each term must have a repeated basis vector, so they are congruent to $0 \mod A(M)$.

Notation

Equivalence classes under $A(M)$ (i.e. elements of $\Lambda^k(M)$) are written with $\wedge$ rather than $\otimes$:

$$v_1 \otimes v_2 \otimes \cdots \otimes v_k \mod A(M) = v_1 \wedge v_2 \wedge \cdots \wedge v_k$$

Similarly,

$$\Lambda^n(M) \neq 0$$

since the determinant is alternating.

Note $\Lambda^k(M)$ is spanned by $v_{i_1} \wedge \cdots \wedge v_{i_k}$ where $1 \leq i_1 < \cdots < i_k \leq n$. In particular, this is a set of $\binom{n}{k}$ elements, and so $\dim(\Lambda^k(M)) \leq \binom{n}{k}$. In fact, this set is linearly independent, so $\dim(\Lambda^k(M)) = \binom{n}{k}$.

Proof. First, for $I \subset \{1, 2, \cdots, n\}$, say $I = \{i_1 < i_2 < \cdots < i_n\}$ then $V_I = v_{i_1} \wedge \cdots \wedge v_{i_n}$.

Suppose $0 = \sum_{|I|=k} \alpha_I V_I$. Then $0 \wedge V_J = \sum_I \alpha_I V_I \wedge V_J$. Choose J of size $n - k$.

Then $0 = \alpha_I \cdot (-1)^? \cdot V_{\{1,2,\ldots,n\}}$ so $\alpha_I = 0$. □

Say we have a subspace $M' \subset M$ and $u_1, \cdots, u_t$ is a basis for M'. $u_1 \wedge \cdots \wedge u_t \in \Lambda^t(M)$.

$$u_1 \wedge (u_2 + \lambda u_1) \wedge \cdots \wedge u_t = u_1 \wedge u_2 \wedge \cdots \wedge u_t$$

The element $u_1 \wedge \cdots \wedge u_m$ up to some constant F^* is determined by M'. Therefore, we have a way to map k-dimensional subspaces into $\Lambda^k(M)/F^*$.

0.14 Modules over PIDs

Assume R is a PID.

Definition 0.14.1. Elements $v_1, v_2, \cdots, v_n \in M$ are *linearly dependent* if $\exists r_1, \cdots, r_n \in R$ such that $r_1 v_1 + \cdots + r_n v_n = 0$.

Definition 0.14.2. A set $B \subset M$ is a *basis* if B is linearly independent and generates M.

Definition 0.14.3. An R-module M is *free* if it has a basis.

Example. If p is a prime element in R, then $R/(p)$ is an R-module that is not free because $rv = 0$ $\forall v \in R/(p)$. ◇

Claim. A submodule of a free finitely-generated module over a PID is free.

Proof. Say M is a finitely-generated free module. $N \subset M$ is a submodule, and $\{v_1, \cdots, v_m\}$ is a basis for M. Define $N_r = N \cap (v_1, \cdots, v_r)$ and claim (for induction) that N_r is free. The case where $r = 0$ is trivial. For the induction step, define $I = \{a \in R \colon \exists x \in N,\ x = b_1 v_1 + \cdots + b_r v_r + a v_{r+1}\}$. I is an ideal. Since R is a PID, there exists an a_{r+1} such that $I = (a_{r+1})$. Let $w \in N$ such that $w = b_1 v_1 + \cdots + b_r b_r + a_{r+1} v_{r+1}$ for some $b_1, \cdots, b_r$. Then $N_{r+1} = N_r + (w)$. Note that $N_r \cap (w) = 0$. Indeed, the coefficient of v_{r+1} in aw is $a a_{r+1} =\neq 0$ (if $a \neq 0$ and $w \neq 0$). If $w = 0$, then $N_{r+1} = N_r$, else $N_{r+1} = N_r \oplus (w)$. □

Definition 0.14.4. The *rank* of a free module M is the number of elements in the basis.

Lecture 20: Modules over PIDs

Monday, October 19, 2020

Recall from Wednesday we showed that finitely generated submodules of a free module over a PID are free. We also remarked that if $M \subset N$ are finitely generated R-modules, the number of generates of M is at most the number of generators of N.

Definition 0.14.5. The *rank* of a free module M is the number of linearly independent generators generating M.

Claim. If M is a free R-module over an integral domain and $\text{rank}(M) = n$, then any $n + 1$ elements of M are linearly dependent.

Proof. Say $y_1, \cdots y_{n+1}$ are elements of M. Let F be the field of fractions of R. We can make M into a module over F:

We need to be able to multiply elements of F by elements of M. Elements of F are equivalence classes of the form $\frac{a}{b}$, $a, b \in R$, $b \neq 0$. We can define a module M' over F consisting of equivalence classes of expressions $\frac{m}{r}$ where $r \in R \setminus \{0\}$. Then we can define multiplication as $\frac{a}{b}\frac{m}{r} = \frac{am}{br}$ with $\frac{m}{r} \sim \frac{m'}{r'}$ if $r'm = rm'$. $M' = F \otimes_R M$.

M' is a vector space over F with $\dim F \leq n$, so there exists $\frac{a_1}{b_1}, \cdots, \frac{a_{n+1}}{b_{n+1}} \in F$ such that $\sum_{i=1}^{n+1} \frac{a_i}{b_i} y_i = 0$, which implies $\sum_{i=1}^{n+1} \frac{a_i B}{b_i} y_i = 0$ where $B = \prod_{i=1}^{n+1} b_i$. □

Definition 0.14.6. An element $m \in M$ is a *torsion* element if $\exists m$ such that $rm = 0$. Here, r is called the *order*.

Definition 0.14.7. A module M is called a *torsion module* if all its elements are torsion.

Definition 0.14.8. $e \in R$ is called an *exponent* of M if $rM = 0$.

Example. $\mathbb{Q}/\mathbb{Z}$ (note that this is not finitely generated). ◇

Definition 0.14.9. For module M, $M_{\text{tor}} = \{m \in M : m \text{ is torsion}\}$.

Claim. M/M_{tor} is a torsion-free module.

Proof. $m, m' \in M_{\text{tor}}$, so $rm = 0$ and $r'm' = 0$ implies $rr'(m+m') = 0$, so M_{tor} is closed under addition. Let $mM_{\text{tor}} \in M/M_{\text{tor}}$ and say $r(mM_{\text{tor}}) = M_{\text{tor}}$. Then $rm \in M_{\text{tor}}$ so $\exists r'$ such that $r'(rm) = 0$, so $(r'r)m = 0$ so $m \in M_{\text{tor}}$. □

Claim. If M is a finitely generated R-module where R is a PID, then $M = M_{\text{tor}} \oplus F$ where F is free.

Claim. Every finitely generated torsion R-module (R is PID) is of the form $R/(p_1^{e_1}) \oplus R/(p_2^{e_2}) \oplus \cdots$ where $p_1, p_2, \cdots, p_n$ are prime elements of R.

Example. For $\mathbb{Z}$-modules (abelian groups), every finitely generated abelian group is isomorphic to $\mathbb{Z}^r \oplus \mathbb{Z}/p_1^{e_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{e_2}\mathbb{Z} \oplus \cdots$. ◇

Lemma 0.14.1. *If M is torsion-free and finitely generated, then M is free.*

Proof. Let $g_1, \cdots, g_n$ be generators of M. Pick a finite maximal linearly independent subset $v_1, \cdots, v_m$. Each g_i is linearly dependent with $\{v_i, \cdots, v_m\}$, so $a_i g_i + b_1 v_1 + b_2 v_2 + \cdots + b_n v_n = 0$ for some $a_i, b_i \in R$. $a_i \neq 0$, since otherwise you would have linear dependence. So, $a_i g_i \in R\{v_i, \cdots, v_m\}$. Let $a = \prod_{i=1}^{n} a_i$. Then $ag_i \in R\{v_1, \cdots, v_n\}$, so $aM \subseteq R\{v_1, \cdots, v_m\}$ since $v_1, \cdots, v_m$ are linearly independent. Therefore, aM is a subset of a free module, hence it is free.

Now consider the map $\varphi : M \to aM$. The kernel of φ is trivial, so by the first isomorphism theorem, $M \cong aM$, and aM is free so M is free. □

Lemma 0.14.2. *If $f : M \to M'$ is surjective, M' is free, and $y_1', \cdots, y_n'$ is a basis for M', then $\exists y_1, \cdots, y_n \in M$ which are linearly independent and $f(y_i) = y_i'$.*

We can apply this to $M \to M/M_{\text{tor}}$.

Proof. Construct $y_1, \cdots, y_m$ by induction on m. Say $y_1, \cdots, y_m$ have been constructed such that they are linearly independent. Pick $y_{m+1} \in f^{-1}(y_{m+1}')$. $0 = a_1 y_1 + \cdots + a_m y_m + a_{m+1} y_{m+1}$. Apply f to both sides to get $0 = a_1 y_1' + \cdots + a_{m+1} y_{m+1}'$. We can conclude here that $a_i = 0$. □

Lecture 21: Modules over PIDs, cont.

Wednesday, October 21, 2020

Definition 0.14.10. An element $m \in M$ has *period* r if $rm = 0$.

Theorem 0.14.3. *If M is a module that is finitely generated over a PID, then $M = M_{tor} \oplus F$ where F is free.*

Lemma 0.14.4. *If F is free and there is a mapping $M \to F$, then the generators of F can be pulled back to generatos of a free submodule in M.*

Lemma 0.14.5. *If M_{tor} is torsion free, then M/M_{tor} is free.*

Proof. $\pi\colon M \to M/M_{\text{tor}}$. Let $\{\bar{y}_1, \cdots, \bar{y}_n\}$ be a basis for M/M_{tor}. Let $y_1, \cdots, y_n$ be pullbacks of $\bar{y}_1, \cdots, \bar{y}_n$.

Let $F = R\{y_1, \cdots, y_n\}$. The $\ker \pi = M_{\text{tor}}$. We claim that $M = F \otimes M_{\text{tor}}$. Indeed, $x \in M$, $\pi(x) = a_1\bar{y}_1 + \cdots + a_n\bar{y}_n$.

Then $x - (a_1y_1 + \cdots + a_ny_n) \in \ker \pi$ since applying π to both sides gives 0. Therefore, $x \in M \implies x - (a_1y_1 + \cdots + a_ny_n) \in M_{\text{tor}}$, so $M = F + M_{\text{tor}}$. On the other hand, $F \cap M_{\text{tor}} = 0$, so $M = F \oplus M_{\text{tor}}$. $\square$

A free finitely generated module is isomorphic to R^n.

Theorem 0.14.6. *A torsion module over PID R is isomorphic to $R/(p_1^{r_1}) \oplus R/(p_2^{r_2}) \oplus \cdots \oplus R/(p_m^{r_m})$ where p_i's are prime.*

Theorem 0.14.7. *The multiset of ideals $(p_1^{r_1}), (p_2^{r_2}), \cdots$ is unique.*

Definition 0.14.11. Let $M_r = \{m \in M\colon rm = 0\}$. Also, define $M(p) = \{m \in M\colon \exists i\ p^i m = 0\}$ for prime p.

Claim. If c is an exponent for M and $c = ab$ with $(a, b) = 1$ (coprime), then $M_c = M_a \oplus M_b$.

Proof. If a and b are coprime, then $1 = \alpha a + \beta b$. Therefore, for $m \in M_c$, $m = 1 \cdot m = (\alpha a + \beta b)m = \alpha am + \beta bm$. $\alpha am \in M_b$ since multiplying by b gives $\alpha abm = \alpha cm = 0$ since $m \in M_c$ so $mc = 0$. Respectively $\beta bm \in M_a$, and for $m \in M_a \cap M_b$, $1 \cdot m = 0 + 0 = 0 \implies m = 0$, so $M_c = M_a \otimes M_b$. $\square$

Claim. If M is torsion and finitely generated, $M = M(p_1) \oplus M(p_2) \oplus \cdots \oplus M(p_n)$.

Observe that if p is prime, M_p is a $R/(p)$-module. Indeed $m \in M_p$ implies $rm = 0$ if $r \in (p)$.

Definition 0.14.12. Elements $y_1, y_2, \cdots, y_m \in M$ are *independent* if $a_1y_1 + \cdots + a_my_m = 0 \implies a_1y_1 = a_2y_2 = \cdots = a_my_m = 0$.

Equivalently, $R\{y_1, \cdots, y_m\} = Ry_1 \oplus \cdots \oplus Ry_m$.

Lemma 0.14.8. *Let M be an R-module of exponent p^r, and let x be an element of period p^r. Consider $\bar{M} = M/(x)$ and $\bar{y}_1, \cdots, \bar{y}_m \in \bar{M}$ are independent. Then $\exists y_i \in \bar{y}_i$ (y_i is a representative of $\bar{y}_i$) such that the period of y_i is equal to the period of $\bar{y}_i$ and $x, y_1, \cdots, y_m$ are independent.*

Proof. $\bar{y} \in \bar{M}$ of period p^n. Pick $y \in \bar{y}$. Then $p^ny \in p^n\bar{y}$ so $p^ny = p^scx$ where p does not divide c.

$s \le r$ because exponent is p^r. The period of p^scx is p^{r-s}. Then the period of y is $p^n \cdot p^{r-s} = p^{n+r-s}$. $p^rM = 0$, so $n + r - s \le r \implies n \le s$.

Take $y' = y - p^{s-n}cx$. Then $y' \equiv y \mod (x)$, i.e. $y' \in \bar{y}$. $p^ny' = p^ny - p^scx = 0$, so the period of y' is p^n. Next, we want to show independence.

Suppose $ax + a_1y_1 + \cdots + a_my_m = 0$. Take both sides $\mod (x)$. We are left with $a_1\bar{y}_1 + \cdots + a_m\bar{y}_m = 0$. By independence, $a_i\bar{y}_i = 0 \forall i$. Therefore, the period of y_i is divisible by a_i, so $a_iy_i = 0$, so $ax = 0$. $\square$

LECTURE 22: OPTIONAL DAY
Monday, October 26, 2020

0.15 Zero-Error Communication

Suppose you want to send information from point A to point B. Unfortunately, the process of sending information is prone to errors. The typical way to ensure the message is received is through redundancy. Let's call Σ the set of possible messages to send. Which of these messages can be confused for each other on the receiving end? For example, say you're sending handwriting and the letters a and o look very similar. Let $G = \{\{x, y\} \subset \Sigma \colon x \quad \text{and} \quad y \quad \text{are confusable} \quad \}$. We can represent this as a graph where nodes of the graph are connected if they represent messages which can be confused for each other.

A *confusion-free* set is a subset of elements $I \subset \Sigma$ such that $x, y \in I$ implies $\{x, y\} \notin G$. Denote $\alpha(G) = \max_{\text{confusion-free } I} |I|$.

Suppose our set Σ has five elements $\Sigma = \mathbb{Z}/5\mathbb{Z}$ and $G = \{\{x, x+1\} \colon x \in \Sigma\}$. Naïvely, we can only send one bit at a time, because $\alpha(G) = 2$.

Claim. We can do slightly better than this. In this example, we can transmit one of the 5 messages in 2 uses.

Proof. If we the message we want to send, then a second message such that it is not confusable with the message you would send for the message confusable with the first, you can be sure the combination of messages is not confusable. For example, send $\{0, 0\}$, $\{1, 2\}$, $\{2, 4\}$, $\{3, 1\}$, or $\{4, 3\}$. □

Using this method, we can send $\frac{1}{2}\log_2 5$ or some of $\sqrt{5}$ messages per day. We can construct a more general method:

To each $x \in \Sigma$, associate a vector $v_x \in F^n$ for a field F such that if $\{x, y\} \notin G$, then $\langle v_x, v_y \rangle = 0$ and $\langle v_x, v_x \rangle \neq 0$.

Claim. $\alpha(G) \leq n$.

Proof. If $I = \{x_1, \cdots, x_m\}$ is confusion free, then $v_{x_1}, \cdots, v_{x_m}$ are linearly independent: $0 = \sum \alpha_i v_{x_i} \implies \sum \alpha_i \left\langle v_{x_i, v_{x_j}} \right\rangle = 0 \forall j$. □

More generally, $\alpha(G) \leq \dim \operatorname{span}\{v_x \colon x \in \Sigma\}$.

Given a pair (Σ, G) models a single use of the channel, to model using the channel twice, we call $\Sigma' = \Sigma \times \Sigma$. We then say that $\{(x, y), (x', y')\} \in G$ if ($\{x, x'\} \in G$ or $x = x'$) and ($\{y, y'\} \in G$ or $y = y'$).

Call the map $x \mapsto v_x$ a *representation*. Similarly, we could say that $\Sigma \to V$ where V is a vector space. Then there is a representation of (Σ', G') where $\Sigma' \to V \otimes V$ and $(x, y) \mapsto v_x \otimes v_y$. One representation of the tensor product is $v_x \otimes v_y = v_x v_y^T$, a matrix:

$$\langle v_x \otimes v_y, v_{x'} \otimes v_{y'} \rangle = \sum_{i,j} \langle v_x, b_i \rangle \langle v_y, b_j \rangle \langle v_{x'}, b_i \rangle \langle v_{y'}, b_j \rangle$$

where b_i are an orthonormal basis of V. We can split this into two sums:

$$\langle v_x \otimes v_y, v_{x'} \otimes v_{y'} \rangle = \left(\sum_i \langle v_x, b_i \rangle \langle v_{x'}, b_i \rangle \right) \left(\sum_j \langle v_y, b_j \rangle \langle v_{y'}, b_j \rangle \right) = \langle v_x, v_{x'} \rangle \langle v_y, v_{y'} \rangle$$

so $\dim \operatorname{span}\{v_x \otimes v_y\} \geq \alpha(G')$ and $\alpha(G') \leq (\dim \operatorname{span}\{v_x \colon x \in \Sigma\})^2$. Then we can rename G' to $G^{\otimes 2}$.

Define $G^{\otimes n}$ in this fashion on Σ^n, where $\{(x_1, \cdots, x_n), (y_1, \cdots, y_n)\} \notin G^{\otimes n}$ if $\exists i$ such that $\{x_i, y_i\} \notin G^{\otimes n}$ and $x_i \neq y_i$.

If we are working on a vector space $V = \mathbb{R}^3$, then the largest thing we can send is $\alpha(G^{\otimes n}) \leq 3^n$.

A *representation with a handle* consists of a representation $\varphi\colon \Sigma \to \mathbb{R}^n$ and a vector $h \in \mathbb{R}^n$ such that $\varphi(x)$ and h are all unit vectors. The quality of such a representation is the measure of how far off elements of this representation are from h. $q = \min \langle h, \varphi(x)\rangle$ for $x \in \Sigma$.

Claim. $\alpha(G) \leq 1/q^2(\varphi, h)$.

Claim. Given a representation with handle (φ, h), we can make a representation with handle for $G^{\otimes n}$ with quality $q(\varphi, h)^n$.

Then, $\alpha(G^{\otimes n}) \leq \left(\frac{1}{q^2(\varphi,h)}\right)^n$.

For the second claim, we can represent a vector $(x_1, \cdots, x_n) \mapsto v_{x_1} \otimes \cdots \otimes v_{x_n}$. If we use the handle $h \otimes \cdots \otimes h$, then the claim is true. For the first claim, if $\{x_1, \cdots, x_m\}$ is confusion-free, we can complete it to an orthonormal basis B, and $|h|^2 = \sum_{b\in B} \langle h, b\rangle^2 \geq \sum_{i=1}^m \langle h, v_{x_i}\rangle^2 \geq m \cdot q^2(\varphi, h)$.

Lecture 23: Modules over PIDs, cont.

Wednesday, October 28, 2020

From last class, we discussed R-modules where R is PID. We want to show that every finitely generated module decomposes as $F \oplus \bigoplus_{p\in R} M(p)$ where p is prime in R and $M(p) = \{m \in M\colon \exists t \quad p^t m = 0\}$.

M is a torsion finitely generated module. We also proved the lemma that for a torsion module M of exponent p^r, period$(x) = p^r$ and independent $\bar{y}_1, \cdots, \bar{y}_n$ in $\bar{M} = M/(x)$, then there exist representatives of $y_i \in M$ of $\bar{y}_i$ such that they have the same period and $x_i y_1, \cdots, y_n$ are independent.

Recall that period(z) means we are looking for all elements $\{r\colon rz = 0\}$. The key observation is that $M_p = \{m\colon pm = 0\}$ (note that $M(p)$ is a union of this for all powers of p) is a vector space over $R/(p)$ (a field).

Claim. Each $M(p)$ decomposes as a direct sum of modules isomorphic to $R/(p^t)$ for various t's.

Proof. First note that $M(p)$ is finitely generated. If you look at $M = \bigoplus_p M(p)$, then the projection map $M \to M(p)$ is surjective, so M is finitely generated will imply that $M(p)$ is finitely generated.

So $\dim_{R/(p)} M_p$ is finite. We will now induct on this. Suppose M is a module of exponent p^r. By induction, $\bar{M} = M/(x)$ where period$(x) = p^r$, if $\dim_{R/(p)} \bar{M}_p = n$, there are $\bar{y}_1, \cdots, \bar{y}_n \in \bar{M}_p$ which are linearly independent.

This means that $0 = a_1\bar{y}_1 + \cdots + a_n\bar{y}_n$ implies that $a_i + (p) = 0$ in $R/(p)$, so $\forall i$, $a_i\bar{y}_i = 0$. By the lemma, there are independent $x, y_1, \cdots, y_n$ in M, so $\dim_{R(p)} M_p > \dim_{R/(p)} \bar{M}_p$. Let's reindex y_i so that it starts with y_2.

Induction tells us that $\bar{M} = (\bar{y}_2) \oplus \cdots \oplus (\bar{y}_n)$ where period$(y_i) = p^{t_i}$. By the lemma, period$(x) = p^r =$ exponent(M) and periods$(\bar{y}_i) \leq$ period(x).

Claim. $M = (x) \oplus (y_2) \oplus \cdots \oplus (y_n)$.

Indeed, for $m \in M$, if we look at $\bar{m} \in \bar{M}$ where $\bar{m} = m + (x)$, $\exists a_i \in R$ with $\bar{m} = a_2\bar{y}_2 + \cdots + a_n\bar{y}_n$, so $m - a_2y_2 - \cdots - a_ny_n \in (x)$, and $m = a_1x + a_2y_2 + \cdots + a_ny_n$. □

Theorem 0.15.1. *Every finitely generated module over a PID R is isomorphic to*

$$R^n \oplus \bigoplus_p R/(p^{t_i})$$

where p is prime in R.

1. It suffices to prove uniqueness for torsion modules.
2. Similarly, $M(p)$ was determined by M, and so it suffices to deal with modules of exponent p^r.
3. $M = M/(p^{r_1}) \oplus M/(p^{r_2}) \oplus \cdots \oplus M/(p^{r_n})$, then M_p is of dimension n over $R/(p)$.

Let's define $\varphi\colon R \to bR \to bR/(p^t)$. Then $\ker(\varphi) = \{r \in R\colon br \in (p^t)\}$. By UDF, if p does not divide b, then $r \in (p^t)$. If $b = p$ then $r \in (p^{t-1})$.

By the first isomorphism theorem,

$$\frac{R}{(p^{t-1})} \cong p\frac{R}{(p^t)}$$

Then $pM \cong \frac{R}{p^{r_1-1}} \oplus \frac{R}{(p^{r_2-1})} \oplus \cdots \oplus \frac{R}{p^{r_n-1}}$.

LECTURE 24: MODULES OVER PIDS, CONT.
Friday, October 30, 2020

0.16 Decomposition Theorem for Finitely Generated Modules over a PID

Theorem 0.16.1 (Chinese Remainder Theorem)**.** *Take an integral domain R and ideals $I, J \subset R$ such that $I + J = R$. That is, they are comaxial/coprime.*

For example, if $I = (a)$ and $J = (b)$, then $I + J = R$ is equivalent to saying $I + J \ni 1$ and $\exists c, d$ such that $ca + db = 1$.

The theorem states that

$$\frac{R}{I} \oplus \frac{R}{J} \cong \frac{R}{IJ}$$

Proof. Take a map $\varphi\colon R \to R/I \oplus R/J$, so $r \mapsto r + I \oplus r + J$.

$\ker\varphi = I \cap J$. We claim that $I \cap J = IJ$. To prove this, $IJ \subset I \cap J$ by definition. Since $I + J \ni 1$, that means $\exists x \in I, y \in J$ such that $x + y = 1$. Let $z \in I \cap J$. Then $z = z \cdot 1_R = z(x + y) = zx + zy$. $zx \in JI$ and $zy \in IJ$ so $zx + zy = z \in IJ$.

Now by the first isomorphism theorem, $\frac{R}{\ker\varphi} = \frac{R}{IJ} \cong \varphi(R)$.

Finally, we claim φ is surjective. $\varphi(1) = 1+I\oplus 1+J$. On the other hand, $\varphi(1) = \varphi(x+y) = y+I\oplus x+J$ (since $x + I = I$). $\varphi(x) = 0 \oplus 1 + J$ and $\varphi(y) = 1 + I \oplus 0$. Say we have r_1 and r_2. Then $\varphi(r_2x + r_1y) = r_1 + I \oplus r_2 + J$, so φ is surjective. □

Corollary 0.16.1.1.

$$\frac{\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{\mathbb{Z}}{n\mathbb{Z}} \cong \frac{\mathbb{Z}}{mn\mathbb{Z}}$$

if $(m, n) = 1$ (they are coprime).

Similarly, we can demonstrate this as a ring isomorphism:

$$\frac{R}{(m)} \oplus \frac{R}{(n)} \cong \frac{R}{(mn)}$$

In fact, this is an R-module isomorphism.

In decomposition

$$\bigotimes_p \frac{R}{(p^r)}$$

call the prime exponents for each p r_{ij} such that the exponents of p_1 are $r_{11} \geq r_{12} \geq r_{13} \geq \cdots$. Then

$$\frac{R}{(p_1^{r_{11}})} \oplus \frac{R}{(p_2^{r_{21}})} \oplus \cdots \oplus \frac{R}{(p_l^{r_{l1}})} \cong \frac{R}{(p_1^{r_{11}} p_2^{r_{21}} \cdots p_l^{r_{l1}})}$$

We could then continue with the other exponents. Then we can always decompose such a module like

$$\frac{R}{(a_1)} \oplus \frac{R}{(a_2)} \oplus \cdots \oplus \frac{R}{(a_k)}$$

such that $a_1 | a_2 | a_3 | \cdots | a_k$ (divides).

0.17 Invariant Factor Form

1. Finitely generated $\mathbb{Z}$-modules (abelian groups) are decomposed as $\mathbb{Z}^n \oplus \frac{\mathbb{Z}}{a_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{a_k\mathbb{Z}}$.
2. $F[x]$-modules (vector spaces mod F with a mapping from the space to itself, $T\colon V \to V$). If $F[x]$-module is torsion-free, then $1, T, T^2, \cdots$ are linearly independent, so V is infinite-dimensional.

By the decomposition theorem, every torsion finitely generated $F[x]$-module is isomorphic to

$$\frac{F[x]}{(p_1(x))} \oplus \cdots \oplus \frac{F[x]}{(p_k(x))}$$

What is $F[x]/(p(x))$? $p(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$. Then $\dim_F \frac{F[x]}{(p(x))} = n$ due to the division algorithm (all the things divisible by each power of x). For a basis, we can use $1, x, x^2, \cdots, x^{n-1}$. Let $T\colon \frac{F[x]}{(p(x))} \to \frac{F[x]}{(p(x))}$, $f \mapsto xf$. T in this basis is given by

$$T = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 - a_0 \\ 1 & 0 & 0 & \cdots & 0 - a_1 \\ 0 & 1 & 0 & \cdots & 0 - a_2 \\ 0 & 0 & 1 & \cdots & 0 - a_3 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 - a_{n-1} \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

Hence, if V is a finite dimensional vector space over F and $T\colon V \to V$, we can decompose V as $V_1 \oplus_k$ such that on each V_i, there is a T_i like the T above and T can be written in a block-diagonal form comprised of these T_i called the rational canonical form.

This is unique by uniqueness of module factorization. Note that $T\colon \frac{F[x]}{(p)} \to \frac{F[x]}{(p)}$, $f \mapsto xf$ satisfies $p(T) = 0$, i.e. $0 = a_0 I + a_1 T + \cdots + a_{n-1}T^{n-1} + T^n$. Also, for no polynomial q of $\deg q < n$, $q(T) = 0$, since $q(T)f = q(x)f$ so $q(T)1 = q(x) \neq 0 \mod p(x)$.

So, if

$$\frac{F[x]}{(p_1)} \oplus \cdots \oplus \frac{F[x]}{(p_k)}$$

is the invariant factor decomposition $(p_1 | p_2 | \cdots | p_k)$, then the map T satisfies $p_k(T) = 0$. Furthermore, there is no polynomial of smaller degree with the same property. We call p_k a minimal polynomial. Note that $\deg p_k \leq \dim V$.

As an exercise, the characteristic of the companion matrix is the polynomial $p(x)$:

$$\det(Ix - T) = \det \begin{pmatrix} x & & & a_0 \\ -1 & x & & a_1 \\ & -1 & & \vdots \\ & & & \\ & & -1 & a_{n-1} + x \end{pmatrix}$$

Corollary 0.17.0.1 (Cayley-Hamilton)**.** *If q is the characteristic polynomial of T, then $q(T) = 0$.*

LECTURE 25: FIELDS
Monday, November 02, 2020

Wrapping up modules over PIDs.

Say F is algebraically closed. Then every torsion finitely generated $F[x]$-module can be written

$$\bigotimes_{\lambda} \frac{F[x]}{((x-\lambda)^{\lambda})}$$

In this, pick the basis $\{1, (x-\lambda), (x-\lambda)^2, \cdots, (x-\lambda)^{n-1}\}$. Multiplication by x gives $x(x-\lambda)^t = (x-\lambda)^{t+1} + \lambda(x-\lambda)^t$. Therefore, this operation takes a basis vector to the next basis vector plus λ times itself. The only exception will be the last basis vector: $x(x-\lambda)^{n-1} = \lambda(x-\lambda)^{n-1}$ (in $M = ((x-\lambda)^{\lambda})$).

In this basis, the matrix of T (multiplication by x) is

$$T = \begin{pmatrix} \lambda & & & & \\ 1 & \lambda & & & \\ & 1 & \lambda & & \\ & & \ddots & \ddots & \\ & & & 1 & \lambda \end{pmatrix}$$

This is called the *Jordan normal form*.

0.18 Categories

Definition 0.18.1. A *category* C consists of a class of objects $\mathrm{Ob}(C)$, and for each pair of objects $A, B \in \mathrm{Ob}(C)$, a set of morphisms $\mathrm{Hom}(A, B)$, and a rule to compose morphisms such that $\varphi \in \mathrm{Hom}(A, B)$ and $\psi \in \mathrm{Hom}(B, C)$, there exists a morphism $\psi \circ \varphi \in \mathrm{Hom}(A, C)$ such that $\circ$ is associative and there is an identity morphism.

Example. $\overline{\mathrm{Gp}}$ is the category of groups with maps being group homomorphisms.

$\overline{\mathrm{Rng}}$ is the category of rings with ring homomorphisms.

$\overline{\mathrm{CRng}}$ is the category of commutative rings.

$\overline{\mathrm{Set}}$ is the category of sets with functions.

$\overline{\mathrm{Top}}$ is the category of topological spaces.

$\overline{\mathrm{HTop}}$ is the category of topological spaces with homotopy classes. ◇

$A \cong B$ if $\exists \varphi \in \mathrm{Hom}(A, B)$ and $\psi \in \mathrm{Hom}(B, A)$ such that $\varphi\psi = 1_A$ and $\psi\varphi = 1_B$.

Definition 0.18.2. Take the morphisms $A, B \in \mathrm{Ob}(C)$. P together with $\alpha \in \mathrm{Hom}(P, A)$ and $\beta \in \mathrm{Hom}(P, B)$ is a *product* if every $P' \to A, B$ through α', β' respectively, there exists a unique γ such that $\gamma \in \mathrm{Hom}(P', P)$.

For example, suppose $A \times B \xrightarrow{\alpha,\beta} A, B$ and $G \xrightarrow{\pi_A,\pi_B} A, B$. Then $\gamma(g \in G) = (\pi_A, \pi_B)$.

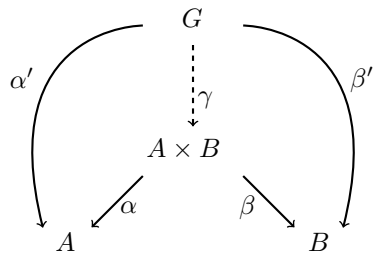

Figure 0.18.1: Product

Definition 0.18.3. $P, \alpha\colon A \to P, \beta\colon B \to P$ is a *coproduct* if for all $P', \alpha'\colon A \to P', \beta'\colon B \to P'$ there exists a $\gamma\colon P \to P'$.

In $\overline{\text{Set}}$, categorical products are the usual products. Coproducts of sets are disjoint unions $A \sqcup B$ (usually defined by something like $(A \times \{0\}) \cup (B \times \{1\})$ or something like this).

Two elements in the category of sets are isomorphic if they have the same cardinality.

$\overline{\text{AB}}$ is the category of abelian groups with group homomorphisms. The categorical product is the product.

For the coproduct, define $\alpha(g) = (g, 0)$ and $\beta(g) = (0, g)$. Then $\gamma\colon A \times B \to G$ is defined by $\gamma(a, b) = (\alpha'(a), \beta'(b))$.

In contrast, in $\overline{\text{Gp}}$, the coproduct is a free product: $A * B$ is the group consisting of formal expressions of the form $a_1 b_1 a_2 b_2 \cdots a_n b_n$, $a_i \in A$, $b_i \in B$.

0.19 Fields

For fields F, G every morphism $F \to G$ is an injection, i.e. the ker is trivial.

Proof. All nonzero elements of F are units, and so the only possible ideals are (0) and F, so $\ker \varphi = 0$ or $\ker \varphi = F$ but $\varphi(1) = 1$ so $1 \notin \ker \varphi$. □

Definition 0.19.1. If F, G are fields and $F \subset G$, we say G is an *extension* of F and F is a *base*.

Definition 0.19.2. The *characteristic* of a field F, $\text{Char}(F) = \min\{n \in \mathbb{N}\colon n1 = 0 \in F\}$. If the set is empty, then $\text{Char}(F) = 0$.

Example. $\text{Char}(\mathbb{Z}/p\mathbb{Z}) = p$, $\text{Char}(\mathbb{Q}) = 0$. ◇

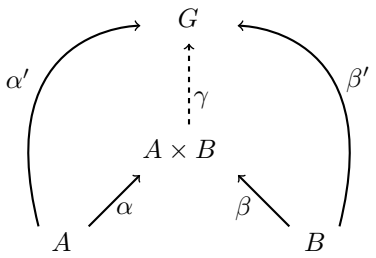

Figure 0.18.2: Coproduct

If $\mathrm{Char}(F) = p$, then F is an extension of $\mathbb{Z}/p\mathbb{Z}$. If $\mathrm{Char}(F) = 0$, then F is an extension of $\mathbb{Q}$.

Lecture 26: Category Theory

Wednesday, November 04, 2020

Definition 0.19.3. An *initial object* in a category $\overline{C}$ is $I \in \mathrm{Ob}(\overline{C})$ such that $\forall A \in \mathrm{Ob}(\overline{C})$ there exists a unique $\varphi\colon I \to A$ ($\varphi \in \mathrm{Hom}(I, A)$).

Definition 0.19.4. A *final object* in a category $\overline{C}$ is $F \in \mathrm{Ob}(\overline{C})$ such that $\forall A \in \mathrm{Ob}(\overline{C})$ there exists a unique $\varphi\colon A \to F$ ($\varphi \in \mathrm{Hom}(F, A)$).

We can then define categories in terms of the initial objects and their morphisms. If we imagine a category with objects P, A, B, P' and maps $\alpha, \beta\colon P \to A, B$ and $\alpha', \beta'\colon P' \to A, B$, the induced product gives us a map from $P \to P'$, so the product is a terminal object in this category.

Definition 0.19.5. If $\overline{C}$ is a category, and we "reverse the arrows", we get the *opposite category* $\overline{C}^{\mathrm{op}}$.

As we said last lecture, every field contains one of the prime fields $\mathbb{Z}/p\mathbb{Z}$ with p prime and $\mathbb{Q}$.

Notation

We denote field extensions by F/K signifying an "F extension of K".

Definition 0.19.6. $[F : K] = \dim_K F$ is the *degree* of an extensions.

Claim. If F/K and G/F are extensions, then $[G : K] = [G : F][F : K]$.

Proof. Let $(\alpha_i)_{i \in I}$ is a basis for G/F and $(\beta_j)_{j \in J}$ is a basis for F/K, we claim that $(\alpha_i \beta_j)_{i \in I, j \in J}$ is a basis for G/K.

We can prove this claim by saying that for $x \in G$, we can write $x = \sum_i y_i \alpha_i$ for $y_i \in F$, since this is how we define the field extension. Each of these $y_i = \sum_j z_{ij}\beta_j$ due to the second field extension, so we can write $x = \sum_{ij} z_{ij}\alpha_i\beta_j$.

Next, we want to show linear independence.

$$0 = \sum_{ij} z_{ij}\alpha_i\beta_j = \sum_i (\sum_j z_{ij}\beta_j)\alpha_i$$

This is an F-linear combination of $(\alpha_i)_{i\in I}$, so linear independence in α implies $\sum_j z_{ij}\beta_j = 0$ for all i. Then linear independence in β implies $z_{ij} = 0\ \forall i, j$, so $\alpha_i\beta_j$ is a basis. □

Definition 0.19.7. Given two extensions F/K and G/K such that $F, G \subseteq H$, the *composition/composite* of F and G denoted FG is the smallest field containing F and G.

Claim. Let F be a field and let $p \in F[x]$ be an irreducible polynomial. Then there exists an extension of F in which p has a root.

Proof. $k = \frac{F[x]}{(p)}$ is a field since $F[x]$ is a PID and so (p) is maximal. If we take the usual map from $F \to K$, calling it π, the $\ker \pi \neq 0$ since $\pi(1) = 1$, so p has a root in K, namely x. □

Note that $[K : F] = \deg p$.

Definition 0.19.8. An element $Q \in F$ is called *algebraic* over K (if F/K) if Q is a root of a polynomial in $K[x]$.

Definition 0.19.9. An extension F/k is *algebraic* if every element is algebraic.

Example. $\mathbb{C}/\mathbb{R}$ is algebraic, but $\mathbb{C}/\mathbb{Q}$ is not. ◇

Claim. If F/K and $Q \in F$ is a root of an irreducible polynomial $p \in K[x]$, then $K(Q) \cong \frac{K[x]}{(p)}$.

Proof. Define $\varphi\colon K[x] \to F$ by $f \mapsto f(Q)$. The $\ker \varphi \supseteq (p)$. Since (p) is maximal, $\ker \varphi \neq (p)$, so $\varphi(1) = 0$. This implies that

$$\frac{K[x]}{(p)} \cong K[Q] = K(Q)$$

□

Example. Take $x^3 - 2$, an irreducible over $\mathbb{Q}$. The roots are $\sqrt[3]{2}$, $w\sqrt[3]{2}$, and $w^2\sqrt[3]{2}$ where $w^3 = 1$, so $\mathbb{Q}[\sqrt[3]{2}] \cong \mathbb{Q}[w\sqrt[3]{2}]$. ◇

Example.

$$\mathbb{C} = \mathbb{R}[\imath] \cong \frac{R[x]}{(x^2 + 1)}$$

◇

Claim. If FG is the composition of F and G and K is an extension of F and G, then $[FG : K] \leq [F : K][G : K]$.

Proof. Take a basis α_i of F/K and β_j of G/K. We claim that $(\alpha_i\beta_j)$ is a spanning set $/K$ for FG. Every polynomial in FG can be written $\sum_{ij} c_{ij}\alpha_i\beta_j$ with $c_{ij} \in K$. Indeed, elements of F are of this form by taking $\beta_j = 1$, and likewise for α_i and G. $\alpha_i\alpha_k \in F$ and is therefore a K-linear combination of α's.

We will finish this proof on the Friday lecture. □

Lecture 27: Zorn's Lemma
Friday, November 06, 2020

In the previous class, we were trying to prove the following claim:

Claim. $[FG\colon K] \leq [F\colon K][G\colon K]$

The first part of the proof concerned showing that if $(\alpha_i)_i$ is a basis for F/K and $(\beta_j)_j$ is a basis for G/K then $FG = K[\{\alpha_i\}_i \cup \{\beta_j\}_j]$.

Proof. Recall that if Q is algebraic over K, then $K[Q] \cong K(Q)$, so $F = K[(\alpha_i)_{i\in I}]$ and similar for G and $FG = K[(\alpha_i), (\beta_j)]$ implies every finite extension is algebraic in F/K for powers of $Q \in F$. □

Corollary 0.19.0.1. *If Q_1 and Q_2 are algebraic over K, then so is $Q_1 + Q_2$, Q_1Q_2, and Q_1/Q_2.*

Example. Consider $[\mathbb{Q}[\sqrt[3]{2}]\colon \mathbb{Q}] = 3$ and $[\mathbb{Q}[\sqrt{5}]\colon \mathbb{Q}] = 2$. Then if $m = [\mathbb{Q}[\sqrt[3]{2}, \sqrt{5}]\colon \mathbb{Q}]$ gives $m \leq 2 \cdot 3 = 6$. Also $m = [\mathbb{Q}[\sqrt{5}]\colon \mathbb{Q}] \cdot [\mathbb{Q}[\sqrt[3]{2}, \sqrt{5}]\colon \mathbb{Q}[\sqrt{5}]\colon \mathbb{Q}[\sqrt{5}]]$ implies $2 \mid m$ and $3 \mid m$ so $m = 6$. This proves that these roots and their powers are all linearly independent in $\mathbb{Q}$. ◇

Recall field K is algebraically closed if every polynomial of deg ≥ 1 has a root.

Definition 0.19.10. A binary relation $\leq$ on a set X is a *partial order* if

- $x \leq x$
- $x \leq y$ and $y \leq x$ implies $x = y$
- $x \leq y$ and $y \leq z$ implies $x \leq z$

An element x is *maximal* if $\nexists y \neq x$ such that $x \leq y$.

Definition 0.19.11. A *chain* is a set $C \subset X$ such that for every $x, y \in C$, either $x \leq y$ or $y \leq x$.

Definition 0.19.12. An *upper bound* for a set $S \subseteq X$ is an element x such that $\forall s \in S$, $s \leq x$.

The lemma states that if every chain has an upper bound, then there is a maximal element. For this class, we will take this to be an axiom.

Claim. If R is a ring with 1, $I \subset R$ is an ideal, then I is contained in a maximal ideal.

Proof. $X = \{\text{ideal} J\colon J \supset I, J \neq R\}$. $J, J' \in X$ and $J \leq J'$ if $J \subseteq J'$. Applying Zorn to $(X, \leq)$, we get the result. □

Lecture 28: Algebraic Closures
Monday, November 09, 2020

Recall that we defined a field F to be algebraically closed if very polynomial $f \in F[x]$ of $\deg f \geq 1$ has a root.

Equivalently, every polynomial splits into linear factors.

Claim. For every field K there is an extension E/K such that E is algebraically closed.

Proof. For each polynomial $f \in K[x]$ of $\deg f \geq 1$, introduce an indeterminate x_f and consider a polynomial ring $K[x_f \colon \deg f \geq 1]$.

Define an ideal $I = (f(x_f) \colon \deg f \geq 1, f \in K[x])$. We claim that $R \neq I$.

To prove this, if they were equal, $1 \in I$ implies $1 = \sum_{f \in S} g_f \cdot f(x_f)$ for $g_f \in R$ and S finite. $g_f \in R[x_f \colon f \in S]$.

Consider finitely many polynomials $f \colon f \in S$ and find an extension K'/K such that all $f \colon f \in S$ have a root each. The identity equation is an identity in $k'[x_f \colon f \in S]$. Evaluate both sides at the point $x_f = Q_f$ where $Q_f \in K'$ is a root of f. This gives a contradiction $(1 = 0)$, so $R \neq I$.

There exists a maximal ideal $M \subset R$ containing I. Let $E_0 = R/M$ be a field since M is maximal. E_0 contains a copy of K, and it also contains a root of every $f \in K[x]$ of $\deg f \geq 1$, namely x_f.

We can then do the same to E_0 to get the set E_1, and so on. We get a chain $E_0 \subset E_1 \subset E_2 \subset \cdots$, and we call $E = \bigcup_n E_n$.

We claim that E is algebraically closed. Take $f \in E[x]$. Since f has only finitely many coefficients, $\exists n$ such that $f \in E_n[x]$. Therefore f has a root in E_{n+1}, so f has a root in E. □

Theorem 0.19.2. *Every field K is contained in an algebraic extension that is algebraically closed.*

Proof. K is any field and E is an algebraically closed extension of K. Let $F = \{\alpha \in E \colon \alpha \text{ algebraic over } k\}$. We claim that F is a field, because if α, β are algebraic, then so are $\alpha + \beta$, $\alpha\beta$, α/β. We then claim that F is algebraically closed. $f \in F[x]$, and let $\alpha_0, \cdots, \alpha_n$ be coefficients of f. Then let $G = F[\alpha_0, \cdots, \alpha_n]$ so $f \in G[x]$. Now $[G \colon K]$ is finite because $[G \colon K] \leq \prod_{i=0}^{n} [K(\alpha_i) \colon K]$. Let $Q \in E$ be a root of f. $[G(Q) \colon G] \leq \deg f$, so $[G(Q) \colon K] \leq [G(Q) \colon G][G \colon K]$ is finite. Therefore, $Q \in F$. □

Definition 0.19.13. If F is algebraically closed and an algebraic extension of K, we call F the *algebraic closure* of K.

Claim. Suppose E/K is an algebraic extension and L is an algebraically closed field containing K. There is an embedding of E into L extending that of K into L.

Proof. Consider the set X of pairs (F, σ) where $K \subset F \subset E$ and F/K and $\sigma \colon F \to L$ is an embedding such that $\sigma\big|_K = \sigma_K$, the embedding of K into L. There is a partial order $(F, \sigma) \leq (F', \sigma')$ if $F \subseteq F'$ and $\sigma'\big|_F = \sigma$. Note that $X \neq \varnothing$ as $(K, \sigma_K) \in X$. If C is a chain where $\tilde{F} = \bigcup_{(F,\sigma) \in C} F$ and $\tilde{\sigma} = \bigcup_{(F,\sigma) \in C} \sigma$, then $(\tilde{F}, \tilde{\sigma})$ is an upper bound for C. Therefore, $\exists (F, \sigma)$ which is maximal in X.

We next claim that $F = E$. If this were not true, $\theta \in E \setminus F$ $F(\theta)/F$ is algebraic because θ is algebraic over K. We may then extend (F, σ) to $(F(\theta), \sigma')$, contradicting the maximality. How? Turns out we skipped a proposition: □

Claim. If K is a field and L is an algebraically closed field containing K, and θ is algebraic over K with minimal polynomial $p \in K[x]$, then there are m extensions of $K(\theta)$ to L, i.e. there are m maps $\sigma \colon K(\theta) \to L$ such that $\sigma\big|_K = \mathrm{id}_K$ where m is the number of distinct roots of p in L.

Proof. $\sigma(\theta)$ is a root of p because $p(\sigma(\theta)) = \sigma(p(x)) = p(\theta) = 0$ since the coefficients of p are in K, $\sigma(ab)$ with $a \in K$, $b \in K(\theta)$ is equal to $a\sigma(b)$.

Once we know where σ goes we know where everything goes. σ is determined by $\sigma(\theta)$ because every extension of $K[\theta]$ is a polynomial in θ. Conversely, if $\beta \in L$ is a root of p, then the map $f(\theta) \mapsto f(\beta)$ $\forall f \in K[x]$ is well-defined and is a homomorphism. We can show this since if $f(\theta) = g(\theta)$, then $h = f = g$ implies $h(\theta) = 0$, so $p\big|_K$ implies that $h(\beta) = 0$. □

LECTURE 29: MISSED LECTURE
Wednesday, November 11, 2020

Missed Lecture, need to type Michael's notes.

LECTURE 30:
Friday, November 13, 2020

0.20 Separable Polynomials

Definition 0.20.1. For a field K, we say that $f \in K[x]$ is *separable* if f has distinct roots in K (or equivalently in the splitting field of K).

The derivative of a polynomial $f = \sum_n a_n x^n \in K[x]$ is

$$\mathrm{D}f = \sum_n n a_n x^{n-1}$$

It's easy to show that $\mathrm{D}(fg) = f\mathrm{D}g + (\mathrm{D}f)g$.

Claim. $f \in K[x]$ is separable iff $\gcd(f, \mathrm{D}f) = 1$.

Proof. If f is not separable, then $f = (x-a)^2 g$ in $K[x]$, so

$$\mathrm{D}f = 2(x-a)g + (x-a)^2 \mathrm{D}g$$

so $x - a \mid f, \mathrm{D}f$.

Conversely, suppose $x - a \mid f, \mathrm{D}f$. Then we could write

$$f = (x-a)g$$

so

$$\mathrm{D}f = g + (x-a)\mathrm{D}g$$

Now we know that $x - a \mid \mathrm{D}f$, so therefore $x - a \mid g$. Substituting this back into the equation, we say that $g = (x-a)h$ so $f = (x-a)^2 h$. □

Claim. If $f \in K[x]$ is irreducible and is not separable, then $\mathrm{char}K = p \neq 0$ and f is of the form $f(x) = g(x^p)$.

Proof. $\deg \mathrm{D}f < \deg f$, and $\gcd(f, \mathrm{D}f) \neq 1$ implies $\exists g \mid f, \mathrm{D}f$. Since f is irreducible and UFD, $\mathrm{D}f = 0$. Therefore, $n a_n x^n = 0$ for all n, so if $a_n \neq 0$ then $n = 0$ in K, so $\mathrm{char}K \mid n \ \forall n$ such that $a_n \neq 0$. □

Claim. If K is a field and $\mathrm{char}K = p \neq 0$, then the map $y \mapsto y^p$ is a homomorphism from $K \to K$.

Proof.

$$(yz)^p = y^p z^p$$

$$(y+z)^p = \sum_{i+j=p} \binom{p}{i} y^i z^j$$

We know that $\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i!}$ if $i \geq 1$, and if $i < p$ then $p \mid \binom{n}{i}$, so $(a+b)^p = a^p + b^p$. □

Corollary 0.20.0.1. *If $k = \mathbb{Z}/p\mathbb{Z}$, the $g \in K[x]$, so $g(x)^p = g(x^p) = (ax^s + bx^t)^p = a^p x^{sp} + b^p x^{pt} = ax^{sp} + bx^{pt}$.*

0.21 Cyclotomic Extensions

Consider $x^n - 1$ over $\mathbb{Q}$. Its roots are nth roots of unity $w_n = \{\tau \in \mathbb{Q} \mid \tau^n = 1\}$.

Definition 0.21.1. The element of

$$w_n \setminus \bigcup_{d|n, d<n} w_d$$

is called a *primitive* root of unity of order n.

Let's define

$$\Phi_n(x) = \prod_{\tau^n=1, \tau \text{ is primitive with order } n} (x - \tau) \in \mathbb{Q}[x]$$

Claim. $\Phi \in \mathbb{Z}[x]$.

Proof.

$$\begin{aligned} x^n - 1 &= \prod_{d|n} \Phi_d \\ &= \Phi_n \prod_{d|n, d<n} \Phi_d \end{aligned}$$

By induction on n, we take the base case where $\Phi_1 = x - 1$. The equation we just showed tells us that $x^n - 1 = \Phi_n f$ where $f \in \mathbb{Z}[x]$ by the division algorithm. $\Phi_n \in \mathbb{Q}[x]$, so by Gauss's lemma, $\text{content}(x^n - 1) = 1$ and $\text{content}(f) = 1$ because $x^n - 1$ and f are monic. Therefore, $\text{content}(\Phi_n) = 1$. □

Note that $\deg \Phi_n$ is the number of the elements of the set $\#\{m \leq n \mid \gcd(m, n) = 1\} = \varphi(n)$ (Euler's totient function).

Theorem 0.21.1. *Φ_n is irreducible over $\mathbb{Q}$.*

Proof. By Gauss's lemma, Φ_n is irreducible over $\mathbb{Z}$. Suppose it is reducible:

$$\Phi_n(x) = f(x)g(x)$$

$$\tau \in w_n \setminus \bigcup_{d|n, d<n} w_d$$

Let p be any prime not dividing n and consider τ^p. Since $p \nmid n$, τ^p is also a primitive root of order n, so $\Phi_n(\tau^p) = 0$.

There are two cases. First, $g(\tau^p) = 0$, so τ is a root of $g(x^p)$. Therefore, $f(x) \mid g(x^p)$. Say $g(x^p) = f(x)h(x)$.

Let $\bar{f}$, $\bar{g}$, $\bar{h}$ be the images of $f, g, h \in \mathbb{Z}[x]$ in $\mathbb{Z}/p\mathbb{Z}[x]$ under the projection map.

Then $\bar{g}(x^p) = \bar{f}(x)\bar{h}(x)$, so $g(x)^p = \bar{f}(x)\bar{h}(x)$. Hence, the right-hand side is not separable.

Then, $\gcd(\bar{g}, \bar{f}) \neq 1$, hence $\bar{\Phi}_n = \bar{f}\bar{g}$ is non-separable.

On the other hand, $\Phi_n \mid x^n - 1$ in $\mathbb{Z}[x]$ and so in $\mathbb{Z}/p\mathbb{Z}[x]$, then $\bar{\Phi}_n$ non-separable implies $x^n - 1$ is non-separable. However, it's easy to check that $x^n - 1$ is separable, since $\mathrm{D}(x^n - 1) = nx^{n-1}$ and $\gcd(nx^{n-1}, x^n - 1) = 1$ if $p \nmid n$, so we have a contradiction. Therefore, the first case leads to a contradiction.

The second case is where $f(\tau^p) = 0$ wherever τ is a prime of order n and $(p, n) = 1$.

Then $\tau^{p_1 p_2 \cdots p_l}$ is a root of f whenever primes $p_1, \cdots, p_l$ do not divide $n, \cdots, l$. Then $f(\tau^m) = 0$ $\forall m$ such that $(m, n) = 1$, so f vanishes on all primitive roots of order n. Therefore $\Phi_n \mid f \implies \Phi_n = f$ is irreducible. □

LECTURE 31: GALOIS THEORY AND AUTOMORPHISMS
Monday, November 16, 2020

Let's look at the group $k = \mathbb{Z}/p\mathbb{Z}$ and consider the roots of $f(x) = x^{p^n} - x$. Let F be the set of roots of $f(x)$ in $\bar{k}$. First, $f(x)$ is separable, since $\mathrm{D}f = \mathrm{D}p^n x^{p^n-1} - 1$. Second, F is a field, since if $a, b \in F$, then $a^{p^n} = a$ and $b^{p^n} = b$, so $(a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b$. If $a \neq 0$, then $a^{p-1} - 1 = 0$ so $a^{p^n-2}a = 1$ so $a^{-1} = a^{p^n-2}$.

Now consider $\frac{F}{\mathbb{Z}/p\mathbb{Z}}$. F is called a finite field of size p^n. We will use the notation $\mathbb{F}_{p^n}$.

Theorem 0.21.2. *If F is a finite field, then $F \cong \mathbb{F}_{p^n}$ for some prime p and some $n \in \mathbb{N}$.*

Proof. $\mathrm{char}F = p \neq 0$ so $\mathbb{F}_p \subseteq F$. Hence $[F\colon \mathbb{F}_p] = n < \infty$.

Then $F^* = F \setminus \{0\}$ is an abelian group of order $|F| - 1 = p^n - 1$, so $\forall a \in F^*$, $a^{p^n-1} = 1$ and $\forall a \in F$, $a^{p^n} - a = 0$. □

0.22 Galois Theory and Automorphisms

We define $\mathrm{Aut}(F) = \{\sigma\colon \sigma \text{ is an automorphism of } F\}$.

If K is a subfield of F, then $\mathrm{Aut}(F/K) = \{\sigma \in \mathrm{Aut}(F)\colon \sigma/K = \mathrm{id}/K\}$.

Example. $\mathrm{Aut}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ where d is not a square. It contains $\{\mathrm{id}, a + b\sqrt{d} \mapsto a - b\sqrt{d}\}$. ◇

Example. $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{id}\}$. ◇

Definition 0.22.1. If $H \subseteq \mathrm{Aut}(F)$, then $\mathrm{Fix}(H) = \{a \in F\colon \sigma a = a \quad \forall \sigma \in H\}$.

- $\mathrm{Fix}(H)$ is a subfield of F.
- Usually, H is a subgroup of $\mathrm{Aut}(F)$.

$\mathrm{Fix}(H)$ is a *fixed field* of H.

$$H_1 \subseteq H_2 \implies \mathrm{Fix}(H_1) \supseteq \mathrm{Fix}(H_2)$$

The important point here is that

$$H \to \mathrm{Fix}(H)$$

is a bijection for nice (normal and separable) extensions.

Claim. If K is a field, $p \in K[x]$ with $\deg p \geq 1$ and F is a splitting field of p, then $|\mathrm{Aut}(K/F)| \leq [K\colon F]$, with equality if p is separable.

Proof. Let p_1 be an irreducible factor of p, and let α be a root of p_1. Let K_1 be the splitting field of K inside F.

Every $\sigma \in \mathrm{Aut}(F/K)$ satisfies $\sigma/K_1 \in \mathrm{Aut}(K_1/K)$. As we proved earlier, $|\mathrm{Aut}(K_1/K)|$ is the number of distinct roots of p_1.

Fix any $\sigma_1 \in \mathrm{Aut}(K_1/K)$. Then we claim the size of $S_{\sigma_1} \equiv \{\sigma \in \mathrm{Aut}(F/K)\colon \ \sigma\big|_{K_1} = \sigma_1\} = |\mathrm{Aut}(F/K_1)|$.

This is true because if we fix any extension of σ_1 to $\mathrm{Aut}(F/K)$, then σ^{-1}, σ for $\sigma \in \mathrm{Aut}(S_{\sigma_1})$, $\sigma^{-1}\sigma\big|_{K_1} = \frac{\mathrm{id}}{K_1}$.

In other words, there is a one-to-one correspondence between S_{σ_1} and $\mathrm{Aut}(F/K_1)$, namely $\sigma \in S_{\sigma_1} \to \sigma_1^{-1}\sigma$.

Since $[F\colon K] = [F\colon K_1][K_1\colon K]$ and $\mathrm{Aut}(K_1/K) \leq [K_1\colon K]$, by induction implied to F/K_1,

$$\mathrm{Aut}(F/K_1) \leq [F\colon K_1]$$

since every $\sigma_1 \in \mathrm{Aut}(K_1/K)$ extends in $|\mathrm{Aut}(F/K_1)|$ ways. □

Definition 0.22.2. A finite extension F/K is *Galois* if $|\mathrm{Aut}(F/K)| = [F\colon K]$.

We will use the notation $\mathrm{Gal}(F/K) = \mathrm{Aut}(F/K)$ for the Galois group of F/K.

If $p \in K[x]$ is irreducible, the Galois group of p is $\mathrm{Gal}(F/K)$ for splitting field F.

Example. Some Galois groups:

- Take $x^2 - d$ for d not square over $\mathbb{Q}$. Then $\mathrm{Gal}(F/K) \cong \mathbb{Z}/2\mathbb{Z}$.
- $K\mathbb{F}_2(t)$, $p = x^2 - t$, then $\mathrm{D}p = 0$, so the only automorphism of this extension is $\mathrm{Aut}(F/K) = 1$, so F/K is not Galois. $\mathbb{F}_2[t]$ are polynomials in indeterminate t with $\mathbb{F}_2 -$ coeff. $\mathbb{F}_2(t)$ is a field of fractions of $\mathbb{F}_2[t]$, i.e. rational functions with $\mathbb{F}_2 -$ coeff.
- $x^3 - 2$, and $F = \mathbb{Q}(\sqrt[3]{2}, w) = \mathbb{Q}(\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2})$, then $|F\colon Q| = 6$ so $\mathrm{Aut}(F/\mathbb{Q})$ is order 6, so $S_3 \cong \{\text{roots of } x^3 - 2\}$.

◇

Lecture 32: Primitive Element Theorem

Wednesday, November 18, 2020

Recall that a finite extension F/K is Galois if F/K is normal and separable. Recall an extension is separable if a minimal polynomial of every $\alpha \in F$ is separable. Finite extensions are separable if they are generated by some roots of a separable polynomial.

Take F/K Galois and finite.

Claim. If $G = \mathrm{Gal}(F/K)$ then $\mathrm{Fix}(G) = K$.

Proof. $\mathrm{Fix}(G) \supseteq K$. Conversely, if $\alpha \in \mathrm{Fix}(G)$, then if $\alpha \notin K$, we can take any $F(\alpha)$ and β where β is another root of the same irreducible polynomial as α. Then $\exists\sigma\colon F(\alpha) \to F(\beta)$, and we can extend σ to an automorphism of F so $\alpha \notin \mathrm{Fix}(G)$, a contradiction. □

Claim. If F/E is an intermediate extension of Galois F/K (E/K is an extension), then F/E is Galois and the map $E \mapsto \mathrm{Gal}(F/E)$ is injective as a map.

Proof. Since F/K is Galois, F/K is normal, so F/E is normal. Next, F/K is separable and finite, so F is generated by separable polynomials over K, so F is generated by the elements of E, so F/E is separable. □

Suppose $H = \mathrm{Gal}(F/E)$ and $H' = \mathrm{Gal}(F'/E)$. If $H = H'$, then $F = \mathrm{Fix}(H)$ and $F' = \mathrm{Fix}(H')$, so $F = F'$.

Corollary 0.22.0.1. *If F/K is finite and Galois, there are only finitely many intermediate extensions.*

Proof. $\mathrm{Gal}(F/K)$ is finite. □

Theorem 0.22.1 (Primitive Element Theorem)**.** *If F/K has only finitely many intermediate extensions, then $\exists alpah \in F$ such that $F = K(\alpha)$.*

Proof. There are a few cases depending on whether K is finite. If K is infinite, then $K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq F$.

Therefore, we just need to prove that if $F = K(\alpha, \beta)$,there exists δ such that $F = K(\delta)$.

Consider $K(\alpha + c\beta)$ where $c \in K$. By the pigeonhole principle, $\exists c, c' \in K$ distinct such that $K(\alpha + c\beta) = K(\alpha + c'\beta) = E$. Then $\alpha + c\beta, \alpha + c'\beta \in E$, so $(c - c')\beta \in E$. $c - c' \neq 0$, so $\beta \in E$ and $\alpha \in E$. Then $K(\alpha, \beta) \subseteq E$, so $K(\alpha, \beta) = K(\gamma)$ where $\gamma = \alpha + c\beta$. □

Lemma 0.22.2. *If F/K is Galois and $[K(\alpha)\colon K] \leq n$, $\forall \alpha \in F$, then $[F\colon K] \leq n$.*

Proof. $F = K(\alpha)$ by the primitive element theorem. □

Theorem 0.22.3. *K is a field and G is a finite subgroup of $Aut(F)$, then $K = Fix(G)$, the extension F/K is Galois, and $Gal(F/K) = G$.*

Proof. Pick $\alpha \in F$. G_α is the orbit of α under G. $G_\alpha = \{\sigma_1\alpha, \sigma_2\alpha, \cdots, \sigma_n\alpha\}$. Note G acts by permutations on G_α. Consider $f(x) = \prod_{i=1}^{n}(x - \sigma_i\alpha)$. Note that $\tau \in G$ implies $\tau f(x) = \prod_{i=1}^{n}(x - \tau\sigma_i\alpha) = f(x)$. f is fixed by τ so every coefficient of f is fixed by τ. This means $f(x) \in K[x]$.

f is separable, so F/K is separable. $\deg f \leq |G|$, so by the lemma, $[F\colon K] \leq |G|$. On the other hand, F/K is normal because all roots of f are in F. $\mathrm{Gal}(F/K) \supseteq G$, and we know $[F\colon K] \geq |\mathrm{Aut}(F/K)| \geq |G|$, so $[F\colon K] = |G|$ and $G = \mathrm{Gal}(F/K)$. □

Corollary 0.22.3.1. *If F/K is Galois, the map of sets of intermediate extensions F/E, E/K to $Gal(F/E)$ is surjective.*

Lecture 33: Primitive Element Theorem, cont.

Friday, November 20, 2020

We will now prove the primitive element theorem for finite fields.

Proof. Recall that elements of $\mathbb{F}_{p^n}$ are the roots of $x^{p^n} - x \in \mathbb{F}[x]$. Let $\theta \in \mathbb{F}_{p^n} \setminus \bigcup_{F \text{ proper subfield } \mathbb{F}_{p^n}} F$. We claim that θ is a root of $x^{p^n} - x$ that is not a root of $\prod_{d|n}(x^{p^d} - x)$. Conversely, if θ is a root of the first and not the second, then $\theta \in \mathbb{F}_{p^n} \setminus \bigcup_{F \text{ proper subfield } \mathbb{F}_{p^n}} F$.

Indeed, $F_p(\theta)$ is a finite field of degree d over $\mathbb{F}_p$ and θ is a root of $x^{p^d} - x$.

The degree of the first equation is p^n. The degree of the second (the product) is

$$\sum_{d<n} p^d < 2p^{n-1} < p^n$$

by properties of geometric series. □

Suppose F/K is Galois and E is an intermediate extension. Then consider the case where E/K is Galois (equivalently E/K is normal). We can take any element of the Galois group $\sigma \in \mathrm{Gal}(F/K)$ and restrict it to E: $\sigma\big|_E \in \mathrm{Gal}(E/K)$ because E/K is normal. We now have a map from the larger Galois group to the smaller by restriction.

$$\varphi\colon \mathrm{Gal}(F/K) \to \mathrm{Gal}(E/K)$$
$$\sigma \mapsto \sigma\Big|_E$$

φ is surjective by the extension lemma. $\ker\varphi = \mathrm{Gal}(F/E)$, and F/E is normal, so by the first isomorphism theorem,

$$\mathrm{Gal}(E/K) \cong \frac{\mathrm{Gal}(F/K)}{\mathrm{Gal}(F/E)}$$

Conversely, consider the same F, E, K fields but suppose we only know F/K is Galois (instead of E/K). Take $\sigma \in \mathrm{Gal}(F/K)$. We can now look at automorphims $\mathrm{Aut}(\sigma E/K)$. This is equivalent to $\sigma\mathrm{Aut}(E/K)\sigma^{-1}$ ($\sigma E = \{\sigma(a)\colon a \in E\}$ is a field).

So, if $G = \mathrm{Gal}(F/E)$ is normal, then $E = \mathrm{Fix}(G)$.

Claim. E/K is a normal extension.

Proof. If E/K is not normal, $\exists\sigma \in \mathrm{Aut}(\bar{E})$ such that $\sigma E \neq E$. $G = \sigma\big|_F \in \mathrm{Gal}(F/K)$. Then $\underbrace{\mathrm{Fix}(\sigma G\sigma^{-1})}_{=\mathrm{Fix}(G)} = \sigma\mathrm{Fix}(G)$ so $\sigma E = E$. □

0.23 Finite Fields

Claim. $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois and the Galois group is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Proof. $\mathbb{F}_{p^n}$ is a splitting field of $x^{p^n} - x$.

$\mathrm{Frob}(y) = y^p$, and $\mathrm{Frob} \in \mathrm{Aut}(\mathbb{F}_{p^n})$. $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$ since $[\mathbb{F}_{p^n}\colon \mathbb{F}_p] = n$.

We now claim that Frob is an element of order n in $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

$\mathrm{Frob}^m = \mathrm{id}$ implies that $\forall a \in \mathbb{F}_{p^n}$, $a = \mathrm{Frob}(a) = a^{p^m}$. This means that $x^{p^m} - x$ vanishes on $\mathbb{F}_{p^n}$. Therefore, $m \geq n$. □

0.24 Cyclotomic Extensions of $\mathbb{Q}$

Let $w_n = \{\text{roots of } x^n - 1 \text{ in } \bar{\mathbb{Q}}\}$.

$$\mathbb{Q}(w_n)/\mathbb{Q} = \mathbb{Q}(\alpha)/\mathbb{Q}$$

where α is any primitive root of order n and the minimal polynomial of $a/\mathbb{Q}$ is Φ_n, and so the extension $\mathbb{Q}(w_n)/\mathbb{Q}$ is of degree $\varphi(n)$.

Claim.

$$\mathrm{Gal}(\mathbb{Q}(w_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^* = \{a\colon \gcd(a, n) = 1\}$$

under multiplication.

Proof.

$$a \in (\mathbb{Z}/n\mathbb{Z})^* \mapsto \varphi_a$$

where $\varphi_a(f(\alpha)) = f(\alpha^a)$ $\forall f \in \mathbb{Q}[x]$.

We need to check that this is well-defined. $f(\alpha) = g(\alpha)$ implies $\Phi_n \mid f - g$. This implies $(f - g)(\alpha^a) = \Phi_n(\alpha^a \times \cdots) = 0$. Therefore, φ_a is a homomorphism: $\varphi_a(f + g) = \varphi_a(f) + \varphi_a(g)$ and $\varphi_a(fg) = \varphi_a(f)\varphi_a(g)$.

Therefore,

$$(\mathbb{Z}/n\mathbb{Z})^* \mapsto \mathrm{Gal}(\mathbb{Q}(w_n)/\mathbb{Q})$$

is well-defined:

$$\begin{aligned}(\varphi_a \circ \varphi_b)(f(\alpha)) &= \varphi_a(f(\alpha^b)) \\ &= f((\alpha^a)^b) \\ &= f(\alpha^{ab}) \\ &= \varphi_{ab}(f(\alpha))\end{aligned}$$

□

Lecture 34: The Quintic Formula

Monday, November 23, 2020

The goal today is to show that an equation $x^n + a_{n-1}x^{n-1} \cdots + a_0$ of degree $n \geq 5$ has no solution in radicals (roots).

Claim. Suppose K/F is Galois and F/F' is an arbitrary finite extension. Then KF'/F' is Galois and $\mathrm{Gal}(KF'/F) \cong \mathrm{Gal}(K/(K \cap F'))$.

Proof. Since K/F is Galois, K is a splitting field over F of some separable polynomial $f \in F[x]$. Then KF' is a splitting field over F' of the same polynomial.

Take $\sigma \in \mathrm{Gal}(KF'/F') \mapsto \sigma\big|_K$. σ fixes F', so σ fixes $K \cap F'$. K/F is normal so $K/(K \cap F')$ is normal, so $\sigma K = K$. Therefore, $\sigma\big|_K \in \mathrm{Gal}(K/(K \cap F'))$. We will define this restriction as $\varphi\colon \mathrm{Gal}(KF'/F') \to \mathrm{Gal}(K/(K \cap F'))$. We know then that $\ker\varphi = \{\sigma \in \mathrm{Gal}(KF'/F')\colon \sigma\big|_K = \mathrm{id}_K\}$. σ fixes K and $\sigma \in \mathrm{Gal}(KF'/F')$, so it also fixes F'. Therefore, σ fixes KF' so $\sigma = \mathrm{id}_{KF'}$.

Let H be the image of φ in $\mathrm{Gal}(K/(K \cap F'))$. Then let $E = \mathrm{Fix}(H)$. Consider $E' = EF'$. On one hand, we claim that E' is fixed by $\mathrm{Gal}(KF'/F')$. To do this, we need to show that E and F' are both fixed. E is fixed because $E = \mathrm{Fix}(H)$. F' is fixed because every element of the Galois group fixes F'. Hence $E' \subseteq F'$, so $E \subseteq F'$, so $E \subseteq F' \cap K$. Therefore, $E = K \cap F'$, and by Galois correspondence, $H = \mathrm{Gal}(K/(K \cap F'))$. □

Definition 0.24.1. An extension K/F is cyclic/abelian/solvable if K/F is Galois and $Gal(K/F)$ is cyclic/abelian/solvable respectively. Note this is not a theorem, this is how we define these properties in extensions.

Corollary 0.24.0.1. *K/F is abelian implies KF'/F' is abelian*

Proof. $\mathrm{Gal}(K/(K \cap F')) \leq \mathrm{Gal}(K/F)$. □

Claim. Suppose $\mathrm{char}F \nmid n$ and F contains all nth roots of unity (roots of $x^n - 1$). Then for $a \in F$, $F(\sqrt[n]{a})/F$ is cyclic.

Proof. $F(\sqrt[n]{a})$ is the splitting field of $x^n - a$. $\sigma \in \mathrm{Gal}(F(\sqrt[n]{a})/F)$.

$$\sigma\sqrt[n]{a} = w(\sigma)\sqrt[n]{a}$$

where $w(\sigma)$ is an nth root of unity.

$$\varphi\colon \sigma \mapsto w(\sigma) \in F$$

We claim that φ is an injective homomorphism. First of all, it's a homomorphism since $\sigma(\sigma'\sqrt[n]{a}) = \sigma(w(\sigma')\sqrt[n]{a}) = w(\sigma')\sigma(\sqrt[n]{a}) = w(\sigma')w(\sigma)\sqrt[n]{a}$. The $\ker\varphi$ is where $w(\sigma) = 1$, so $\sigma = \mathrm{id}$, so it is injective.

Therefore $\mathrm{Gal}(F(\sqrt[n]{a})/F)$ is isomorphic to a subgroup of nth roots of unity, which is cyclic.

Example. Every finite subgroup of a multiplicative group of a field is cyclic. To prove this, let G be such a group. The number of elements of exponent n in G is the number of solutions to $x^n - 1 = 0$. The number of solutions is $\leq n$. Using the classification of finite abelian groups, it must be the product of cyclic groups. $\diamond$

Definition 0.24.2. An extension K/K_0 is a *radical* extension if there is a sequence of extensions $K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n = K$ such that $K_{n+1} = K_n(\tau_n)$ where τ_n is a root of $x^{m_n} - a_n = 0$, or $\tau_n = \sqrt[m]{a}$.

Observe that $\mathrm{char} K_0 = 0$. If K/K_0 is radical, then there exists K'/K such that K'/K_0 is radical and K'_{n+1}/K'_n is abelian.

We can prove this by induction on the length. The induction step goes as follows. We will transform the extension onto roots of a into the sequence of extensions $K(w_n)$, $K(w_{n+1}\sqrt[n]{a})$, etc. This is a cyclotomic extension. Look at the extension of $K(w_n)$. There exists some extension of K which is $\mathbb{Q}$ along with an extension to $\mathbb{Q}(w_n)$ which extends to $K(w_n)$. Since the extension between $\mathbb{Q}$'s is abelian, then the extension between K's is.

We now claim that if $\mathrm{char} K_0 = 0$, K/K_0 is radical from the above observation. Then $\mathrm{Gal}(K/K_0)$ is solvable.

Define $G_m = \mathrm{Gal}(K_m/K_0)$. We know that since all these extensions are normal, $G_{m+1}/G_m \cong \mathrm{Gal}(K_{m+1}/K_m)$, which is abelian. We then have a sequence $1 \triangleright G_1 \triangleright \cdots \triangleright G_n$, such that G_{m+1}/G_m is abelian. This is the definition of solvablility. We will conclude this proof in the next lecture. $\square$

Lecture 35: The Quintic Formula, Cont.

Monday, November 30, 2020

Last time, we proved that every radical extension of characteristic 0 field is contained in a solvable extension. We now want to use this to prove that there are equations that don't have a radical solution.

Take equations of quadratic form, $x^2 + bx + c = 0$. We know that the roots are given by the quadratic equation:

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

Theorem 0.24.1. *There exists a degree-5 equation with $\mathbb{Z}$-coefficients whose roots are not in a radical extension.*

Lemma 0.24.2. *If $p \in \mathbb{Q}[x]$ all of prime degree and all but 2 of whose roots are real, then the Galois group of p in $\mathbb{Q}$ is S_n where $n = \deg p$.*

Proof. Suppose G is the Galois group of p. We can think of G as the group which permutes the roots of p. $G \leq \mathrm{Sym}(\text{roots of p})$. We will call the roots of p R. G acts transitively on R, i.e. R is the orbit of G.

The reason for this is the following. K is a splitting field of p such that $G = \mathrm{Gal}(K/\mathbb{Q})$. If $r \in R$, $f \equiv \prod_{r' \in Gr}(x - r')$. f is fixed by G, such that $\tau f = \prod_{r' \in Gr}(x - \tau r')$, so $f \in \mathrm{Fix}(G)[x] = \mathbb{Q}[x]$.

Because G acts transitively on R, $R = \frac{|G|}{|G_r|}$ where G_r is the stabilizer of some $r \in R$ (from very early in this class). We assumed that $|R| = n$ is prime, so $n \mid |G|$.

By Cayley's theorem, there exists an element $g \in G$ of order n, so g is an n-cycle on R. Indeed, if g is a product of an a_1-cycle, a_2-cycle, a_3-cycle, etc., then the order of $g = \mathrm{lcm}(a_1, a_2, a_3, \cdots)$.

Now we will use the assumption that all but two roots are real. Since complex conjugation is an automorphism of $\mathbb{C}$ and hence of $K \subseteq \mathbb{C}$, it gives us an element $g' \in G$ which is a transposition on R. We have shown that the Galois group contains two elements, an n-cycle on the roots and this transposition:

$$S_n = \langle (12\cdots n), (ij) \rangle$$

□

Now for the proof of the original theorem:

Proof. Take $p = x^5 - 4x + 2$. This is irreducible in $\mathbb{Q}$ using the Eisenstein theorem for prime 2. The derivative is $p' = 5x^4 - 4$, so the roots of p' are $\pm(4/5)^{1/4}$ and those are simple. □

Theorem 0.24.3. *If K/F is a degree n extension and $\mathrm{char}(F) \nmid n$ and F contains all nth roots and K/F is cyclic, then $K = F(\sqrt[n]{a})$ for $a \in F$.*

If we have a solvable extension K/K_0 with Galois group G, then $\frac{G_{m+1}}{G_m}$ are cyclic. Suppose there is a sequence of extensions K_n between K and K_0. Then if K_0 has enough roots of unity, then the theorem implies that $\frac{K_{i+1}}{K_i}$ are radical.

Definition 0.24.3. The *character* of a field F in a field K is a map $\varphi\colon F^* \to K^*$ that is a homomorphism of abelian groups.

Lemma 0.24.4. *If $\sigma_1, \cdots, \sigma_m$ are distinct characters $F^* \to K^*$, then $\sigma_1, \cdots, \sigma_m$ are linearly independent over K.*

Proof. Induction on m (base case is trivial): Suppose $a_1\sigma_1 + \cdots + a_m\sigma_m = 0$, i.e. $\forall b \in F^*$, $a_1\sigma_1(b) + \cdots + a_m\sigma_m(b) = 0$ (call this equation 1). There must exist some c such that $\sigma_1(c) \neq \sigma_2(c)$. Then, $\forall b$, $a_1\sigma_1(bc) + \cdots = 0$, but this is equal to $a_1\sigma_1(c)\sigma_1(b) + \cdots = 0$ (call this equation 2).

Then $\sigma_1(c)(\text{Eq } 1) - \text{Eq } 2 = a_2(\sigma_1(c) - \sigma_2(c))\sigma_2(b) + \cdots = 0$. The first term in parentheses here is nonzero by definition. □

Corollary 0.24.4.1. *If F/E is Galois and $\sigma_1, \cdots, \sigma_n \in Gal(F/E)$, then $\sigma_1, \cdots, \sigma_n$ are linearly independent over F.*

Now the proof of the theorem:

Proof. Define for $\alpha \in K$ and nth root $w \in F$ the following expression:

$$[\alpha, w] \equiv \alpha + w\sigma(\alpha) + w^2\sigma^2(\alpha) + \cdots + w^{n-1}\sigma^{n-1}(\alpha)$$

where $\mathrm{Gal}(K/F) = \langle \sigma \rangle$. Now examine the action of this generator on the expression:

$$\sigma[\alpha, w] = \sigma(\alpha) + w\sigma^2(\alpha) + \cdots + w^{n-1}\sigma^n(\alpha)$$

Now $\sigma^n(\alpha) = \alpha$ and $w^n = 1$ so we can write

$$\sigma[\alpha, w] = w^{-1}[\alpha, w]$$

Therefore, $\sigma[\alpha, w]^n = [\alpha, w]^n$, so this element is fixed by σ: $[a, w]^n \in \mathrm{Fix}(\langle\sigma\rangle) = \mathrm{Fix}(\mathrm{Gal}) = F$. So we've found some element whose nth power is in F. It now suffices to show that $[F([\alpha, w])\colon F] = n$.

Chose an α such that $[\alpha, w] \neq 0$ using the lemma, because $\mathrm{id} + w\sigma + w^2\sigma^2 + \cdots \neq 0$. If $[F([\alpha, w])\colon F] = m$, this means $[\alpha, w]$ is fixed by σ^m by the Galois correspondence. We know that $\sigma^m[\alpha, w] = w^{-m}[\alpha, w]$, and $w^{-m} = 1 \iff n \mid m$. □

Lecture 36: Algebraic Geometry

Wednesday, December 02, 2020

0.25 Intro to Algebraic Geometry

If $f_1, \cdots, f_s \in k[X]$ (where $X = (x_1, \cdots, x_n)$), we can examine

$$V(f_1, \cdots, f_s) = \{a \in k^n \colon f_i(a) = 0 \quad \forall i\}$$

We call this an affine variety, which is an algebraic set. Equivalently, if $I = (f_1, \cdots, f_s)$,

$$V(f_1, \cdots, f_s) = V(I)$$

Example. Over $\mathbb{R}$,

$$V(x^2 + y^2 - 1)$$

is a circle and

$$V(xy - 1)$$

is a hyperbola, etc. ◇

More generally, given a set $S \in k^n$, we can look at an ideal

$$I(S) = \{f \in k[X] \colon \left. f \right|_S = 0\}$$

Let's combine these notions:

$$I(V(I)) \supseteq I$$

Definition 0.25.1. $\text{rad}I = \{r \colon \exists m \quad r^m \in I\}$. Note that rad$I$ is an ideal.

Theorem 0.25.1 (Hilbert's Nullstellensatz)**.** *If k is algebraically closed, then there is a bijection between the set of radical ideals in $k[X]$ and the varieties in k^n.*

Definition 0.25.2. A function $f \colon V \to k$ ($Vsubsetk^n$) is called *regular* if f agrees with a polynomial map $k^n \to k$.

If we look at the variety $V = V(xy - 1)$, then x and $x + (xy - 1)$ induce the same $V \to k$.

The ring of regular functions is denoted by $k[V] \equiv \frac{k[X]}{I(V)}$. People often denote k^n by $\mathbb{A}^n = V(\varnothing)$, called the affine n-space. In other words, $k[\mathbb{A}^n] = k[X]$.

Say we have two varieties, V and W, possibly living in different spaces: $V \subset \mathbb{A}^n$ and $W \subset \mathbb{A}^m$.

Then a regular map $\varphi \colon V \to W$ is a map such that $\varphi = (\varphi_1, \cdots, \varphi_m)\big|_V$ where each φ_i is a polynomial.
Claim. There is a bijection between regular maps $V \to W$ and k-algebra homomorphisms $k[W] \to k[V]$.

Proof. $\varphi \colon V \to W$ with the mapping $\varphi' = (f \in k[W] \mapsto f \circ \varphi \in k[V])$.

If φ is regular, then $\varphi'(f + g) = \varphi'(f) + \varphi'(g)$ and $\varphi'(cf) = c\varphi'(k)$ $\forall c \in k$.

For the converse direction, $\varphi' \colon k[W] \to k[V]$. Consider the image of $x_1, \cdots, x_m \in k[x_1, \cdots, x_m]$ in $k[W]$ and call it $\tilde{x}_i$.

Let $F_i = \varphi'(\tilde{x}_i) \in k[V]$ and define $\varphi \colon V \to k^m$ by $\varphi(a) = (F_1(a), \cdots, F_m(a))$. We claim that φ maps to W.

Recall that $k[W] = \frac{k[x_1, \cdots, x_m]}{I(W)}$, so if $f \in I(W)$, then $f \circ \varphi = 0$.

Then

$$\begin{aligned} f(F_1, \cdots, F_m) &= f(\varphi'(\tilde{x}_1), \cdots, \varphi'(\tilde{x}_m)) \\ &= \varphi'(f(\tilde{x}_1, \cdots, \tilde{x}_m)) \\ &= \varphi'(0) = 0 \end{aligned}$$

□

A particular case of the Nullstellensatz (the weak Nullstellensatz) appears if $1 \notin I \subset k[X]$. If k is algebraically closed, then there is a point in $V(I)$, i.e. a solution to a system of equations $f = 0 \; \forall f \in I$.

0.25.1 Projection

If $V = V(I) \subseteq \mathbb{A}^n$, we can project V to $\mathbb{A}^{n-1}$ with the mapping

$$(a_1, a_2, \cdots, a_n) \mapsto (a_2, \cdots, a_n)$$

We think of $I_1 = I \cap k[X_2, \cdots, X_n]$.

Note

The projection of V, denoted $\pi(V)$, satisfies $V(I_1) \supseteq \pi(V)$.

Example. $V = V(xy - 1)$. The projection of V is $\pi(V) = \mathbb{A}^1 \setminus \{0\}$ (you can see this if you plot the function and project onto the x-axis). In this case, $I_1 = (0)$ so $V(I_1) = \mathbb{A}^1$. $\diamond$

0.25.2 Resultants

When do two polynomials have a common map?

Claim. If $f, g \in k[x]$ (one variable for now) are polynomials of degree m and l respectively, then the following are equivalent:

- f and g have a common factor
- $\exists A, B \in k[x]$ with

$$0 < \deg(A) < l$$
$$0 < \deg(B) < m$$

such that $Af + Bg = 0$

Proof. If $f = hf'$, $g = hg'$, and $\deg(h) > 0$, then $A = g'$, $B = -f'$ and $Af + Bg = h(g'f' - f'g') = 0$.

Conversely, if A and B satisfy the second condition and $\gcd(f, g) = 1$ then $1 = \tilde{A}f + \tilde{B}g$ and so

$$\begin{aligned} B &= B(\tilde{A}f + \tilde{B}g) \\ &= B\tilde{A}f + \tilde{B}Bg \\ &= B\tilde{A}f - \tilde{B}Af \\ &= f(B\tilde{A} - \tilde{B}A) \end{aligned}$$

but $\deg(B) \geq \deg(f) = m$, and this is a contradiction. $\square$

LECTURE 37:
Friday, December 04, 2020

In the last lecture we were discussing a proof that f and g having a common factor is equivalent to saying that $Af + Bg = 0$ for some nonzero A and B of degree less than g and f respectively.

$$f = a_0 x^m a_1 x^{m-1} + \cdots + a_m$$

$$g = b_0 x^l b_1 x^{l-1} + \cdots + b_l$$

Then let

$$A = c_0 x^{l-1} + \cdots + c_{l-1}$$
$$B = d_0 x^{m-1} + \cdots + d_{m-1}$$

Then by matching coefficients we have, for the x^{l+m-1} term, $c_0 a_0 + d_0 b_0 = 0$, for the x^{l+m-2} term $c_0 a_1 + c_1 a_0 + d_0 b_1 + d_1 b_0 = 0$, and so on. We can write this system as a matrix:

$$\begin{pmatrix} a_0 & \cdots & b_0 & \cdots \\ a_1 a_0 & \cdots & b_1 b_0 & \cdots \\ a_2 a_1 a_0 & \cdots & b_2 b_1 b_0 & \cdots \\ \vdots & \vdots & \vdots & \vdots \\ \cdots & a_0 & \cdots & a_0 \\ A & & B & \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{l-1} \\ d_0 \\ d_1 \\ \vdots \\ d_{m-1} \end{pmatrix} = \vec{\mathbf{0}}$$

where $A = \begin{pmatrix} a_m & & \\ & \ddots & \\ & & a_m \end{pmatrix}$ and $B = \begin{pmatrix} b_l & & \\ & \ddots & \\ & & b_l \end{pmatrix}$. This is called the Sylvester matrix $\operatorname{Syl}(f, g, x)$.

The resultant of f and g with respect to x is $\operatorname{Res}(f, g, x) = \det \operatorname{Syl}(f, g, x)$.

Note that $\operatorname{Res}(f, g, x)$ is a polynomial in a_i and b_i.

Claim. There are A, B with $\deg(A) \leq l - 1$ and $\deg(B) \leq m - 1$ such that $\operatorname{Res}(f, g, x) = Af + Bg$ and furthermore the coefficients of A and B are polynomials with integer-coefficients in a_i and b_i.

Proof.

$$f \in k(a_0, \cdots, a_m)[X]$$
$$g \in k(b_0, \cdots, b_l)[X]$$

f and g have no common factor, so $\operatorname{Res}(f, g, x) \neq 0$. Consider the equation $\tilde{A}f + \tilde{B}g = 1$ with $\deg(\tilde{A}) \leq l - 1$ and $\deg(\tilde{B}) \leq m - 1$. In matrix form, we have

$$\operatorname{Syl}(f, g, x) \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{l-1} \\ d_0 \vdots \\ d_{m-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

We can determine the inverse of the Sylvester matrix:

$$\begin{pmatrix} c_0 \\ \vdots \\ d_{m-1} \end{pmatrix} = \frac{\operatorname{adj}(\operatorname{Syl}(f, g, x))}{\det(\operatorname{Syl}(f, g, x))} \begin{pmatrix} 0 \\ \vdots \\ 1 \end{pmatrix}$$

Therefore, if $A = \tilde{A}\operatorname{Res}(f, g, x)$ and $B = \tilde{B}\operatorname{Res}(f, g, x)$, then we get the result that we want. □

Claim. If $f, g \in k[x_1, \cdots, x_n] = k[x_2, \cdots, x_n][x_1]$, then $\text{Res}(f, g, x) \in k[x_2, \cdots, x_n]$ and so if $I = (f, g)$, then $\text{Res}(f, g) \in I_1$, where $I_1 = I \cap k[x_2, \cdots, x_n]$ is the first elimination ideal.

Claim. If $f, g \in k[x_1, \cdots, x_n]$ and $c \in k^{n-1}$, then consider $* = \text{Res}(f(x_1, c), g(x_1, c), x_1)$.

Let

$$h = \text{Res}(f, g, x_1) \in k[x_2, \cdots, x_n]$$

If $\deg(f(x_1, c)) = m$, then $* = a_0(c)^{\deg(g) - \deg(g(\cdots, c))} \cdot \text{Res}(f(x_1, c), g(x_1, c), x_1)$.

Proof. We are interested in the determinant of the Sylvester matrix (I won't write it down again). We know that $a_0(c) \neq 0$ by assumption. If $b_0(c) \neq 0$, then we obtain $\text{Syl}(f(x_1, c), g(x_1, c), x_1)$. What happens if $b_0(c) = 0$? Then we are left with a bunch of diagonal stripes of $b_1(c)$, $b_2(c)$, etc. Let's do expansion along the first row. The determinant becomes

$$\det(\text{Syl}) = a_0(c) \det(M)$$

where M is a submatrix of the Sylvester matrix without the first row or column. Then we can induct on the degree. □

Theorem 0.25.2 (Extension Theorem)**.** *Let k be an algebraically closed field and $I = (f_1, \cdots, f_s)$ with $f_i \in k[x_1, \cdots, x_n]$. Let $f_i = g_i(x_2, \cdots, x_{n-1}) x_1^{N_i} + \text{lower order terms with } x_1$.*

Suppose $(c_2, \cdots, c_n) \in V(I_1)$ and $(c_2, \cdots, c_n) \notin V(g_1, \cdots, g_s)$.

Then $\exists c_1 \in k$ such that

$$(c_1, c_2, \cdots, c_n) \in V(I)$$

Proof. Take $\varphi \colon k[x_1, \cdots, x_n] \to k[x_1]$ and $c = (c_2, \cdots, c_n)$ with the mapping $f \mapsto f(x_1, c)$. The image of this map is an ideal $I' = \varphi(I)$.

$k[x_1]$ is PID so $\exists u \in k[x_1]$ such that $I = (u)$. Then let $f \in I$ be such that $u = \varphi(f)$, which means $u(x_1) = f(x_1, c)$. If $\deg(u) > 0$, then since k is algebraically closed, there is a $c_1 \in k$ with $u(c_1) = 0$.

Then $\forall g \in I$, $\varphi(g)$ is a multiple of u and so $\varphi(g)(c_1) = 0$. Hence, $g(c_1, c) = 0$. This means that $(c_1, c) \in V(I)$, and in this case we are done.

On the other hand, suppose $\deg(u) = 0$, so u is constant. Then since $c \notin V(g_1, \cdots, g_s)$, $\exists i$ such that $g_i(c) \neq 0$. We then consider $h = \text{Res}(f_i, f, x_1)$. $h(c) = g_i(c)^{\deg(f) - \deg(u)} \text{Res}(f_i(x_1, c), f(x_1, c), x_1)$. The first coefficient is nonzero. The second term in this resultant is u, a constant, but the constant won't have any roots so this whole thing is nonzero.

$h \in (f_i, f) \cap k[x_2, \cdots, x_n] \subseteq I_1$, so $h(c = 0)$. This is a contradiction. □

Lecture 38: Proof of the Nullstellensatz

Monday, December 07, 2020

Example of the extension theorem:

Example.

$$f_1 = xy - 1$$
$$g_1 = y$$

Then $I = (f_1)$ and $I_1 = (0)$ so $V(I_1) = k^1$. ◇

The aim of this is to use it to prove the Nullstellensatz.

Remark

If g_1 is constant, then the extension is always possible.

Lemma 0.25.3 (Schwartz-Zippel)**.** *(Not Schwartz from Cauchy-Schwarz)*

If $f \in k[x_1, \cdots, x_n]$ and $S_1, \cdots, S_n \subset k$ of size $|S_1| = \cdots = |S_n| = m$, then

$$V(f) \cap (S_1 \times \cdots \times S_n) \leq dm^{n-1}$$

where $d = deg(f)$.

Proof. The proof is by induction on n. $f(x_1, \cdots, x_n) = \sum_{i=0}^{s} x_1^i g_i(x_2, \cdots, x_n)$ where $g_s \neq 0$. Given a solution of $f(c_1, \cdots, c_n) = 0$, either $g_s(c_2, \cdots, c_n) = 0$ or $g_s(c_2, \cdots, c_n) \neq 0$.

In the first case, the number of solutions of this type is $\leq (\deg(g_s)) \cdot m^{n-2} \cdot m \leq (d-s)m^{n-1}$.

The number of solutions of the other case is $\leq m^{n-1} \cdot s$.

Therefore, the total number of solutions is $\leq dm^{n-1}$. □

Corollary 0.25.3.1. *If k is infinite and $f \in k[x_1, \cdots, x_n]$ is nonzero, then $\exists c$ such that $f(c) \neq 0$.*

Corollary 0.25.3.2. *This is also true if k is algebraically closed, since no finite field is algebraically closed.*

Theorem 0.25.4 (Weak Nullsellensatz)**.** *If k is algebraically closed and $V(I) = \varnothing$, then $1 \in I$.*

Proof. $I = (f_1, f_2, \cdots, f_s)$. If we just tried to apply the extension theorem, we'd get stuck because we don't know the leading coefficients of these functions. We will apply a linear change of coordinates to remedy this:

$$(x_1, \cdots, x_n) \mapsto M(x_1, \cdots, x_n)$$

where M is an invertible $n \times n$ matrix.

$$\begin{aligned} x_1 &= \tilde{x}_1 \\ x_2 &= \tilde{x}_2 + a_2\tilde{x}_1 \\ x_3 &= \tilde{x}_3 + a_3\tilde{x}_1 \\ &\vdots \\ x_n &= \tilde{x}_n + a_n\tilde{x}_1 \end{aligned}$$

Write f_1 as a sum of homogeneous components

$$f_1(x_1, \cdots, x_n) = g_d(x_1, \cdots, x_n) + g_{d-1}(\cdots) + \cdots$$

where all terms in g_i are of degree i. Then

$$\begin{aligned} g_d(x_1, \cdots, x_n) &= g_d(a_1\tilde{x}_1, \tilde{x}_1 + a_2\tilde{x}_2, \cdots, \tilde{x}_1 + a_n\tilde{x}_n) \\ &= \tilde{x}_1^d \cdot g_d(a_1, \cdots, a_n) + \cdots \end{aligned}$$

We can choose $a_1, \cdots, a_n$ such that $g(a_1, \cdots, a_n) \neq 0$. Then,

$$g_d(a_1, \cdots, a_n) = a_1^d g_d\left(1, \frac{a_2}{a_1}, \cdots, \frac{a_n}{a_1}\right)$$

Without loss of generality, let $a_1 = 1$. Let $\tilde{I} = \{f(\tilde{x}, \cdots, \tilde{x}usn) \colon f \in I\}$. Now we use induction on n. If $1 \notin \tilde{I}$, then $V(\tilde{I}) \neq \varnothing$. Consider $\tilde{I}_1 = \tilde{I} \cap k[x_2, \cdots, x_n]$. Then $1 \notin \tilde{I}$ implies that $1 \notin \tilde{I}_1$, so by induction $V(\tilde{I}_1) \neq \varnothing$. Let $c \in V(\tilde{I}_1)$. Then by the extension theorem, $\exists c_1$ such that $(c_1, c) \in V(\tilde{I})$. □

Theorem 0.25.5 (Strong Nullstellensatz)**.** *If k is algebraically closed and $f \in I(V(f_1, \cdots, f_s))$ then $f \in rad(f_1, \cdots, f_s)$, i.e. $\exists m$ such that $f^m \in (f_1, \cdots, f_s)$.*

Proof. $f_1, \cdots, f_s \in k[x_1, \cdots, x_n]$. Consider $J = (f_1, \cdots, f_s, 1 - yf) \subset K[x_1, \cdots, x_n, y]$. Then for $c \in V(J)$, $f_i(c) = 0\ \forall i$. This implies $f(c) = 0$, so $(1 - yf)(c) \neq 0$. Therefore, $V(J) = \varnothing$. By the Weak Nullstellensatz, $1 \in J$. Therefore,

$$1 = \sum g_i(x_1, \cdots, x_n, y) f_i + g(\cdots)(1 - yf)$$

We now work in $k(x_1, \cdots, x_n, y)$. Plug $y = 1/f$ into the previous equation, and we find that

$$1 = \sum_i g_i(X, 1/f) f_i$$

Therefore,

$$f^m = \sum_i f^m g_i(X, 1/f) f_i \in (f_1, \cdots, f_s)$$

□

This gives us a correspondence between varieties and ideals:

(1) V is a variety, then $V(I(U)) = U$

(2) If k is algebraically closed, then J is a radical ideal implies $I(V(J)) = J$.

Proof. $\forall f \in I(U)$ (vanishes on U), $U \subseteq V(I(U)) \implies U = V(f_1, \cdots, f_s)$. $U \in V(f_1, \cdots, f_s)$. Then $U \supseteq V(I(U))$ and $V(f_1, \cdots, f_s) \supseteq V(I(U))$.

Also, $f_1, \cdots, f_s \in I(U)$ so $(f_1, \cdots, f_s) \subseteq I(U)$. Therefore $V(f_1, \cdots, f_s) \supseteq V(I(U))$. □

Lecture 39: Intersections

Wednesday, December 09, 2020

Recall that a variety is a set $V(I) = \{c \in k^n \colon f(c) = 0, \quad V_f \in I\}$ where $I \subset k[x_1, \cdots, x_n]$

Claim. If U and W are varieties, then so are $U \cup W$ and $U \cap W$.

Proof. Suppose $U = V(I)$ and $W = V(J)$. Then

$$U \cap W = V(I + J)$$

where $I + J$ is the ideal generated by $I \cup J$.

$$U \cup W = V(IJ)$$

This is a bit less obvious. First note that $U \subseteq V(IJ)$ because $IJ \subseteq I$, and similar for W, so $U \cup W \subseteq V(IJ)$. If $c \notin U \cup W$, then $\exists f \in I$ with $f(c) \neq 0$ and $\exists g \in G$ such that $g(c) \neq 0$. Then $fg \in IJ$ implies $(fg)(c) \neq 0$ so $c \notin V(IJ)$. □

Definition 0.25.3. A variety U is irreducible if whenever $U = U_1 \cup U_2$, then either $U = U_1$ or $U = U_2$.

Theorem 0.25.6. *Every variety can be written as a union of finitely many irreducible varieties.*

Lemma 0.25.7. *If $V_1 \subseteq V_2 \subseteq V_3 \subseteq \cdots$ is an infinite chain of varieties, then $\exists n$ such that $V_n = V_{n+1} = \cdots$.*

Proof. Recall than $(I(V_i)) = V_i$, so $I(V_1) \subseteq I(V_2) \subseteq \cdots$. Since $k[X]$ is Noetherian, any sequence of ideals must stabilize, which implies that the sequence of varieties must stabilize. □

We can now prove the theorem:

Proof. Say V_1 is not a union of finitely many irreducibles. V_1 is therefore not irreducible, so $V_1 = V_2 \cup V_2'$ and $V_1 \neq V_2$ and $V_1 \neq V_2'$. Since V_1 is "bad" then at least one of these V_2 or V_2' must be "bad" as well, because if it wasn't, then we could write them both as finite unions of irreducibles. Without loss of generality, suppose V_2 is "bad". Write $V_2 = V_3 \cup V_3'$. This process must continue, so

$$V_1 \supsetneq V_2 \supsetneq V_3 \supsetneq \cdots$$

Because of the lemma we just proved, this is a contradiction. □

Remark

$V(f)$ is irreducible iff f is irreducible.

Theorem 0.25.8 (Bezout's Theorem in the Plane)**.** *The number of intersections of $f = 0$ and $g = 0$ is equal to $(deg(f)) \times (deg(g))$ if $\gcd(f, g) = 1$.*

Before we prove this, let's do an example to convince ourselves it's even right.

Example. Suppose

$$f = (x - a_1)(x - a_2) \cdots (x - a_n)$$

and

$$g = (y - b_1)(y - b_2) \cdots (y - b_m)$$

If you look at the points (a_i, b_i) which make these functions zero, there are clearly no more than $n \times m$ of them. However, there is the possibility that one of the roots has multiplicity greater than one. ⋄

The other problem is if the curves f and g are in the same variable, like $f = x$ and $g = x - 1$.

0.26 Projective Geometry

Consider $\mathbb{R}^2 \subset \mathbb{R}^3$. If we take a plane $z = 1$ in $\mathbb{R}^3$, we can imagine a 1-to-1 correspondence between points in the plane and lines through the origin meeting the plane. This correspondence ensures that a line in the $z = 1$ plane corresponds to a plane meeting $z = 1$ in a line. Suppose there are now two parallel lines in the $z = 1$ plane, l_1, l_2. Then $l_1 \leftrightarrow \pi_1$ and $l_2 \leftrightarrow \pi_2$ where π_1 and π_2 are planes in $\mathbb{R}^3$. $\pi_1 \cap \pi_2$ is a line parallel to the $z = 1$ plane.

We denote the real projective plane by $\mathbb{RP}^2$ or $\mathbb{P}^2(\mathbb{R})$. Points of this set are lines through the origin in $\mathbb{R}^3$ and lines in this set are planes through the origin in $\mathbb{R}^3$.

A point in $\mathbb{P}^2(\mathbb{R})$ is an equivalence of triples $(x, y, z) \neq 0$ and (cx, cy, cz). More generally, we can extend this to $\mathbb{P}^d(\mathbb{R})$ with

$$(x_0, \cdots, x_d) \sim (cx_0, \cdots, cx_d)$$

If f is a homogeneous polynomial, then $f(cx) = c^{\deg(f)} f(x)$, so $f(cx) = 0 \iff f(x) = 0$.

Lemma 0.26.1. *Let k be a field and $f, g \in k[x, y]$ have no common factors. Then Res$(f, g, x) \neq 0$.*

Proof. If $\text{Res}(f, g, x) = 0$, then $f, g \in k(y)[x]$ have a common factor in $k(y)[x]$.

By Gauss's lemma, since $k[y]$ is a UFD, this implies that f and g have a common factor in $k[y][x] = k[x, y]$. □

Lecture 40:
Friday, December 11, 2020

(Missed first 10 minutes)

Recall the coordinate transform

$$\begin{aligned} x &= a_1\tilde{x} \\ y &= \tilde{y} + a_2\tilde{x}f(x,y) && = f_n(x,y) + f_{n-1}(x,y) + \cdots \\ f_n(x,y) &= \tilde{x}^n f_n(a_1, a_2) + \text{ lower order} \end{aligned}$$

Write $g(x, y) = g_n(x, y)+g_{n-1}(x, y)+\cdots$ so that $g_m(x, y) = \tilde{x}^m g_m(a_1, a_2)$. Consider $g_n(a_1, a_2)f_n(a_1, a_2) = k$. Then there exists an a_1 and a_2 with $a_1 \neq 0$ such that $h(a_1, a_2) \neq 0$.

There are in fact many such a_1 and a_2. Suppose there exist a_1 and a_2, a_2' such that both $h(a_1, a_2) \neq 0$ and $h(a_1, a_2') \neq 0$. Without loss of generality, say that $\deg(f) = m$ and $\deg(g) = n$. $f(x, y)$ is of the form $x^m a_0 + x^{m+1}a_1 + \cdots$ and $g(x, y)$ is of the form $x^n b_0 + x^{n-1}b_1+$ where $a_0 \neq 0$ and $b_0 \neq 0$. In general, $\deg(a_i) \leq i$ and $\deg(b_j) \leq j$. Consider the resultant,

$$\text{Res}(f, g, x) = \det S$$

where S is the Sylvester matrix. The left half contains diagonals of the coefficients a_i and the right half contains diagonals of b_i We denote the (i, j) entry as $S_{ij} \in k[y]$. The degree of the matrix elements are

$$\begin{aligned} \deg(S_{ij}) &\leq i - j \qquad j \leq n \\ \deg(S_{ij}) &\leq i - (j - n) \qquad j > n \end{aligned}$$

$$\text{Res}(f, g, x) = \sum_{\sigma \in S} (-1)^\sigma \prod S_{ij\sigma(i)}$$

so

$$\begin{aligned} \deg(\text{Res}(f, g, x)) &\leq \max_\sigma \sum_{i=1} \deg(S_{ij} < ++ > \sigma(i)) \\ &\leq \sum_{1}^{n+m} (1 - \sigma(i)) + \sum_{\sigma(i)>n} n \qquad (1 - \sigma(i) \to 0) \\ &= nm \end{aligned}$$

So $\deg(\text{Res}(f, g, x)) \leq nm$. As long as it is nonzero, then it has at most nm roots, but we know that it is nonzero because we supposed f and g had no common factor.

We know that $V(f, g)$ is finite because it is finite in projections in at least two coordinate systems, and once we know that it is finite, we can choose a coordinate transform such that no two points are horizontal.