Graduate Algebra, Spring 2015
Lecture Notes

Andrei Jorza

Last updated April 30, 2015

Lecture 1
2015-01-14

---

1 Linear algebra

1.1 Symmetric and exterior powers

Definition 1. If M is an R-module define the **symmetric k-th power** $\mathrm{Sym}^k M$ be the quotient of $M^{\otimes k} := M \otimes \cdots \otimes M$ by the submodule S^k_M generated by $m_1 \otimes \ldots \otimes m_k - m_{\sigma(1)} \otimes \ldots \otimes m_{\sigma(k)}$ where $m_i \in M$ and $\sigma \in S_k$. We denote the image of a pure tensor $v_1 \otimes \ldots \otimes v_k$ in $\mathrm{Sym}^k M$ by $v_1 \cdots v_k$.

Definition 2. If M is an R-module define the **exterior k-th power** $\wedge^k M$ be the quotient of $M^{\otimes k}$ by the submodule E^k_M generated by $m_1 \otimes \ldots \otimes m_k - \varepsilon(\sigma) m_{\sigma(1)} \otimes \ldots \otimes m_{\sigma(k)}$ where $m_i \in M$ and $\sigma \in S_k$. We denote the image of a pure tensor $v_1 \otimes \ldots \otimes v_k$ in $\wedge^k M$ by $v_1 \wedge \cdots \wedge v_k$.

Proposition 3. *The assignments $(-)^{\otimes k}$, $\mathrm{Sym}^k(-)$ and $\wedge^k(-)$ are functors on R-modules.*

Proof. If $f : M \to N$ is a homomorphism of R-modules then $f^{\otimes k} : M^{\otimes k} \to N^{\otimes k}$ defined by $f^{\otimes k}(\sum m_{i_1} \otimes \cdots \otimes m_{i_k}) = \sum f(m_{i_1}) \otimes \cdots \otimes f(m_{i_k})$ is an R-module homomorphism.

Projecting $\pi_k : N^{\otimes k} \to \mathrm{Sym}^k N$ and $\tau_k : N^{\otimes k} \to \wedge^k N$ we see that S^k_M (resp. E^k_M) is in the kernel of the composite map $\pi_k \circ f^{\otimes k}$ (resp. $\tau_k \circ f^{\otimes k}$). Thus $\pi_k \circ f^{\otimes k}$ (resp. $\tau_k \circ f^{\otimes k}$) factor through $\mathrm{Sym}^k M$ (resp. $\wedge^k M$) yielding R-module homomorphisms $\mathrm{Sym}^k f$ and $\wedge^k f$.

It's not hard to check that $(f \circ g)^{\otimes k} = f^{\otimes k} \circ g^{\otimes k}$, $\mathrm{Sym}^k(f \circ g) = \mathrm{Sym}^k(f) \circ \mathrm{Sym}^k(g)$ and $\wedge^k(f \circ g) = \wedge^k f \circ \wedge^k g$. Finally, $\mathrm{id}^{\otimes k} = \mathrm{id}$, $\mathrm{Sym}^k \mathrm{id} = \mathrm{id}$ and $\wedge^k \mathrm{id} = \mathrm{id}$. □

Proposition 4. *If M is a free R-module of rank n then $M^{\otimes k}$ is free of rank n^k, $\mathrm{Sym}^k M$ is free of rank $\binom{n+k-1}{k}$ and $\wedge^k M$ is free of rank $\binom{n}{k}$.*

Proof. Let $v_1, \ldots, v_n$ be a basis of M over R.

Then $M^{\otimes k} = (\oplus R v_i)^{\otimes k} \cong \bigoplus_{1 \le i_1, \ldots, i_k \le n} R v_{i_1} \otimes \cdots \otimes v_{i_k}$. Let $s = \bigoplus_{1 \le i_1 \le \ldots \le i_k \le n} R v_{i_1} \otimes \cdots \otimes v_{i_k}$ and $e = \bigoplus_{1 \le i_1 < \ldots < i_k \le n} R v_{i_1} \otimes \cdots \otimes v_{i_k}$. From the definition of S^k_M and E^k_M it follows that $\pi_k(s)$ spans $\mathrm{Sym}^k M$ and $\tau_k(e)$ spans $\wedge^k M$. Thus it suffices to show that $\pi_k|_s$ and $\tau_k|_e$ are injective, in which case the first isomorphism theorem yields the statement.

Note that S^k_M is spanned by $v_{i_1} \otimes \cdots \otimes v_{i_k} - v_{i_{\sigma(1)}} \otimes \cdots \otimes v_{i_{\sigma(k)}}$ for $1 \le i_1 \le \ldots \le i_k \le n$ and E^k_M is spanned by $v_{i_1} \otimes \cdots \otimes v_{i_k} - \varepsilon(\sigma) v_{i_{\sigma(1)}} \otimes \cdots \otimes v_{i_{\sigma(k)}}$ for $1 \le i_1 < \ldots < i_k \le n$.

For the first one: we need to show that $s \cap S^k_M = 0$. Suppose

$$\sum_{1 \le i_1 \le \ldots \le i_k \le n} \alpha_{i_1, \ldots, i_k} v_{i_1} \otimes \cdots \otimes v_{i_k} = \sum_{1 \le i_1 \le \ldots \le i_k \le n} \sum_{\sigma \in S_k} \beta_{i_1, \ldots, i_k, \sigma} (v_{i_1} \otimes \cdots \otimes v_{i_k} - v_{i_{\sigma(1)}} \otimes \cdots \otimes v_{i_{\sigma(k)}})$$

such that the RHS contains only nonzero vectors $v_{i_1} \otimes \cdots \otimes v_{i_k} - v_{i_{\sigma(1)}} \otimes \cdots \otimes v_{i_{\sigma(k)}}$. Note that if $v_{i_{\sigma(1)}} \otimes \cdots \otimes v_{i_{\sigma(k)}} = v_{j_{\tau(1)}} \otimes \cdots \otimes v_{j_{\tau(k)}}$ appears in the above sum then it must be that $\sigma = \tau$ and $i_u = j_u$ or else the tensor would not appear at all in the sum. This shows that all the coefficients β are trivial and so all the coefficients α are also trivial.

The second case is similar. □

Proposition 5. *Let R be a commutative ring and M and N free R-modules.*

1. *Then*
$$\operatorname{Sym}^k(M \oplus N) \cong \oplus_{i+j=k} \operatorname{Sym}^i M \otimes_R \operatorname{Sym}^j N$$
$$\wedge^k(M \oplus N) \cong \oplus_{i+j=k} \wedge^i M \otimes_R \wedge^j N$$
2. *If $f \in \operatorname{End}_R(M)$ and $g \in \operatorname{End}_R(N)$ then $\operatorname{Sym}^k(f \oplus g) = \oplus \operatorname{Sym}^i(f) \oplus \operatorname{Sym}^j(g)$ and similarly for $\wedge^n$.*
3. *If $R \to S$ is a ring homomorphism then $S \otimes_R M$ is a free S-module and $\operatorname{Sym}^k_S(S \otimes_R M) \cong S \otimes_R \operatorname{Sym}^k_R M$ and $\wedge^k_S(S \otimes_R M) \cong S \otimes_R \wedge^k_R M$.*

Proof. See homework 1. □

Lecture 2
2015-01-16

1.2 Determinants and Traces

Suppose R is a commutative ring, M is a rank n-dimensional free R-module and $T \in \operatorname{Hom}_F(V, V)$. Fixing a basis $m_1, \ldots, m_n$ of M we may represent T as a matrix $A = (a_{i,j}) \in M_n(R)$ such that $T(m_i) = \sum a_{i,j} m_j$.

Definition 6. The trace of A is $\operatorname{Tr} A = \sum a_{i,i}$ and the determinant of A is

$$\det A := \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$$

Definition 7. Let R, M, T as above. Recall that $\wedge^n M$ is a rank 1 R-module and so $\wedge^n T : \wedge^n M \to \wedge^n M$ is in $\operatorname{Hom}_R(R, R)$ so is given by multiplication by an element $\det T \in R$ called the **determinant** of T.

Proposition 8. *Let R, M, T and A as above.*

1. $\det T = \det A$
2. *If A and B are two matrices then* $\det(AB) = \det(A)\det(B)$.

Proof. (1): $\wedge^n M = Rm_1 \wedge \ldots \wedge m_n$ and

$$\begin{aligned}
\wedge^n T(m_1 \wedge \ldots \wedge m_n) &= (Tm_1) \wedge \ldots \wedge (Tm_n) \\
&= \wedge^n_{i=1}(\sum a_{i,j} m_j) \\
&= \sum_{1 \le k_1, \ldots, k_n \le n} \prod a_{i,k_i} m_{k_1} \wedge \ldots \wedge m_{k_n} \\
&= \sum_{\sigma \in S_n} \prod a_{i,\sigma(i)} m_{\sigma(1)} \wedge \ldots \wedge m_{\sigma(n)} \\
&= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod a_{i,\sigma(i)} m_1 \wedge \ldots \wedge m_n \\
&= \det T m_1 \wedge \ldots \wedge m_n
\end{aligned}$$

(2): Also represent by A and B the two homomorphism. Then AB is the matrix of $A \circ B$ so we need to check that $\det(A \circ B) = \det(A)\det(B)$. But $\wedge^n$ is a functor so $\wedge^n(A \circ B) = \wedge^n A \circ \wedge^n B$ and multiplication by $\det B$ composed with multiplication by $\det A$ is the same as multiplication by $\det A \det B$. □

Proposition 9. *1. The map $M \otimes_R \wedge^{n-1} M \to \wedge^n M$ defined by $\langle u, v\rangle := u \wedge v$ is a well-defined R-module homomorphism which is a perfect pairing, i.e., $\langle u, -\rangle$ and $\langle -, v\rangle$ are not the zero homomorphisms for $u, v \neq 0$. Thus $\wedge^{n-1} M \cong \mathrm{Hom}_R(M, \wedge^n M)$.*

2. The adjoint homomorphism is $T^* = \wedge^{n-1} T \in \mathrm{End}_R(\wedge^{n-1} M)$ where $\wedge^{n-1} M$ has rank n. Then $\langle Tu, T^* v\rangle = \det T \langle u, v\rangle$ for all u and v.

3. Under the isomorphism $M \cong \mathrm{Hom}_R(M, \wedge^n M)$ (given by sending m_i to the linear map attaching to $m \in M$ the coefficient of m_i in the expansion of m as a linear combination of $m_1, \ldots, m_n$ times $m_1 \wedge \ldots \wedge m_n$) interpret T^* in $\mathrm{End}_R(M)$. Then $T \circ T^* = \det T \,\mathrm{id}$.

4. T is invertible in the ring $\mathrm{End}_R(M)$ if and only if $\det T \in R^\times$.

Proof. (1): The map is well-defined so only need to check that that it is perfect. Let $u = \sum u_i m_i$ with, e.g., $u_i \neq 0$. Then $\langle u, \wedge_{j \neq i} m_j\rangle = \pm u_i \neq 0$. This implies that $\wedge^{n-1} M \to \mathrm{Hom}_R(M, R)$ sending v to $u \mapsto \langle u, v\rangle$ is an injective homomorphism of R-vector spaces. If $f : M \to R$ is a homomorphism such that $f(m_i) = \sum s_{i,j} m_j$ let $v = \sum (-1)^{j-1} s_{i,j} \wedge_{k \neq j} m_k$. Then $u \mapsto \langle u, v\rangle$ is f so we get an isomorphism.

(2): Write $v = \sum u_2 \wedge \ldots \wedge u_n$ in which case

$$\begin{aligned}
\langle Tu, T^* v\rangle &= (Tu) \wedge (T^* v) \\
&= (Tu) \wedge (\sum (Tu_2) \wedge \ldots \wedge (Tu_n)) \\
&= \wedge^n T \sum u \wedge u_2 \wedge \ldots \wedge u_n \\
&= \det T u \wedge v \\
&= \det T \langle u, v\rangle
\end{aligned}$$

Lecture 3
2015-01-19

---

(3): Let $m \mapsto \phi_m$ be the isomorphism $M \cong \mathrm{Hom}_R(M, \wedge^n M)$ and let $v \in \wedge^{n-1} M$ such that $\phi_m = \langle -, v\rangle$. Then T^* on M is defined by $\phi_{T^*(m)}(u) = \langle u, T^* v\rangle$. Also note that $\phi_{T(m)}(u) = \phi_m(T(u))$. Indeed, if $m = \sum \alpha_i m_i$ and $Tm_i = \sum s_{i,j} m_j$ then $\phi_{T(m)}(m_i) = \sum \alpha_j s_{j,i} m_1 \wedge \ldots \wedge m_n$ which is the same as $\phi_m(T(m_i))$. Finally,

$$\begin{aligned}
\phi_{T \circ T^*(m)}(u) &= \phi_{T^*(m)}(T(u)) \\
&= \langle Tu, T^* m\rangle \\
&= \det T \langle u, m\rangle \\
&= \det T \phi_m(u) \\
&= \phi_{\det T \cdot m}(u)
\end{aligned}$$

so $T \circ T^* = \det T \,\mathrm{id}$.

(4): If T is invertible with inverse S then $1 = \det(\mathrm{id}) = \det(T \circ S) = \det(T) \det(S)$ so $\det T \in R^\times$. Reciprocally, if $\det T \in R^\times$ then $(\det T)^{-1} T^* \in \mathrm{End}_R(M)$ is an inverse of T. □

Definition 10. For a matrix $A \in M_{n \times n}(R)$ let $\mathrm{Tr}\, A$ be the sum of the elements on the diagonal.

Proposition 11. *1. $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ for any matrices $A, B \in M_n(R)$.*

2. Consider $m'_1, \ldots, m'_n \in M$ such that $m'_i = \sum s_{i,j} m_j$. Then $m'_1, \ldots, m'_n$ is also a basis of M over T if and only if the matrix $S = (s_{i,j})$ is invertible, i.e., $\det S \in R^\times$.

3. The trace $\mathrm{Tr}\, T$ defined as $\mathrm{Tr}\, A$ is independent of the choice of basis of M over R.

4. $\det T = \mathrm{Tr} \wedge^n T$.

Proof. (1): A simple calculation yields this.

(2): Suppose m_i' is a basis. Then $m_i = \sum t_{i,j} m_j'$ gives the matrix $T = (t_{i,j})$ which is an inverse of S and so S is invertible. Reciprocally, if S is invertible then the linear map given by S is an isomorphism and so the image of a basis is a basis.

(3): If m_i' is another basis given by the matrix S then S is invertible and the matrix of T with respect to m_i' is SAS^{-1}. Thus $\mathrm{Tr}(SAS^{-1}) = \mathrm{Tr}(AS^{-1}S) = \mathrm{Tr}(A)$ as desired.

(4): Nothing to prove. □

1.3 Characteristic and minimal polynomials

Definition 12. Let R be a commutative ring, M a rank n free R-module and $T \in \mathrm{End}_R(M)$. Define $X - T$ as an $R[X]$-linear map on the $R[X]$-module $M_X := R[X] \otimes_R M$ as $X \otimes \mathrm{id} - 1 \otimes T$. The **characteristic polynomial** of T is $P_T(X) := \det(X - T)$.

Definition 13. Any R-module M is naturally a module over the ring $\mathrm{End}_R(M)$, scalar multiplication given by evaluation. Suppose now that $R = F$ is a field and $M = V$ is an n-dimensional F-vector space with linear map T. Consider the ring homomorphism $F[T] \to \mathrm{End}_F(V)$ sending $\sum a_i T^i$ to $v \mapsto \sum a_i T^i v$. By restrictions of scalars this gives V the structure of an $F[T]$-module which we denote V_T.

But $F[T]$ is a PID since F is a field and V is finite dimensional as an F-vector space so it is finitely generated over $F[T]$ (the F-basis generates it). The structure theorem then says that

$$V \cong F[T]^r \oplus \bigoplus F[T]/(P_i)$$

Finite dimensionality gives $r = 0$ and $P_i \in F[T]$ such that $P_1 \mid \ldots \mid P_k$ which we can choose to be monic.

Define the **minimal polynomial** of T as the monic polynomial $\min_T := P_k$.

Proposition 14. *If $P(X) \in F[X]$ then $P(T) = 0$ as a linear map on V if and only if $\min_T(X) \mid P(X)$.*

Proof. $P(T) = 0$ iff $P \in \mathrm{Ann}_{F[T]}(V_T) = (\min_T)$ (see the section on characteristic ideals from the lectures on modules over PIDs last semester) iff $P \in (\min_T)$ as desired. □

Proposition 15 (Cayley-Hamilton)**.** *1. Suppose M and N are finite rank free R-modules and $S \in \mathrm{End}_R(M)$ and $T \in \mathrm{End}_R(N)$. Then*

$$P_{S \oplus T}(X) = P_S(X) P_T(X)$$

2. $P_T(T) = 0$ and so $\min_T \mid P_T$.

3.

$$P_T(X) = \sum_{i=0}^{n} (-1)^i (\mathrm{Tr} \wedge^i T) X^{n-i}$$

4. If A is the matrix of T with respect to some basis then $P_T(X) = P_A(X) := \det(XI_n - A)$ and so $P_A(X)$ depends on A only up to conjugacy.

5. If S is another linear map then $P_{S \circ T}(X) = P_{T \circ S}(X)$ or, in terms of matrices, $P_{AB} = P_{BA}$.

Proof. (1): Let M have rank m and N rank n. Then $\wedge^{m+n}(M \oplus N) = \wedge^m M \otimes \wedge^n N$.

$$\begin{aligned}
\wedge^{m+n}(X \otimes I_{m+n} - 1 \otimes (S \oplus T)) &= \wedge^{m+n}(X \otimes (\mathrm{id}_M \oplus \mathrm{id}_N) - 1 \otimes (S \oplus T)) \\
&= \wedge^{m+n}(X \otimes \mathrm{id}_M - 1 \otimes S) \oplus (X \otimes \mathrm{id}_N - 1 \otimes T) \\
&= \wedge^m(X \otimes \mathrm{id}_M - 1 \otimes S) \otimes \wedge^n(X \otimes \mathrm{id}_N - 1 \otimes T) \\
&= P_S(X) P_T(X)
\end{aligned}$$

where in the second line we used the exercise from homework 1.

(2): I'll give two proofs. One, direct, given below. The other, using Jordan canonical forms, will come in the next section.

From homework 1 we see that $P_A(X) = P_1(X)\cdots P_k(X)$ and $P_k = \min_A$ and so $\min_A \mid P_A$ as desired.

(3): Remark that $\wedge^i V \otimes_F \wedge^{n-i} V \to \wedge^n V$ sending $\sum u_i \otimes v_i \mapsto \sum u_i \wedge v_i$ is an R-module homomorphism. Next, for $I \subset \{1,\ldots,n\}$ denote $v_I = \wedge_{s\in I} v_s$ and by $\overline{I}$ the complement. Write $\wedge^i T(v_I) = \sum_{|J|=|I|} \alpha_{I,J} v_J$. Let σ_I be the permutation obtained by concatenating the ordered sets I and $\overline{I}$. Then

$$(\operatorname{Tr} \wedge^i T) v_1 \wedge \ldots \wedge v_n = \sum_{|I|=i} \varepsilon(\sigma_I) \wedge^i T(v_I) \wedge v_{\overline{I}}$$

We compute

$$\begin{aligned}
\wedge^n (X - T) v_1 \wedge \ldots \wedge v_n &= (Xv_1 - Tv_1) \wedge \ldots \wedge (Xv_n - Tv_n) \\
&= \sum_{I \subset \{1,\ldots,n\}} \varepsilon(\sigma_I) (\wedge^{|I|}(-T) v_I) \wedge (\wedge^{|\overline{I}|} X v_{\overline{I}}) \\
&= \sum_{i=0}^{n} (-1)^i X^{n-i} \sum_{|I|=i} \varepsilon(\sigma_I) \wedge^i T v_I \wedge v_{\overline{I}} \\
&= \sum_{i=0}^{n} (-1)^i X^{n-i} \operatorname{Tr} \wedge^i T v_1 \wedge \ldots \wedge v_n
\end{aligned}$$

and the conclusion follows.

(4): This follows from the analogous statement for determinants of linear maps.

(5): From the second part it suffices to show that $\operatorname{Tr} \wedge^i (T \circ S) = \operatorname{Tr} \wedge^i (S \circ T)$ for all i. But this is immediate from the properties of Tr as $\wedge^i (T \circ S) = \wedge^i T \circ \wedge^i S$. □

Lecture 4
2015-01-21

1.4 Canonical forms

Definition 16. By a form of a matrix A we mean another matrix B such that $A \sim B$, i.e., there exists S invertible such that $A = SBS^{-1}$.

Theorem 17. *Let $A \in M_n(F)$ where F is a field. Then A is conjugate to a block-diagonal matrix* $\operatorname{diag}(A_1,\ldots,A_k)$ *where A_i are of the form*

$$\begin{pmatrix} 0_{1,r-1} & *_{1,1} \\ I_{r-1} & *_{r-1,1} \end{pmatrix}$$

and have entries in F. This is the **rational canonical form** *of A.*

Proof. It suffices to find a basis with respect to which the linear transformation T defined by A has matrix of the required form. As an $F[T]$-module the vector space F^n takes the form

$$\oplus F[T]/(P_i(T))$$

The required basis is given by $0 \oplus \cdots \oplus 0 \oplus T^k \oplus 0 \oplus \cdots \oplus 0$ where T^k is in position i and $0 \le k < \deg P_i$. □

Theorem 18. *Let F be a field and $A \in M_n(F)$.*

1. *An eigenvalue of A is $\lambda \in F$ such that for some $v \neq 0$, $Av = \lambda v$ in which case v is called an eigenvector. Then $\lambda \in F$ is an eigenvalue if and only if $P_A(\lambda) = 0$. By the set of eigenvalues of A we mean the set of roots of $P_A(X)$ counted with multiplicities.*

2. *If $A \sim B$ then A and B have the same set of eigenvalues.*

3. *If the roots of $P_T(X)$ are all in F then A is conjugate to a block diagonal matrix $B = \mathrm{diag}(A_1, \ldots, A_k)$ where A_i are of the form*

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

such that the set of elements on the diagonal of B coincides with the set of roots of $P_A(X)$. This is the **Jordan canonical form**.

4. *Let A be as above and $R(X) \in F[X]$. Then the set of eigenvalues of $R(A)$ equals the set $\{R(\lambda) | P_A(\lambda) = 0\}$.*

Proof. (1): $Av = \lambda v$ iff $(\lambda - A)v = 0$ iff $\ker(\lambda - A) \neq 0$. By the first isomorphism theorem this is equivalent to $\lambda - A$ being not invertible which we know to be equivalent to $\det(\lambda - A) = 0$ (as $F^\times = F - 0$) and this is equivalent to $P_A(\lambda) = 0$.

(2): This follows from either the definition or $P_A = P_B$ as polynomials.

(3): Consider again F^n as an $F[T]$ module written as $\oplus F[T]/(P_i)$ and we know that $P_i \mid P_T(X)$ which splits as a product of linear terms by hypothesis. Thus each P_i splits as a product of linear term. The Chinese Remainder Theorem then tells us that

$$F^n \cong \oplus F[T]/(Q_i(T))$$

where $Q_i(T) = (T - \lambda_i)^{k_i}$. We now choose as basis of F^n the vectors

$$0 \oplus \cdots \oplus 0 \oplus (T - \lambda_i)^k \oplus 0 \oplus \cdots \oplus 0$$

where $(T - \lambda_i)^k$ is in position i and $0 \leq k < k_i$. Then with respect to this basis T has matrix of the form B and so A and B are conjugate. Finally, it is immediate that the set of diagonal elements of B are its set of eigenvalues, which coincides with the set of eigenvalues of A.

(4): Note that if $A = SBS^{-1}$ then $R(A) = SR(B)S^{-1}$ and so $R(A)$ has Jordan canonical form $R(B)$ and the eigenvalues of $R(A)$, which are the diagonal elements of $R(B)$ are exactly as required. □

Lecture 5
2015-01-23

---

2 Integral rings

2.1 Basic properties

Definition 19. Suppose $A \subset B$ are commutative rings. An element $b \in B$ is integral over A if there exists a monic polynomial $P(X) \in A[X]$ such that $P(b) = 0$.

Say that B is integral over A if every element of B is integral over A.

Example 20.

1. $\sqrt{5} \in \mathbb{Q}(\sqrt{5})$ is integral over $\mathbb{Z}$. Indeed it's a root of $X^2 - 5$.

2. $\dfrac{1 + \sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5})$ is integral over $\mathbb{Z}$. Indeed, it satisfies $x^2 - x - 1 = 0$.

3. $\sqrt{5}/2$ is not integral over $\mathbb{Z}$ since it satisfies no monic equation.

Proposition 21. *Suppose $A \subset B$ are commutative rings. The following are equivalent.*

1. *$x \in B$ is integral over A.*

2. *$A[x]$ is finitely generated as an A-module.*

3. *$A[x] \subset M$ for an A-algebra M which is finitely generated as an A-module.*

Proof. (a) implies (b): If $x^n + a_{n-1}x^{n-1} + \cdots a_0 = 0$ then for $k \geq 0$, $x^{n+k} = -(a_{n-1}x^{n+k-1} + \cdots + a_0 x^k)$ and so $A[x] = A[x]_{\deg \leq n-1}$. Thus $A[x]$ is generated by $1, x, \ldots, x^{n-1}$.

(b) implies (c): Take $M = A[x]$.

(c) implies (a): Suppose $M = Am_1 + \cdots Am_r$. Consider ϕ multiplication by x on M. Let $\phi(m_i) = \sum a_{ij}m_j$. Then $T = \phi I_r - (a_{ij})$ acts trivially on $\oplus Am_i$. Let T^* be the adjoint matrix, still in $M_{r\times r}(A[\phi])$ and compute $T*\cdot T$. Since T acts by 0 we deduce $T^*\cdot T = 0$ and so $\det(T) = 0$. But $\det(T) = \det(\phi I_r - (a_{ij}))$ is a monic polynomial in ϕ. Write $\det(T) = \phi^r + a_{r-1}\phi^{r-1} + \cdots a_0 = 0$. Since ϕ is multiplication by 0 we deduce that $x^r + a_{r-1}x^{r-1} + \cdots + a_0 = 0$ and so x is integral over A. □

Corollary 22. *Let $\widetilde{A} = \{b \in B | b \text{ integral over } A\}$. Then $\widetilde{A}$ is a subring of B which contains A.*

Remark 1. The ring $\widetilde{A}$ is called the integral closure of A in B. If $A = \widetilde{A}$ say that A is integrally closed in B. An integral domain A is said to be integrally closed if it is so in its fraction field.

Proof. If $x \in \widetilde{A}$ then $A[x]$ is finitely generated over A. If $y \in \widetilde{A}$ then clearly y is also integral over $A[x]$ so $A[x, y]$ is finitely generated over $A[x]$ and so it is finitely generated over A. But $A[x + y], A[xy] \subset A[x, y]$ and so $x + y$ and xy are integral over A. □

Corollary 23. *Let $A \subset B \subset C$. If C is integral over B and B is integral over A then C is integral over A.*

Proof. Pick $c \in C$ satisfying $c^n + \sum b_{n-i}c^{n-i} = 0$. Then c is integral over $A[b_0, \ldots, b_{n-1}] \subset B$. Thus $A[b_0, \ldots, b_{n-1}, c]$ is finitely generated over $A[b_0, \ldots, b_{n-1}]$. But $b_i \in B$ are integral over A so $A[b_0, \ldots, b_{n-1}]$ are finitely generated over A. Thus $A[c] \subset A[b_0, \ldots, b_{n-1}, c]$ which is finitely generated over A and so c is integral over A. □

Corollary 24. *Suppose $A \subset B$ and $\widetilde{A}$ is the integral closure of A in B. Then $\widetilde{A}$ is integrally closed in B.*

Proof. We need to show that $\widetilde{\widetilde{A}} = \widetilde{A}$. But by the previous proposition $\widetilde{\widetilde{A}}$ is integral over A and thus it is contained in $\widetilde{A}$ and the equality follows. □

2.2 Integrality and localizations

Proposition 25. *Let $A \subset B$ such that B is integral over A.*

1. *If $\mathfrak{b} \subset B$ is an ideal then $B/\mathfrak{b}$ is integral over $A/(A \cap \mathfrak{b})$.*

2. *If $S \subset A$ is multiplicatively closed containing 1 then $S^{-1}B$ is integral over $S^{-1}A$.*

Proof. (1): The monic equation in $A[X]$ works for the residue classes too.

(2): If $b^n + a_{n-1}b^{n-1} + \cdots a_0 = 0$ then

$$(b/s)^n + (a_{n-1}/s)(b/s)^{n-1} + \cdots + a_0/s^n = 0$$

is a monic equation in $S^{-1}A[X]$ satisfied by $b/s \in S^{-1}A$. □

Corollary 26. *Suppose $A \subset B$ are integral domains and $S \subset A$ is multiplicatively closed containing 1. Let $\widetilde{A}$ be the integral closure of A in B. Then $S^{-1}\widetilde{A}$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

Proof. From the proposition we know that $S^{-1}\widetilde{A} \subset \widetilde{S^{-1}A}$ so we only need the other implication. Suppose b/s is integral over $S^{-1}A$. Then b/s satisfies a monic equation of the form

$$(b/s)^n + (a_{n-1}/s_{n-1})(b/s)^{n-1} + \cdots + a_0/s_0 = 0$$

in $S^{-1}B$.

Multiply by $(s\prod s_i)^n$. We get

$$W = (b\prod s_i)^n + a_{n-1}(\prod s_i)/s_{n-1}(b\prod s_i)^{n-1} + \cdots + a_0(\prod s_i)^n/s_0 = 0$$

which occurs in $S^{-1}B$ but $W \in B$ and all the coefficients are in A. Thus there exists $t \in S$ such that $tW = 0$.

Since B is a domain either $t = 0$ or $W = 0$. If $t = 0$ then $0 \in S$ so $S^{-1}? = 0$ for all ? and there is nothing to prove. Else we have $W = 0$ and so $b\prod s_i$ is integral over A. Finally

$$b/s = \frac{b\prod s_i}{s\prod s_i} \in S^{-1}\widetilde{A}$$

as desired. □

Example 27. Let $R = \mathbb{C}[t^2, t^3] \subset \mathbb{C}[t]$. Then $\operatorname{Frac} R = \mathbb{C}(t)$. Moreover, next time we'll show that UFDs are integrally closed and so $\mathbb{C}[t]$ is integrally closed.

Now $x = t^3/t^2 = t \in \operatorname{Frac} R$ and $x^2 - t^2 = 0$ is monic in $R[x]$ so $x = t$ is integral over R. Thus $\mathbb{C}[t] \subset \widetilde{R}$ and we conclude that $\mathbb{C}[t] \subset \widetilde{R} \subset \widetilde{\mathbb{C}[t]} = \mathbb{C}[t]$ and so the integral closure of R (in its fraction field) is $\mathbb{C}[t]$.

Lecture 6

2015-01-26

Proposition 28. *Suppose R is a UFD. Then R is integrally closed.*

Proof. Suppose $x = p/q \in \operatorname{Frac} R$ is written in lowest terms, i.e., $(p, q) = 1$. If x is integral over R we want to show that in fact $x \in R$. Suppose $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$. Clearing denominators we get

$$p^n + a_{n-1}p^{n-1}q + \cdots + a_0q^n = 0$$

but then we see that $q \mid p^n$. This implies that every prime factor of q must also divide p yielding a contradiction. Thus q has no prime factors and so q is a unit which implies that $x = p/q \in R$ as desired. □

Proposition 29. *Let A be an integral domain. The property "A is integrally closed" is local, i.e., the following are equivalent:*

1. *A is integrally closed.*
2. *$A_{\mathfrak{p}}$ is integrally closed for all prime ideals $\mathfrak{p}$.*
3. *$A_{\mathfrak{m}}$ is integrally closed for all maximal ideals $\mathfrak{m}$.*

Proof. (1) implies (2): Let $B = \operatorname{Frac} A$. Then $A = \widetilde{A}$ implies, from a previous proposition, that $\widetilde{(A - \mathfrak{p})^{-1}A} = (A - \mathfrak{p})^{-1}\widetilde{A}$ and it so $A_{\mathfrak{p}}$ is integrally closed.

(2) implies (3) is tautological.

(3) implies (1): Consider $f : A \to \widetilde{A}$ and its localizations $f_{\mathfrak{m}} : A_{\mathfrak{m}} \to \widetilde{A}_{\mathfrak{m}}$. Since $A_{\mathfrak{m}}$ are integrally closed it follows that $f_{\mathfrak{m}}$ are all surjective. But surjectivity is a local property (from last semester; actually last semester we proved that injective is a local property but surjective is analogous) and so f is surjective. Thus A is also integrally closed.

For completion, here is a proof (don't include in lecture, mention these notes). Suppose $f : M \to N$ is a homomorphism of modules over a ring R. (E.g., $M = A$ and $N = \widetilde{A}$ as A-modules.) If f is surjective then $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is surjective for each prime ideal $\mathfrak{p}$ of A. Indeed, if $f(m) = n$ then $f(m/s) = n/s$. Now suppose that $f_{\mathfrak{m}}$ is surjective for all maximal ideals $\mathfrak{m} \subset A$. Consider the exact sequence $M \to N \to \operatorname{coker} f \to 0$ which yields the exact sequence $M_{\mathfrak{m}} \to N_{\mathfrak{m}} \to (\operatorname{coker} f)_{\mathfrak{m}} \to 0$. Surjectivity of $f_{\mathfrak{m}}$ implies that $(\operatorname{coker} f)_{\mathfrak{m}} = 0$ and "equal to 0" is a local property of modules and so $\operatorname{coker} f = 0$. Thus f is surjective. □

2.3 Dedekind Domains

We've seen that UFDs are very convenient rings but there are many rings that are not UFDs. These rings occur naturally in number theory but we'll study them a little mainly because of their use in Galois theory later in the semester. For example they will provide an algorithm for computing Galois groups of polynomials with rational coefficients.

Definition 30. A **Dedekind domain** is an integral domain R which is not a field satisfying

1. R is integrally closed.
2. R is Noetherian.
3. Every nonzero prime ideal of R is maximal.

Remark 2. Dedekind domains are the next best thing after UFDs. There are non-UFD Dedekind domains (see later) but they still satisfy a UFD property for ideals and not for elements.

Example 31.
1. Every PID is Noetherian, integrally closed (being UFD) and every prime ideal is maximal by UFD. Thus every PID is a Dedekind domain.
2. In particular $\mathbb{Z}$ and $\mathbb{F}_p[X]$ are Dedekind domains.

The following is a plentiful source of Dedekind domains.

Proposition 32. *Suppose R is a Dedekind domain with fraction field K. Let L be a field which contains K and is finitely generated as a K-module. Then the integral closure S of R in L is also a Dedekind domain.*

Before we give the proof here are some examples.

Example 33.
1. Let $K \subset \mathbb{C}$ be a field which is generated by finitely many elements which are integral over $\mathbb{Q}$ (these are the algebraic elements). Then the integral closure of $\mathbb{Z}$ in K (the so-called ring of integers of K) is a Dedekind domain.
2. Let R be the integral closure of $\mathbb{Z}$ inside any field $K \supset \mathbb{F}_p(X)$ which is generated by finitely many algebraic elements. Then R is a Dedekind domain. (Such R appear as smooth functions on smooth curves over $\mathbb{F}_p$.)

Lemma 34. *Suppose R is an integral domain which is integral over a field. Then R is also a field.*

Proof. See homework 2. □

(Partial) Proof of Proposition 32. The ring S is integrally closed by definition.

Suppose $\mathfrak{q}$ is a prime ideal of S. We already saw that $S/\mathfrak{q}$ is integral over $R/(\mathfrak{q} \cap R)$. But $\mathfrak{q} \cap R$ is a nonzero prime ideal and so is maximal as R is Dedekind. (Need to check that in fact $\mathfrak{q} \cap R$ is nonzero. This too will be on homework 2.)

The previous lemma then implies that $S/\mathfrak{q}$ is a field and so $\mathfrak{q}$ is maximal.

Finally, we need that S is Noetherian. This is the harder part and requires Galois theory. □

Proposition 35. *Suppose R is a Dedekind domain and $S \subset R$ is multiplicatively closed and contains 1. Then $S^{-1}R$ is a Dedekind domain.*

Proof. Indeed, $S^{-1}R$ is integrally closed (see last lecture). Moreover, every prime ideal of $S^{-1}R$ is of the form $S^{-1}\mathfrak{p}$ for a prime ideal of R. Since R is Dedekind we deduce that $\mathfrak{p}$ is maximal and thus we get that $S^{-1}\mathfrak{p}$ is maximal as $S^{-1}R/S^{-1}\mathfrak{p} \cong S^{-1}(R/\mathfrak{p})$ and the localization of a field is a field.

Finally, we need that $S^{-1}R$ is Noetherian. Every ideal of $S^{-1}R$ is of the form $S^{-1}I$ for some ideal I of R. Since $S^{-1}I \cong S^{-1}R \otimes_R I$ it follows that $S^{-1}I$ is finitely generated over $S^{-1}R$ as I is finitely generated over R. □

A challenge:

Remark 3. Take $P(X,Y) \in \mathbb{C}[X,Y]$. Then $\mathbb{C}[X,Y]/(P(X,Y))$ is integrally closed if and only if the set $\{(a,b) \in \mathbb{C}^2 | P(a,b) = 0\}$ is a complex manifold.

Lecture 7
2015-01-28

2.4 Discrete Valuation Rings

Definition 36. A discrete valuation on a field K is a surjective function $v : K^\times \to \mathbb{Z}$ such that:

1. $v(xy) = v(x) + v(y)$ for all $x, y \in K^\times$ and
2. $v(x+y) \geq \min(v(x), v(y))$.

If we set $v(0) = \infty$ then we see that the above two properties are satisfied for all $x, y \in K$.

Example 37.
1. Take $K = \mathbb{C}(X)$ and $\alpha \in \mathbb{C}$. Define $v_\alpha(P(X)/Q(X))$ as the power of $X - \alpha$ in $R = P/Q$ written in lowest terms. It is easy to see that v_α satisfies the two conditions for valuations and is a discrete valuation.
2. More generally if $K = F(x)$ and $P(X) \in F[X]$ an irreducible polynomial let $v_P(M(X)/N(X))$ to tbe power of $P(X)$ in the rational function $M(X)/N(X)$.
3. Take $K = \mathbb{Q}$ and p a prime. Let $v_p(m/n)$ to be the power of p in m/n.

Remark 4. Let (K, v) be a discretely valued field and $\alpha \in (1, \infty)$. Define $|x| := \alpha^{-v(\alpha)}$. Then $|xy| = |x||y|$ and $|x+y| \leq \max(|x|, |y|) \leq |x| + |y|$. Thus $|\cdot|$ defines a metric space structure on K.

Lemma 38. *Let v be a discrete valuation on a field K. Then the set $\mathcal{O}_v = \{x \in K | v(x) \geq 0\}$ is a Noetherian local ring called the discrete valuation ring of v. The unique maximal ideal $\mathfrak{m}_v = \{x \in K | v(x) > 0\}$ is principal. Every proper ideal of $\mathcal{O}_v$ is of the form $\mathfrak{m}_v^n$ for some $n > 0$.*

Proof. The set $\mathcal{O}_v$ is clearly a ring and $\mathfrak{m}_v$ is clearly an ideal since $v(x+y) \geq \min(v(x), v(y))$ and $v(xy) = v(x) + v(y)$.

Suppose that $v(x) = 0$, i.e., $x \in \mathcal{O}_v - \mathfrak{m}_v$. Then $v(1/x) = -v(x) = 0$ ($v(1) = v(1^2) = 2v(1)$) so $1/x \in \mathcal{O}_v$ which implies that $\mathcal{O}_v$ is local.

The map v is surjective and if $v(a) = 1$ then for all $x \in \mathfrak{m}_v$ have $v(x/a) \geq 0$ so $\mathfrak{m}_v = (a)$.

Suppose I is an ideal of $\mathcal{O}_v$ and $x \in \mathcal{O}_v$ has minimal valuation $v(x) = k$. If $y \in I$ then $v(y) \geq v(x) = kv(a)$ so $v(y/x) \geq 0$ so $I = (x)$ is principal. Since $v(x) = v(a^k)$ it follows that x/a^k is a unit and so $I = (a^k) = \mathfrak{m}_v^k$. □

Definition 39. A **discrete valuation ring** is $\mathcal{O}_v$ for some field K and discrete valuation v.

The following proposition shows that discrete valuation rings appear naturally.

Proposition 40. *Let R be a Dedekind domain. Then $R_\mathfrak{p}$ is a discrete valuation ring for every prime ideal $\mathfrak{p}$.*

Proof. The ring $R_\mathfrak{p}$ is Noetherian and local. A prime ideal of $R_\mathfrak{p}$ is the localization of a prime ideal of R contained in $\mathfrak{p}$. Thus the localization is either 0 or $\mathfrak{p}$ since every prime ideal of R is either 0 or maximal. Finally, $R_\mathfrak{p}$ is integrally closed as R is and so $R_\mathfrak{p}$ is a discrete valuation ring by the following lemma. □

Lemma 41. *Let R be a local Noetherian integral domain with maximal ideal $\mathfrak{m}$. Suppose that $\mathfrak{m}$ is the only nonzero prime ideal of R. Then the following are equivalent.*

1. *R is a discrete valuation ring.*

2. *The maximal ideal* $\mathfrak{m}$ *is principal.*

3. *R is integrally closed.*

Proof. (1) implies (2) and (3): From the above we already know that if R is a dvr then $\mathfrak{m}$ is principal and in fact R is a PID. Thus R is integrally closed, being a UFD.

(2) implies (3): If R is a field then it is a dvr by taking $v(a) = 0$ for all $a \neq 0$. Otherwise we may choose $a \in R$, nonzero and not a unit.

Recall that $\sqrt{(a)}$ is the intersection of all maximal ideals containing (a). Since $\mathfrak{m}$ is the only maximal ideal it follows that $\sqrt{(a)} = \mathfrak{m}$. As R is Noetherian the ideal $\mathfrak{m}$ is generated by $m_1, \ldots, m_k$ (in fact by a single element as it must be principal, but we don't know this yet). Since $m_i \in \sqrt{(a)}$ it follows that $m_i^N \in (a)$ for some big enough N. Using the multinomial formula we deduce that if $u \in \mathfrak{m}$ then $u^{kN} \in (a)$ and so $\mathfrak{m}^{kN} \subset (a)$. Choose n minimal such that $\mathfrak{m}^n \subset (a)$. Since a is not a unit it follows that $n \geq 1$.

Pick $b \in \mathfrak{m}^{n-1} - (a)$ (by minimality of n). Take $x = a/b \in K$ and by construction $x^{-1} = b/a \notin R$ but $x^{-1}\mathfrak{m} \subset R$. The set $x^{-1}\mathfrak{m}$ is a submodule of R and thus an ideal. If $x^{-1}\mathfrak{m} = R$ then immediately $\mathfrak{m} = (x)$ as desired. Otherwise it is contained in the maximal ideal $x^{-1}\mathfrak{m} \subset \mathfrak{m}$. Consider the action of $A[x^{-1}]$ on $\mathfrak{m}$. Since $\mathfrak{m}$ is finitely generated the element x^{-1} satisfies the characteristic polynomial of the multiplication by x^{-1} map on this finite dimensional space and so x^{-1} would be integral. But R is integrally closed by assumption and so $x^{-1} \in R$ contradicting the choice of x.

Lecture 8
2015-01-30

---

(3) implies (1): For $a \in R - 0$ we have seen that there exists a smallest $n \geq 0$ such that $\mathfrak{m}^n \subset (a)$. Define $v(a) := n$.

Now let's check the conditions on v. Write $\mathfrak{m} = (x)$. Then $(a) \supset (x^{v(a)})$ and $v(a)$ is the largest such exponent. This implies that $a \mid x^{v(a)}$ but $a \nmid x^{v(a)-1}$, i.e., $x^{v(a)}/a \in R - \mathfrak{m}$. But then $x^{v(a)}/a = u$ is a unit and so $(a) = (x^{v(a)})$.

Suppose $a = x^m u$ and $b = x^n v$ where $0 \leq m \leq n$ and $u, v \in R^\times$. Then $v(a) = m$ and $v(b) = n$. Note that $ab = x^{m+n}uv$ with $uv \in R^\times$ and so $v(ab) = m + n$. Moreover, $a + b = x^m(u + x^{n-m}v) = x^{v(a+b)}w$ for some unit w. But then clearly $m \leq v(a + b)$. Thus v is a discrete valuation on R.

Finally, let $K = \operatorname{Frac} R$ and define $v(x/y) := v(x) - v(y)$. Then v is easily checked to be a discrete valuation on K and $R = \mathcal{O}_v$. □

3 Homological algebra

3.1 Categories and functors

Definition 42. A **category** is an algebraic structure consisting of a class of objects Ob as well as, for each $X, Y \in \text{Ob}$, a class of morphisms $\text{Hom}(X, Y)$ satisfying the following properties:

1. If $X, Y, Z \in \text{Ob}$ there exists a composition operation $\text{Hom}(X, Y) \times \text{Hom}(Y, Z) \to \text{Hom}(X, Z)$ sending $f \times g$ to $g \circ f$;

2. For morphisms $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} W$ the associativity relation $h \circ (g \circ f) = (h \circ g) \circ f$ holds;

3. For each $X \in \text{Ob}$, there exists $\text{id}_X \in \text{Hom}(X, X)$ such that for any $X \xrightarrow{f} Y$ we have $\text{id}_Y \circ f = f$ and $f \circ \text{id}_X = f$.

Example 43.

1. The category Sets whose objects are sets and morphisms are functions of sets.

2. The category Groups whose objects are groups and morphisms are group homomorphisms.

3. The category TopSpaces whose objects are topological spaces and morphisms are continuous maps.

4. The category Manifolds whose objects are manifolds and morphisms are smooth functions.

Definition 44. Let $\mathcal{C}$ be a category. A **subcategory** $\mathcal{A}$ of $\mathcal{C}$ is a category such that $\mathrm{Ob}(\mathcal{A}) \subset \mathrm{Ob}(\mathcal{C})$ and for $X, Y \in \mathrm{Ob}(\mathcal{A})$, $\mathrm{Hom}_{\mathcal{A}}(X,Y) \subset \mathrm{Hom}_{\mathcal{C}}(X,Y)$.

Example 45. 1. The category AbGroups is a subcategory of Groups.

2. The category Manifolds is a subcategory of TopSpaces.

Definition 46. A **covariant functor** $F : \mathcal{A} \to \mathcal{B}$ between two categories $\mathcal{A}$ and $\mathcal{B}$ is an assignment $F : \mathrm{Ob}(\mathcal{A}) \to \mathrm{Ob}(\mathcal{B})$ together with, for each $X, Y \in \mathrm{Ob}(\mathcal{A})$, an assignment $F : \mathrm{Hom}(X,Y) \to \mathrm{Hom}(F(X), F(Y))$ such that:

1. $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$;
2. $F(g \circ f) = F(g) \circ F(f)$.

A contravariant functor is similar except the assignment $F : \mathrm{Hom}(X,Y) \to \mathrm{Hom}(F(Y), F(X))$ is in the opposite direction.

Example 47. 1. Consider the assignment $F : \mathrm{Groups} \to \mathrm{Sets}$ sending the groups G to the set G. This is a covariant functor, called the **forgetful functor**.

2. Let R be a ring. The following are covariant functors:
   (a) $F_a(R) = (R, +)$ from Rings $\to$ AbGroups.
   (b) $F_m(R) = (R, \cdot)$ from Rings $\to$ Monoids.
   (c) $F_n(R) = (\mathrm{Nil}(R), +)$ from Rings $\to$ AbGroups. This last one needs an argument: Certainly F_n takes rings to abelian groups. Suppose $f : R \to S$ is a ring homomorphism. If $x \in \mathrm{Nil}(R)$ then $x^n = 0$ for some n in which case $0 = f(0) = f(x^n) = f(x)^n$ and so $f(x) \in \mathrm{Nil}(S)$. Thus we get a homomorphism $\mathrm{Nil}(f) : \mathrm{Nil}(R) \to \mathrm{Nil}(S)$.

3. Let Rings$'$ be the category whose objects are rings R and whose morphisms $f : R \to S$ are ring homomorphisms such that $f(1) = 1$. (Next time we'll see that this is simply the category of $\mathbb{Z}$-algebras.) Then $\mathbb{G}_m(R) := (R^\times, \cdot)$ is a covariant functor. Certainly the assignment takes rings to groups. Suppose $f : R \to S$ is a ring homomorphism such that $f(1) = 1$. If $x \in R^\times$ then $xx^{-1} = 1$ so $1 = f(1) = f(x)f(x^{-1})$ and so $f(x) \in S^\times$. This yields the group homomorphism $f : R^\times \to S^\times$ as desired.

Definition 48. Some adjectives related to functors. A covariant functor $F : \mathcal{A} \to \mathcal{B}$ is said to be:

1. **Full** if for $X, Y \in \mathrm{Ob}(\mathcal{A})$ the assignment $F : \mathrm{Hom}_{\mathcal{A}}(X,Y) \to \mathrm{Hom}_{\mathcal{B}}(F(X), F(Y))$ is surjective.
2. **Faithful** if $F : \mathrm{Hom}_{\mathcal{A}}(X,Y) \to \mathrm{Hom}_{\mathcal{B}}(F(X), F(Y))$ is injective.
3. **Essentially surjective** if for every $Y \in \mathrm{Ob}(\mathcal{B})$ there exists $X \in \mathrm{Ob}(\mathcal{A})$ such that $Y \cong F(X)$.

Example 49. 1. The subcategory AbGroups of Groups is a full subcategory in the sense that the inclusion morphism is full. Indeed, a morphism of abelian groups is just a morphism of groups that happen to be abelian.

2. Let LocRings be the category whose objects are local rings R with maximal ideal $\mathfrak{m}$, denoted $(R, \mathfrak{m})$. A morphism $f : (R, \mathfrak{m}) \to (S, \mathfrak{n})$ is a ring homomorphism $R \to S$ such that $f(\mathfrak{m}) \subset \mathfrak{n}$. Then LocRings is a subcategory of Rings but it is not full. Indeed, there exist ring homomorphism of local rings $f : R \to S$ such that f is not a local ring homomorphism, i.e., $f(\mathfrak{m}) \not\subset \mathfrak{n}$; for example, for any ring R and two prime ideals $\mathfrak{p} \subset \mathfrak{q}$ one gets (see last semester's final lectures) a ring homomorphism $f : R_{\mathfrak{q}} \to R_{\mathfrak{p}}$. The localizations are local rings but $\mathfrak{q}R_{\mathfrak{p}} = R_{\mathfrak{p}}$ and so is not included in $\mathfrak{p}R_{\mathfrak{p}}$, thus is not a local ring homomorphism.

Example 50. 1. For a ring R consider direct systems of R-modules. These form a category with morphisms $(f_i) : (M_i) \to (N_i)$ such that $\iota_{i,j} \circ f_i = f_j \circ \iota_{i,j}$ for $i \leq j$.

2. For a ring R consider inverse systems of R-modules. These form a category with morphisms $(f_i) : (M_i) \to (N_i)$ such that $\pi_{i,j} \circ f_i = f_j \circ \pi_{i,j}$ for $i \geq j$.

Example 51. Suppose $\mathcal{C}$ is a category and $X \in \mathrm{Ob}(\mathcal{C})$. One can construct two categories relative to X.

1. Define $\mathcal{C}_{\to X}$ with objects morphisms $f : Y \to X$. A morphisms $\phi : (Y \xrightarrow{f} X) \to (Z \xrightarrow{g} X)$ in this category consists of a morphism $\phi : Y \to Z$ such that $f \circ \phi = g$. When $\mathcal{C}$ is the category of topological spaces then $\mathcal{C}_{\to X}$ is the category of families of topological spaces indexed by the fixed topological space X.

2. Define $\mathcal{C}_{X \to}$ with objects morphisms $f : X \to Y$. A morphisms $\phi : (X \xrightarrow{f} Y) \to (X \xrightarrow{g} Z)$ in this category consists of a morphism $\phi : Y \to Z$ such that $\phi \circ f = g$. When $\mathcal{C}$ is the category of rings and R is a ring then $\mathcal{C}_{R \to}$ is the category of R-algebras.

3.2 Complexes of modules over a ring R

Definition 52. Let R be a ring. A **complex** over R is a sequence of R-module homomorphisms

$$\ldots \to M_{n-1} \xrightarrow{d_{n-1}} M_n \xrightarrow{d_n} M_n \to \ldots$$

such that $d_n \circ d_{n-1} = 0$. This complex is denoted $M^\bullet$.

A morphism of complexes $(f^\bullet) : M^\bullet \to N^\bullet$ is a collection of morphisms $f_n : M_n \to N_n$ such that $f_n \circ d_{n-1} = d_n \circ f_{n-1}$ for all n. This yields a category $\mathrm{Complexes}_R$ of complexes of modules over R.

Definition 53. Let $M^\bullet$ be a complex over R. The i-th cohomology of $M^\bullet$ is the R-module quotient

$$H^i(M^\bullet) = \ker d_i / \operatorname{Im} d_{i-1}$$

Example 54. Consider the two term complex $M \xrightarrow{f} N$ by which I mean $\ldots \to 0 \to M \xrightarrow{f} N \to 0 \to \ldots$ with M in degree 0 and N in degree 1. Then

$$H^i(M \to N) = \begin{cases} \ker f & i = 0 \\ \operatorname{coker} f & i = 1 \\ 0 & i \neq 0, 1 \end{cases}$$

Lemma 55. *The construction H^i is a functor* $\mathrm{Complexes}_R \to \mathrm{Mod}_R$.

Proof. We need to show that if $f^\bullet : M^\bullet \to N^\bullet$ is a morphism of complexes then we get a morphism $H^i(f^\bullet) : H^i(M^\bullet) \to H^i(N^\bullet)$ of R-modules satisfying the requirements of H^i being a functor. If $x \in H^i(M^\bullet)$ then $d_i x = 0$ and so $d_i(f_i(x)) = f_{i+1}(d_i(x)) = 0$ so $f_i(x) \in \ker d_i$ so f_i restricts to a morphism $\ker d_i \to \ker d_i$. Moreover, $f_i(d_{i-1}(y)) = d_{i-1}(f_{i-1}(y))$ so $f_i(\operatorname{Im} d_{i-1}) \subset \operatorname{Im} d_{i-1}$ and so f_i yields the quotient morpshism $H^i(M^\bullet) \to H^i(N^\bullet)$. □

Definition 56. A complex $M^\bullet$ is said to be **exact** if $H^i(M^\bullet) = 0$ for all i.

An exact sequence of complexes is a sequence of complex maps $0 \to M^\bullet \xrightarrow{f^\bullet} N^\bullet \xrightarrow{g^\bullet} P \to 0$ such that for each i, the sequence $0 \to M_i \to N_i \to P_i \to 0$ is exact.

Theorem 57. *Suppose* $0 \to M^\bullet \xrightarrow{f^\bullet} N^\bullet \xrightarrow{g^\bullet} P \to 0$ *is an exact sequence in* Complexes_R*. Then there exist* R*-module homomorphisms* $\delta^i : H^i(P^\bullet) \to H^{i+1}(M^\bullet)$ *such that the following sequence is exact:*

$$\ldots \to H^{i-1}(P^\bullet) \xrightarrow{\delta^{i-1}} H^i(M^\bullet) \xrightarrow{H^i(f^\bullet)} H^i(N^\bullet) \xrightarrow{H^i(g^\bullet)} H^i(P^\bullet) \xrightarrow{\delta^i} H^{i+1}(M^\bullet) \to \ldots$$

Proof. In class I constructed δ^i and left as an exercise that the sequence is exact. The whole proof amounts to simple diagram chasing. See, for instance, Dummit and Foote Theorem 2 on page 778. □

Lecture 10
2015-02-04

Example 58. As an application of the theorem we'll compute the de Rham cohomology of the n-sphere S^n. First, a little notation.

If M is a real manifold of dimension n then the differential forms fit in a complex:

$$\mathcal{A}_m^\bullet : 0 \to \mathcal{A}_M^0 \to \mathcal{A}_M^1 \to \ldots \mathcal{A}_M^n \to 0$$

where $\mathcal{A}_M^i$ are the real i-differential forms. For example $\mathcal{A}_M^0$ are the functions on M. Then the de Rham cohomology of M is defined as the cohomology of this complex of differentials

$$H^i_{\text{dR}}(M) := H^i(\mathcal{A}_M^\bullet)$$

It satisfies the following properties:

1. If M is connected then $H^0_{\text{dR}}(M) = \mathbb{R}$. Indeed, $H^0_{\text{dR}}(M) = \ker(d : \mathcal{A}_M^0 \to \mathcal{A}_M^1)$ and on a connected manifold the only functions with zero differential are the constant functions. [More generally $H^0(M)$ is $\mathbb{R}^k$ where k is the number of connected components of M.]
2. $H^i_{\text{dR}}(M) = 0$ if $i > \dim M$. Indeed, the complex terminates in degree n.
3. If $M \supset N$ are manifolds such that there exists a smooth retraction, i.e., a smooth function $f : M \to N$ such that $f|_N = \text{id}_N$, then $H^i_{\text{dR}}(M) = H^i_{\text{dR}}(N)$ for all i.
4. If $M = A \cup B$ for two manifolds A and B then there exists an exact sequence of complexes

$$0 \to \mathcal{A}_M^\bullet \to \mathcal{A}_A^\bullet \oplus \mathcal{A}_B^\bullet \to \mathcal{A}_{A\cap B}^\bullet \to 0$$

We're ready to show that

$$H^i_{\text{dR}}(S^n) = \begin{cases} \mathbb{R} & i = 0, n \\ 0 & i \neq 0, n \end{cases}$$

First $H^0_{\text{dR}}(S^n) = \mathbb{R}$ as S^n is connected and $H^i_{\text{dR}}(S^n) = 0$ for $i > n$. Take A to be the upper semisphere and B the lower semisphere, enlarged so that $A \cup B = S^n$. Then A has a smooth retraction to the top pole, B has a smooth retraction to the lower pole and $A \cap B$ has a smooth retraction to the equator, which is S^{n-1}.

Apply Theorem 57 to the exact sequence of complexes $0 \to \mathcal{A}_{S^n}^\bullet \to \mathcal{A}_A^\bullet \oplus \mathcal{A}_B^\bullet \to \mathcal{A}_{A\cap B}^\bullet \to 0$ to get the so-called Mayer-Vietoris long exact sequence

$$\ldots \to H^i_{\text{dR}}(S^n) \to H^i_{\text{dR}}(A) \oplus H^i_{\text{dR}}(B) \to H^i_{\text{dR}}(A \cap B) \to H^{i+1}_{\text{dR}}(S^n) \to \ldots$$

Applying the property about smooth retractions this becomes

$$\ldots \to H^i_{\text{dR}}(S^n) \to H^i_{\text{dR}}(\text{point}) \oplus H^i_{\text{dR}}(\text{point}) \to H^i_{\text{dR}}(S^{n-1}) \to H^{i+1}_{\text{dR}}(S^n) \to \ldots$$

If $i > 0$ then $H^i(\text{point}) = 0$ as the point has dimension 0 and so we see that

$$0 \to H^i_{\text{dR}}(S^{n-1}) \to H^{i+1}_{\text{dR}}(S^n) \to 0$$

and exactness implies that the connecting homomorphism must be an isomorphism. Thus $H^{i+1}_{\text{dR}}(S^n) \cong H^i(S^{n-1})$. By induction this yields the result when $1 < i \leq n$.

Finally, to compute $H^1_{\text{dR}}(S^n)$ note that the beginning of the long exact sequence is

$$0 \to \mathbb{R} \to \mathbb{R}^2 \to \mathbb{R} \to H^1_{\text{dR}}(S^n) \to 0$$

and a little diagram chasing implies that $H^1_{\text{dR}}(S^n) = 0$. Indeed, the first map is injective so the kernel of the second map is $\mathbb{R}$. The first isomorphism theorem implies that its image is also $\mathbb{R}$. But then the third map is the 0 map and so the kernel of the last map is 0, which implies that $H^1_{\text{dR}}(S^n) = 0$.

3.3 Derived functors

Definition 59. Recall that a covariant functor $F : \text{Mod}_R \to \text{Mod}_S$ is right-exact (left-exact) if for any exact sequence $0 \to M' \to M \to M'' \to 0$ the sequence

$$0 \to F(M') \to F(M) \to F(M'') \to 0$$

is right-exact (left-exact).

Definition 60. We say that a covariant functor $F : \text{Mod}_R \to \text{Mod}_R$ is **additive** if for any $M, N \in \text{Mod}_R$ the functor induces a homomorphism of abelian groups $F : \text{Hom}_R(M, N) \to \text{Hom}_S(F(M), F(N))$.

Theorem 61 (Derived functors)**.** *Suppose F is right-exact and additive from Mod_R to Mod_S. There exist functors $L_iF : \text{Mod}_R \to \text{Mod}_S$ such that for any exact sequence $0 \to M' \to M \to M'' \to 0$ the sequence*

$$\ldots L_2F(M') \to L_2F(M) \to L_2F(M'') \to L_1F(M') \to L_1F(M) \to L_1F(M'') \to F(M') \to F(M) \to F(M'') \to 0$$

is exact. The functors L_iF are the left-derived functors of F.

If F were left-exact then there would exist right-derived functors R^iF such that

$$0 \to F(M') \to F(M) \to F(M'') \to R^1F(M') \to R^1F(M) \to R^1F(M'') \to R^2F(M') \to \ldots$$

is exact.

Remark 5. The defining long exact sequence for derived functors is reminiscent of Theorem 57 and in fact our strategy of proving Theorem 61 will be to construct, for each module M, a complex $C^\bullet_M$ and then define $L_iF(M) := H^i(C^\bullet_M)$. There are two challenges:

1. To construct $C^\bullet_M$ in a way which yields the long exact sequence
2. To ensure that the definition of $L_iF(M)$ depends only on M and not on the complex $C^\bullet_M$.

In order to overcome these challenges we'll need some technical tools.

3.3.1 Chain homotopies

Definition 62. A map of complexes $f^\bullet : M^\bullet \to N^\bullet$ is said to be **null-homotopic** if there exist R-module homomorphisms $s_n : M_n \to N_{n-1}$ such that

$$f_n = s_{n+1} \circ d_n + d_{n-1} \circ s_n$$

for all n.

Two morphisms of complexes $f^\bullet$ and $g^\bullet$ are said to be **chain homotopic** if $f^\bullet - g^\bullet$ is null-homotopic.

Proposition 63. *Suppose $f^\bullet, g^\bullet : M^\bullet \to N^\bullet$ are chain homotopic. Then $H^i(f^\bullet) = H^i(g^\bullet) : H^i(M^\bullet) \to H^i(N^\bullet)$ for all i.*

Proof. Suppose $x \in H^i(M^\bullet)$. Since $f^\bullet - g^\bullet$ is null homotopic we may write $f_i - g_i$ as $s_{i+1} \circ d_i + d_{i-1} \circ s_i$. Then $f_i(x) - g_i(x) = d_{i-1}(s_i(x))$ and so $H^i(f^\bullet)(x) - H^i(g^\bullet)(x) = 0 \in H^i(N^\bullet)$. □

Corollary 64. *Suppose $M^\bullet$ is a complex such that* $\mathrm{id} : M^\bullet \to M^\bullet$ *is null-homotopic. Then $M^\bullet$ is exact.*

Proof. The previous proposition implies that $H^i(\mathrm{id}) = H^i(0)$ on $H^i(M^\bullet)$. Thus $\mathrm{id} = 0$ on $H^i(M^\bullet)$ which can only happen if $H^i(M^\bullet) = 0$, i.e., if $M^\bullet$ is exact. □

Lecture 11
2015-02-06

Lemma 65. *Suppose $f^\bullet, g^\bullet : M^\bullet \to N^\bullet$ are chain homotopics maps. If F is a covariant additive functor then $F(f^\bullet), F(g^\bullet) : F(M^\bullet) \to F(N^\bullet)$ are also chain homotopic.*

Proof. If $f = ds + sd$ then $F(f) = F(ds + sd) = F(d)F(s) + F(s)F(d)$ and $F(d)$ are the differentials on the complex $F(M^\bullet)$. □

3.3.2 Projective resolutions

Recall that a module P over R is said to be projective if the left-exact functor $\mathrm{Hom}_R(P, -)$ is in fact exact. In other words, for any surjection $A \to B \to 0$ and any $f : P \to B$ there exists $g : P \to A$ making the diagram commute. Also recall that

1. Free modules are projective.
2. In fact a module is projective if and only if it is a direct summand of a free module.
3. Projective modules are flat over R.
4. (From HW 4) Every projective module M over a ring R is locally free in the sense that $M_\mathfrak{p}$ is free for every prime ideal $\mathfrak{p}$ of R. Moreover, every finitely generated and locally free module over a Noetherian ring is in fact projective.

Definition 66. A left resolution of an R-module M is an exact sequence of the form

$$\ldots \to M_2 \to M_1 \to M_0 \to M \to 0$$

in which case we denote $M_\bullet$ the complex $\ldots \to M_2 \to M_1 \to M_0$.

Proposition 67. *Every R-module M has a projective resolution, i.e., a left resolution*

$$\ldots \to P_2 \to P_1 \to P_0 \to M$$

such that P_i are projective R-modules.

Proof. I did this in class. In fact you get a free resolution. See, for example, Dummit and Foote, the first half of page 779. □

Example 68. If R is a PID and M finitely generated then we know that M has a projective resolution of the form $0 \to R^{n-r} \to R^n \to M \to 0$ where r is the rank of M.

Proposition 69. *Let M and N be two R-modules. Suppose $\ldots \to P_2 \to P_1 \to P_0 \to M \to 0$ is a projective resolution of M and $\ldots \to Q_2 \to Q_1 \to Q_0 \to N$ is any left resolution of N. Then for any R-module homomorphism $f : M \to N$ there exist R-module homomorphisms $f_n : P_n \to Q_n$ such that*

$$\begin{array}{ccccccccccc}
\ldots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f} & & \\
\ldots & \longrightarrow & Q_2 & \longrightarrow & Q_1 & \longrightarrow & Q_0 & \longrightarrow & N & \longrightarrow & 0
\end{array}$$

is a commutative diagram.

Moreover, the map of complexes $f_\bullet : P_\bullet \to Q_\bullet$ is unique up to a chain homotopy.

Proof. We'll construct f_n by induction on n. Since P_0 is projective, the composite morphism $P_0 \to M \to N$ lifts to $f_0 : P_0 \to Q_0$.

$$\begin{array}{ccccc}
P_0 & \longrightarrow & M & \longrightarrow & 0 \\
\vdots{\scriptstyle f_0} & \searrow & \downarrow{\scriptstyle f} & & \\
Q_0 & \longrightarrow & N & \longrightarrow & 0
\end{array}$$

Suppose f_i is constructed for $i \leq n$. Let $K = \ker(P_n \to P_{n-1})$ and $L = \ker(Q_n \to Q_{n-1})$. We get a commutative diagram with exact rows

$$\begin{array}{ccccccc}
0 & \longrightarrow & K & \longrightarrow & P_n & \longrightarrow & P_{n-1} \\
 & & \vdots{\scriptstyle \phi} & \overset{j}{\searrow} & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} \\
0 & \longrightarrow & L & \xrightarrow{\iota} & Q_n & \longrightarrow & Q_{n-1}
\end{array}$$

Here the diagonal morphism j is composition. Since the bottom row is left-exact we get an exact sequence

$$0 \to \mathrm{Hom}(K, L) \xrightarrow{\iota_*} \mathrm{Hom}(K, Q_n) \xrightarrow{d_*} \mathrm{Hom}(K, Q_{n-1})$$

Note that $d_* j = d \circ j = f_{n-1} \circ d^2 = 0$ and by exactness in the middle $j = \iota_* \phi$ for some $\phi \in \mathrm{Hom}(K, L)$.

Exactness of the two resolutions implies that we also get a commutative diagram with exact rows

$$\begin{array}{ccccc}
P_{n+1} & \longrightarrow & K & \longrightarrow & 0 \\
\vdots{\scriptstyle f_{n+1}} & \searrow & \downarrow{\scriptstyle \phi} & & \\
Q_{n+1} & \longrightarrow & L & \longrightarrow & 0
\end{array}$$

and the same argument as in the $n = 0$ case yields f_{n+1}.

Now we need to show that $f_\bullet$ is uniquely defined up to homotopy. Equivalently, if $f = 0$ then we need to show that $f_\bullet$ is null homotopic. Again, we'll construct the maps $s_n : P_n \to Q_{n+1}$ by induction on n. For $n = -1$ with $P_{-1} = M$ simply take $s_{-1} = 0$. Suppose $f_n = ds_{n-1} + s_n d$. We would like to construct $s_{n+1} : P_{n+1} \to Q_{n+2}$ such that $f_{n+1} = ds_n + s_{n+1} d$.

$$\begin{array}{ccccccccc}
P_{n+2} & \longrightarrow & P_{n+1} & \longrightarrow & P_n & \longrightarrow & P_{n-1} \\
\downarrow{\scriptstyle f_{n+2}} & & \downarrow{\scriptstyle f_{n+1}} \swarrow{\scriptstyle s_n} & & \downarrow{\scriptstyle f_n} \swarrow{\scriptstyle s_{n-1}} & & \downarrow{\scriptstyle f_{n-1}} \\
Q_{n+2} & \longrightarrow & Q_{n+1} & \longrightarrow & Q_n & \longrightarrow & Q_{n-1}
\end{array}$$

Note that $df_{n+1} = f_n d = (ds_n + s_{n-1} d)d = ds_n d$ and so $d(f_{n+1} - s_n d) = 0$. This implies that $f_{n+1} - s_n d$ yields a homomorphism

$$\begin{array}{ccc}
 & & P_{n+1} \\
 & \swarrow & \downarrow{\scriptstyle f_{n+1} - s_n d} \\
Q_{n+2} & \twoheadrightarrow & \ker(Q_{n+1} \to Q_n)
\end{array}$$

where the diagonal arrow, call it s_{n+1}, exists because P_{n+1} is projective. Thus $f_{n+1} - s_n d = d s_{n+1}$ as desired.

□

3.3.3 Derived functors

We are ready to construct derived functors.

Construction of the left-derived functors from Theorem 61. Suppose F is a right-exact additive functor of R-modules.

Construction of L_iF on objects: Let M be an R-module and let $P_\bullet \to M \to 0$ be a projective resolution. Consider the complex $F(P_\bullet) : \ldots \to F(P_2) \to F(P_1) \to F(P_0)$ and define $L_iF(M) := H^i(F(P_\bullet)) = \ker(F(P_i) \to F(P_{i-1}))/\operatorname{Im}(F(P_{i+1}) \to F(P_i))$. We will show that these satisfy the requirements in the theorem.

Independence of choice of projective resolution: First, we show that $L_iF(M)$ is independent of the choice of projective resolution. Suppose $Q_\bullet \to M \to 0$ is another projective resolution. Consider the identity map $\mathrm{id} : M \to M$. The previous proposition implies the existence of maps of complexes $f_\bullet : P_\bullet \to Q_\bullet$ and $g_\bullet : Q_\bullet \to P_\bullet$ such that the following diagram commutes

$$\begin{array}{ccccccccccc}
\ldots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 \\
 & & {\scriptstyle g_2}\uparrow\downarrow{\scriptstyle f_2} & & {\scriptstyle g_1}\uparrow\downarrow{\scriptstyle f_1} & & {\scriptstyle g_0}\uparrow\downarrow{\scriptstyle f_0} & & \| & & \\
\ldots & \longrightarrow & Q_2 & \longrightarrow & Q_1 & \longrightarrow & Q_0 & \longrightarrow & M & \longrightarrow & 0
\end{array}$$

and the maps $f_\bullet$ and $g_\bullet$ are unique up to chain homotopies.

Applying the functor F yields the commutative diagram

$$\begin{array}{ccccccccccc}
\ldots & \longrightarrow & F(P_2) & \longrightarrow & F(P_1) & \longrightarrow & F(P_0) & \longrightarrow & F(M) & \longrightarrow & 0 \\
 & & {\scriptstyle F(g_2)}\uparrow\downarrow{\scriptstyle F(f_2)} & & {\scriptstyle F(g_1)}\uparrow\downarrow{\scriptstyle F(f_1)} & & {\scriptstyle F(g_0)}\uparrow\downarrow{\scriptstyle F(f_0)} & & \| & & \\
\ldots & \longrightarrow & F(Q_2) & \longrightarrow & F(Q_1) & \longrightarrow & F(Q_0) & \longrightarrow & F(M) & \longrightarrow & 0
\end{array}$$

and again the maps $F(f_\bullet)$ and $F(g_\bullet)$ are unique up to chain homotopy by Lemma 65.

Since H^i is a functor on complexes we get maps $H^i(f_i) : H^i(F(P^\bullet)) \to H^i(F(Q^\bullet))$ and $H^i(g_i) : H^i(F(Q^\bullet)) \to H^i(F(P^\bullet))$ which are now uniquely defined because null homotopic maps of complexes become the zero map on cohomology.

Next, note that $f_i \circ g_i$ lifts the identity on $M \to M$. But the identity $\mathrm{id} : P_i \to P_i$ also lifts the identity $M \to M$ and so $f_i \circ g_i$ is chain homotopic to id. But then $H^i(f_i) \circ H^i(g_i) = H^i(f_i \circ g_i) = H^i(\mathrm{id}) = \mathrm{id}$ and similarly for $H^i(g_i) \circ H^i(f_i)$. We conclude that $H^i(F(P^\bullet)) \cong H^i(F(Q^\bullet))$ are isomorphic and that this isomorphism is natural since the maps $H^i(f_i)$ and $H^i(g_i)$ are unique.

Thus $L_iF(M)$ is well-defined.

Computing L_0F: Note that $L_0F(M) = \ker(F(P_0) \to 0)/\operatorname{Im}(F(P_1) \to F(P_0))$. Since F is right-exact it follows that $F(P_1) \to F(P_0) \to F(M) \to 0$ is right-exact and so $\ker(F(P_0) \to F(M)) = \operatorname{Im}(F(P_1) \to F(P_0))$. The first isomorphism theorem then gives $L_0F(M) = F(M)$.

Lecture 12
2015-02-09

Construction of L_iF on morphisms: If $M \to N$ is a homomorphism and $P^\bullet \to M \to 0$ and $Q^\bullet \to N \to 0$ are projective resolutions then lift $M \to N$ to maps $P^\bullet \to Q^\bullet$. This map is unique up to chain homotopy and thus induces a unique map $H^i(F(P^\bullet)) \to H^i(F(Q^\bullet))$ which is the map $L_iF(M) \to L_iF(N)$ as desired. □

Theorem 70 (Derived functors)**.** *Suppose $F : \mathrm{Mod}_R \to \mathrm{Mod}_S$ is covariant, additive and right-exact.*

1. *For every exact sequence $0 \to M' \to M \to M'' \to 0$ there exists a long exact sequeence*

$$\ldots \to L_iF(M') \to L_iF(M) \to L_iF(M'') \to L_{i-1}F(M') \to \ldots \to L_1F(M'') \to F(M') \to F(M) \to F(M'') \to 0$$

2. *If*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0 \end{array}$$

is a commutative diagram with exact rows then the resulting diagram is also commutative

$$\begin{array}{ccccccccccc} \ldots & \longrightarrow & L_iF(M') & \longrightarrow & L_iF(M) & \longrightarrow & L_iF(M'') & \longrightarrow & L_{i-1}F(M') & \longrightarrow & \ldots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \ldots & \longrightarrow & L_iF(N') & \longrightarrow & L_iF(N) & \longrightarrow & L_iF(N'') & \longrightarrow & L_{i-1}F(N') & \longrightarrow & \ldots \end{array}$$

Proof. I'll prove part 1 and leave part 2 as a laborious but straightforward exercise.

Let $(P')^\bullet \to M' \to 0$ and $(P'')^\bullet \to M'' \to 0$ be projective resolutions. From homework 4 there exists a projective resolution $(P')^\bullet \oplus (P'')^\bullet \to M \to 0$ yielding a commutative diagram with exact rows and columns

$$\begin{array}{ccccc} & 0 & & 0 & \\ & \downarrow & & \downarrow & \\ & (P')^\bullet & \longrightarrow & M' & \longrightarrow 0 \\ & \downarrow & & \downarrow & \\ (P')^\bullet \oplus (P'')^\bullet & \longrightarrow & M & \longrightarrow & 0 \\ & \downarrow & & \downarrow & \\ & (P'')^\bullet & \longrightarrow & M'' & \longrightarrow 0 \\ & \downarrow & & \downarrow & \\ & 0 & & 0 & \end{array}$$

Note that F commutes with direct sums. Indeed, let i_A, i_B be the natural inclusions of A and B into $A \oplus B$ and let p_A, p_B be the natural projections. Then $F(p_A) \circ F(i_A) = F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$ and similarly for B. Consider $F(i_A) + F(i_B) : F(A) \oplus F(B) \to F(A \oplus B)$ and $F(p_A) \oplus F(p_B) : F(A \oplus B) \to F(A) \oplus F(B)$. The compositions are the identity in both directions so $F(A \oplus B) \cong F(A) \oplus F(B)$. This implies that we get the commutative diagram

$$\begin{array}{ccccc} F((P')^\bullet) & \longrightarrow & F(M') & \longrightarrow 0 \\ \downarrow & & \downarrow & \\ F((P')^\bullet) \oplus F((P'')^\bullet) & \longrightarrow & F(M) & \longrightarrow 0 \\ \downarrow & & \downarrow & \\ F((P'')^\bullet) & \longrightarrow & F(M'') & \longrightarrow 0 \end{array}$$

Finally the long exact sequence attached to the exact sequence of complexes $0 \to F((P')^\bullet) \to F((P')^\bullet) \oplus F((P'')^\bullet) \to F((P'')^\bullet) \to 0$ yields the desired long exact sequence. □

Theorem 71. *The functors in this theorem are* $\mathrm{Mod}_R \to \mathrm{Mod}_S$.

1. *If F is contravariant right-exact additive then there exist contravariant additive left-derived functors L_iF with $L_0F = F$ such that*

   (a) *For every exact sequence $0 \to M' \to M \to M'' \to 0$ there exists a long exact sequeence*

   $$\ldots \to L_iF(M'') \to L_iF(M) \to L_iF(M') \to L_{i-1}F(M'') \to \ldots \to L_1F(M'') \to F(M') \to F(M) \to F(M'') \to 0$$

   (b) *If*

   $$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0 \end{array}$$

   is a commutative diagram with exact rows then the resulting diagram is also commutative

   $$\begin{array}{ccccccccccc} \ldots & \longrightarrow & L_iF(M'') & \longrightarrow & L_iF(M) & \longrightarrow & L_iF(M') & \longrightarrow & L_{i-1}F(M'') & \longrightarrow & \ldots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \ldots & \longrightarrow & L_iF(N'') & \longrightarrow & L_iF(N) & \longrightarrow & L_iF(N') & \longrightarrow & L_{i-1}F(N'') & \longrightarrow & \ldots \end{array}$$

2. *If F is covariant left-exact additive then there exist covariant additive right-derived functors R^iF with $R^0F = F$ such that*

   (a) *For every exact sequence $0 \to M' \to M \to M'' \to 0$ there exists a long exact sequeence*

   $$\ldots \to R^iF(M') \to R^iF(M) \to R^iF(M'') \to R^{i+1}F(M') \to \ldots$$

   (b) *If*

   $$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0 \end{array}$$

   is a commutative diagram with exact rows then the resulting diagram is also commutative

   $$\begin{array}{ccccccccccc} \ldots & \longrightarrow & R^iF(M') & \longrightarrow & R^iF(M) & \longrightarrow & R^iF(M'') & \longrightarrow & R^{i+1}F(M') & \longrightarrow & \ldots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \ldots & \longrightarrow & R^iF(N') & \longrightarrow & R^iF(N) & \longrightarrow & R^iF(N'') & \longrightarrow & R^{i+1}F(N') & \longrightarrow & \ldots \end{array}$$

3. *If F is contravariant left-exact additive then there exist covariant additive right-derived functors R^iF with $R^0F = F$ such that*

   (a) *For every exact sequence $0 \to M' \to M \to M'' \to 0$ there exists a long exact sequeence*

   $$\ldots \to R^iF(M'') \to R^iF(M) \to R^iF(M') \to R^{i+1}F(M'') \to \ldots$$

   (b) *If*

   $$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0 \end{array}$$

is a commutative diagram with exact rows then the resulting diagram is also commutative

$$\begin{array}{ccccccccc} \dots & \longrightarrow & R^iF(M'') & \longrightarrow & R^iF(M) & \longrightarrow & R^iF(M') & \longrightarrow & R^{i+1}F(M'') & \longrightarrow & \dots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \dots & \longrightarrow & R^iF(N'') & \longrightarrow & R^iF(N) & \longrightarrow & R^iF(N') & \longrightarrow & R^{i+1}F(N'') & \longrightarrow & \dots \end{array}$$

Proof. For a category $\mathcal{C}$ denote $\mathcal{C}^{\text{op}}$ be the opposite category whose objects are $\text{Ob}(\mathcal{C}^{\text{op}}) = \text{Ob}(\mathcal{C})$ but such that a morphism $X \to Y$ in $\mathcal{C}^{\text{op}}$ is simply a morphism $Y \to X$ in $\mathcal{C}$.

Thus $\text{Hom}_{\mathcal{C}}(X, -) = \text{Hom}_{\mathcal{C}^{\text{op}}}(-, X)$ and $\text{Hom}_{\mathcal{C}^{\text{op}}}(X, -) = \text{Hom}_{\mathcal{C}}(-, X)$. Thus implies that projectives/injectives in $\mathcal{C}$ are the same as injectives/projectives in $\mathcal{C}^{\text{op}}$.

Suppose $F : \mathcal{C} \to \mathcal{D}$ is a functor. Let ${}^oF : \mathcal{C}^{\text{op}} \to \mathcal{D}$ be the same as F on objects and defining ${}^oF(X \to Y) = F(Y \to X)$ where the second morphism is in $\mathcal{C}$. Also define $F^o : \mathcal{C} \to \mathcal{D}^{\text{op}}$ such that $F^o(X) = F(X)$ and $F(X \to Y)$ be the corresponding morphism in the opposite category.

Note that if F is contravariant then ${}^oF$ and F^o are covariant. If F is left/right exact then F^o is right/left exact.

In class I used the notation $F^{\text{op}} =^o F^o$.

(1): Define $L_iF =^o (L_i({}^oF))$.

(2): Define $R^iF = (L_iF^{\text{op}})^{\text{op}}$.

(3): Define $R^iF = (L_iF^o)^o$.

Then all the conditions follow from the previous theorem. □

Example 72. For modules over a ring R the functor $\text{Hom}_R(M, -)$ is covariant left-exact additive while $\text{Hom}_R(-, N)$ is contravariant left-exact additive.

Lemma 73. *Let R be a ring, F covariant right-exact additive and G covariant left-exact additive.*

1. *If P is projective then $L_nF(P) = 0$ for $n \geq 1$.*
2. *If R is a PID then $L_nF(M) = 0$ for $n \geq 2$ for all finitely generated M.*
3. *If $R = \mathbb{Z}$ then $L_nF(M) = 0$ for $n \geq 2$ without restrictions on M.*
4. *If I is injective then $R^nG(I) = 0$ for $n \geq 1$.*
5. *If R is a PID then $R^nG(M) = 0$ for $n \geq 2$ and all M.*
6. *If F is exact then $L_nF = 0$ and $R^nF = 0$ for all $n \geq 1$.*

Proof. (1): Consider the projective resolution $\dots \to 0 \to P \to P \to 0$. Then $L_nF(P) = H^n(F(\dots \to 0 \to P))$ which vanishes for $n \geq 1$.

(2): If M is finitely generated over R a PID then M sits in an exact sequence $0 \to R^a \to R^b \to M \to 0$ which is a free and so projective resolution. Then $L_nF(M) = H^n(F(\dots 0 \to R^a \to R^b))$ which vanishes for $n \geq 2$.

(3): If $R = \mathbb{Z}$ take N the free abelian group generated by elements of M and the surjection $N \to M \to 0$. From last semester: every subgroup of a free abelian group is free abelian and so we have a free resolution $0 \to K \to N \to M \to 0$. The argument from (2) yields the vanishing result again.

(4): By definition $R^nF(I) = (L_nF^{\text{op}})^{\text{op}}(I) = L_nF^{\text{op}}(I)$. But I is now an object in the opposite category where it is projective. Part (1) this yields $R^nF(I) = 0$ for $n \geq 1$.

(5): Recall from last semester that injective over PID is equivalent to divisible. From the homework every R module injects into an injective R-module so $0 \to M \to I_0$. The cokernel is also divisible and so injective. Thus $0 \to M \to I_0 \to I_1 \to 0$ is an injective resolution in Mod_R which yields a projective resolution in the opposite category. The argument from (3) then gives $R^nF(M) = 0$ for $n \geq 2$.

(6): Suppose $P^\bullet \to M \to 0$ is a projective resolution with differentials $d_i : P_i \to P_{i-1}$. Then for each $i \geq 1$ we have the exact sequence $0 \to \ker d_i \to P_i \xrightarrow{d_i} \operatorname{Im} d_i \to 0$ yielding $0 \to F(\ker d_i) \to F(P_i) \xrightarrow{F(d_i)} F(\operatorname{Im} d_i) \to 0$. This is also exact as F is exact and so $F(\ker d_i) = \ker F(d_i)$ and $F(\operatorname{Im} d_i) = \operatorname{Im} F(d_i)$.

In the complex $F(P^\bullet)$ note that $\operatorname{Im} F(d_{i+1}) = F(\operatorname{Im} d_{i+1}) = F(\ker d_i) = \ker F(d_i)$ so $F(P^\bullet)$ is also exact, except in degree $i = 0$. Thus $L_n F(M) = 0$ for $n \geq 1$. For $R^n F$ use injective resolutions instead. □

3.4 Tor and Ext

3.4.1 Definitions

I skipped the proofs in this section since they are elaborated exercises in the diagram chases of double complexes, which, while straightforward, we haven't discussed.

Proposition 74. *Let R be a ring and M and N two R-modules. Recall that $M \otimes_R -$ and $- \otimes_R N$ are covariant right-exact additive. Then*

$$L_n(M \otimes_R -)(N) \cong L_n(- \otimes_R N)(M)$$

and this common module is denoted $\operatorname{Tor}_n^R(M, N)$.

Corollary 75. *Since $M \otimes_R N \cong N \otimes_R M$ we get an isomorphism $\operatorname{Tor}_n^R(M, N) \cong \operatorname{Tor}_n^R(N, M)$ for all n.*

Proposition 76. *Let R be a ring and M and N two R-modules. Recall that $\operatorname{Hom}_R(M, -)$ is covariant left-exact additive while $\operatorname{Hom}_R(-, N)$ is contravariant left-exact additive. Then*

$$R^n \operatorname{Hom}_R(M, -)(N) \cong R^n \operatorname{Hom}_R(-, N)(M)$$

and this common module is denoted $\operatorname{Ext}_R^n(M, N)$.

3.4.2 Basic properties

Proposition 77.

1. *If $r \in R$ is not a zero divisor then $\operatorname{Tor}_1^R(R/(r), M) = M[r] := \{m \in M | rm = 0\}$ while $\operatorname{Tor}_n^R(R/(r), M) = 0$ for $n \geq 2$.*
2. *If $I \subset R$ is an ideal then $\operatorname{Tor}_1^R(I, M) = \ker(I \otimes_R M \to M)$ where the map is the natural multiplication map.*
3. *If M is flat over R then $\operatorname{Tor}_n^R(M, N) = 0$ for all $n \geq 1$ and N.*
4. *If $\operatorname{Tor}_1^R(M, N) = 0$ for all N then M is flat over R.*

Proof. (1): Since r is not a zero divisor we get the free resolution $\ldots \to 0 \to R \xrightarrow{\times r} R \to R/(r) \to 0$. Immediately we get vanishing in degrees $n \geq 2$. The long exact sequence yields

$$0 \to \operatorname{Tor}_1^R(R/(r), M) \to M \xrightarrow{\times r} M \to M/rM \to 0$$

and the isomorphism follows.

(2): Consider the exact sequence $0 \to I \to R \to R/I \to 0$. This is no longer a projective resolution in general and so there's no vanishing in degrees $n \geq 2$. But again $0 \to \operatorname{Tor}_1^R(R/I, M) \to I \otimes_R M \to M$ is exact and the isomorphism follows.

(3): If M is flat then $M \otimes_R -$ is exact and so the left-derived functors vanish.

(4): If $0 \to N' \to N \to N'' \to 0$ is exact then the long exact sequence

$$\ldots \to \operatorname{Tor}_1^R(M, N'') \to N' \otimes_R M \to N \otimes_R M \to N'' \otimes_R M \to 0$$

yields exactness of $M \otimes_R -$ because of the vanishing of $\operatorname{Tor}_1^R(M, -)$. □

Example 78. Let $I = (x, y) \subset R = \mathbb{C}[x, y]$. Then I is not flat over R. In homework 5 you'll show that $\operatorname{Tor}_1^R(I, R/I) \cong \operatorname{Tor}_2^R(R/I, R/I) \cong \mathbb{C}$. This procedure is known as dimension shifting.

Proposition 79 (Dimension shifting)**.** *Suppose F is covariant additive right-exact. Let M be an R-module and $0 \to K \to P \to M \to 0$ an exact sequence with P projective. Then*

$$L_n F(M) \cong L_{n-1} F(K)$$

for $n \geq 2$.

Proof. For $n \geq 2$ the long exact sequence gives

$$\ldots \to L_n F(K) \to L_n F(P) \to L_n F(M) \to L_{n-1} F(K) \to L_{n-1} F(P) \to \ldots$$

and the result follows since left-derived functors vanish on projectives in degree ≥ 1. □

Proposition 80. *1. If $r \in R$ is not a zero divisor then $\operatorname{Ext}_R^n(R/(r), M) = 0$ for $n \geq 2$ and $\operatorname{Ext}_R^1(R/(r), M) \cong M/rM$.*

2. If P is projective and I is injective then $\operatorname{Ext}_R^n(P, -) = 0$ and $\operatorname{Ext}_R^n(-, I) = 0$ for $n \geq 1$.

Proof. (1): The long exact sequence of $\operatorname{Hom}_R(-, M)$ attached to $0 \to R \xrightarrow{\times r} R \to R/(r) \to 0$ gives

$$0 \to \operatorname{Hom}_R(R/(r), M) \to \operatorname{Hom}_R(R, M) \xrightarrow{\times r} \operatorname{Hom}_R(R, M) \to \operatorname{Ext}_R^1(R/(r), M) \to \operatorname{Ext}_R^1(R, M)$$

Since R is projective we get that $\operatorname{Ext}_R^1(R, M) = 0$ and so $\operatorname{Ext}_R^1(R/(r), M) = \operatorname{Hom}_R(R, M)/r \operatorname{Hom}_R(R, M)$. Since $\operatorname{Hom}_R(R, M) \cong M$ the result follows.

(2): Follows from the fact that the two ext groups are right derived functors of the exact functors $\operatorname{Hom}_R(P, -)$ and $\operatorname{Hom}_R(-, I)$. □

3.4.3 Ext and extensions

Definition 81. Let R be a ring and M and N two R-modules. An extension of M by N is an exact sequence of R-modules

$$0 \to N \xrightarrow{i} X \xrightarrow{j} M \to 0$$

An isomorphism of extensions is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & X & \longrightarrow & M & \longrightarrow & 0 \\ & & \| & & \downarrow & & \| & & \\ 0 & \longrightarrow & N & \longrightarrow & Y & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

Denote $\mathcal{EXT}_R(M, N)$ the isomorphism classes of extensions.

Theorem 82. *There is a bijection between $\mathcal{EXT}_R(M, N)$ and $\operatorname{Ext}_R^1(M, N)$.*

Lecture 14
2015-02-13

Example 83. Suppose we want to count the extensions of $\mathbb{Z}/p\mathbb{Z}$ by itself, i.e., exact sequences of the form $0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0$ as $\mathbb{Z}$-modules. (This is related to representation theory where such extensions are reducible 2-dimensional representations of the finite group $\mathbb{Z}/p\mathbb{Z}$ over the field $\mathbb{F}_p$.) To count the number of extensions we find the cardinality of $\operatorname{Ext}_{\mathbb{Z}}^1(\mathbb{Z}/p, \mathbb{Z}/p) \cong (\mathbb{Z}/p)/p(\mathbb{Z}/p) = \mathbb{Z}/p$, which is p.

Proof of Theorem. We will construct two maps $\theta : \mathcal{EXT}_R(M,N) \to \mathrm{Ext}^1_R(M,N)$ and $\xi : \mathrm{Ext}^1_R(M,N) \to \mathcal{EXT}_R(M,N)$ such that $\theta \circ \xi = \mathrm{id}$ and $\xi \circ \theta = \mathrm{id}$ which yields the required bijection.

Construction of θ: Suppose $\mathcal{E} : 0 \to N \to X \to M \to 0$ is an extension. Taking $\mathrm{Hom}_R(M,-)$ yields

$$\ldots \to \mathrm{Hom}_R(M,M) \xrightarrow{\delta} \mathrm{Ext}^1_R(M,N) \to \ldots$$

and define $\theta(\mathcal{E}) = \delta(\mathrm{id}_M)$.

Construction of ξ: Let $0 \to K \xrightarrow{i} P \xrightarrow{j} M \to 0$ be an exact sequence with P projective. Taking $\mathrm{Hom}_R(-,N)$ gives

$$\ldots \to \mathrm{Hom}_R(K,N) \to \mathrm{Ext}^1_R(M,N) \to \mathrm{Ext}^1_R(P,N) \to \ldots$$

Since P is projective $\mathrm{Ext}^1_R(P,N) = 0$ and so $\mathrm{Hom}_R(K,N) \to \mathrm{Ext}^1_R(M,N)$ is a surjection. For $\alpha \in \mathrm{Ext}^1_R(M,N)$ we can find $\beta : K \to N$ projecting to α.

Define $X = \mathrm{coker}(K \xrightarrow{i\oplus(-\beta)} P \oplus N)$, $N \to X$ via $n \mapsto 0 \oplus n$, $P \to X$ via $p \mapsto p \oplus 0$ and $X \to M$ via $p \oplus n \mapsto j(p)$. All but the last map are clearly R-module homomorphisms. For the last one we only need to check it is well-defined, which follows since $i(k) \oplus -\beta(k)$ maps to $j(i(k)) = 0$.

It is straightforward to check that the following diagram is commutative with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K & \xrightarrow{i} & P & \xrightarrow{j} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \beta} & & \downarrow & & \| & & \\
0 & \longrightarrow & N & \longrightarrow & X & \longrightarrow & M & \longrightarrow & 0
\end{array}$$

Define $\xi(\alpha)$ as the bottom extension. I left it as an exercise to check that different lifts β of α yield isomorphim extensions.

Checking $\xi \circ \theta = \mathrm{id}$: Start with $0 \to N \to X \to M \to 0$.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K & \xrightarrow{i} & P & \xrightarrow{j} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \zeta} & & \| & & \\
0 & \longrightarrow & N & \xrightarrow{u} & X & \xrightarrow{v} & M & \longrightarrow & 0
\end{array}$$

Here $\zeta : P \to X$ is a lift of $\mathrm{id}_M \circ j$ which exists since P is projective. Next, $\mathrm{Hom}_R(K,-)$ is left-exact and so

$$\mathrm{Hom}_R(K,N) \to \mathrm{Hom}_R(K,X) \to \mathrm{Hom}_R(K,M)$$

is exact. Note that $v_*(\zeta \circ i) = v(\zeta(i)) = j(i) = 0$ and by exactness $\zeta \circ i = u_*(\beta)$ for some $\beta : K \to N$.

Then $P \oplus N \xrightarrow{\zeta+u} X$ is surjective. Indeed, let $x \in X$. By surjectivity of j there is $p \in P$ such that $j(p) = v(x)$ and so $u(x - \zeta(p)) = 0$ which implies that $x - \zeta(p) \in \mathrm{Im}\, u$ as desired. What is the kernel? If $\zeta(p) + u(n) = 0$ then $v(\zeta(p)) = 0$ so $j(p) = 0$ so $p = i(k)$ for some $k \in K$. Moreover, $u(n) = -\zeta(i(k)) = -u(\beta(k))$ so by injectivity of u we get $n = -\beta(k)$. We get the exact sequence $0 \to K \xrightarrow{i\oplus-\beta} P \oplus N \to X \to 0$.

Thus the original extension is isomorphic to the above construction attached to the map β. It is an elaborate exercise to check that in fact β is a lift of $\theta(\mathcal{E}) = \delta(\mathrm{id}_M)$.

Similarly, I left as an exercise that $\theta \circ \xi = \mathrm{id}$.

□

Remark 6. In fact $\mathcal{EXT}_R(M,N)$ can be made into an R-module in which case one gets $\mathcal{EXT}_R(M,N) \cong \mathrm{Ext}^1_R(M,N)$ as an isomorphism of R-modules by showing that θ and ξ are R-module homomorphisms.

Remark 7. In fact one can show that there is a bijection (and in fact an R-module homomorphism, suitably defined) between $\mathrm{Ext}^n_R(M,N)$ and isomorphism classes of exact sequences

$$0 \to N \to X_n \to \ldots \to X_1 \to M \to 0$$

3.4.4 More properties of Tor and Ext

I didn't prove any of the statements in this section. The applications are more interesting than the proofs.

Proposition 84.

$$\operatorname{Tor}_n^R(M, \varinjlim N_i) = \varinjlim \operatorname{Tor}_n^R(M, N_i)$$
$$\operatorname{Tor}_n^R(M, \bigoplus N_i) = \bigoplus \operatorname{Tor}_n^R(M, N_i)$$

Corollary 85. *If A is an abelian group then $\operatorname{Tor}_1^{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, A) = A_{\text{tors}}$.*

Proof. Recall from last semester that $\mathbb{Q}/\mathbb{Z} = \varinjlim \mathbb{Z}/n\mathbb{Z}$ and so

$$\begin{aligned}\operatorname{Tor}_1^{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, A) &\cong \operatorname{Tor}_1^{\mathbb{Z}}(\varinjlim \mathbb{Z}/n\mathbb{Z}, A)\\ &\cong \varinjlim \operatorname{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)\\ &\cong \varinjlim A[n]\\ &\cong A_{\text{tors}}\end{aligned}$$

where the last line comes from the midterm last semester. □

Lecture 15
2015-02-16

Proposition 86. *Suppose R is commutative and S is a flat R-algebra. Then*

$$S \otimes_R \operatorname{Tor}_n^R(M, N) \cong \operatorname{Tor}_n^S(M \otimes_R S, N \otimes_R S)$$

Corollary 87. *If R is commutative and $\mathfrak{p} \subset R$ is a prime ideal then $\operatorname{Tor}_n^R(M,N)_{\mathfrak{p}} \cong \operatorname{Tor}_n^{R_{\mathfrak{p}}}(M_{\mathfrak{p}}, N_{\mathfrak{p}})$. Moreover, $\operatorname{Tor}_n^R(M,N) = 0$ if and only if $\operatorname{Tor}_n^{R_{\mathfrak{p}}}(M_{\mathfrak{p}}, N_{\mathfrak{p}}) = 0$ for all prime ideals $\mathfrak{p}$.*

Proof. It follows from the proposition applied to the flat R-algebra $R_{\mathfrak{p}}$ recalling that localization at $\mathfrak{p}$ is $\otimes_R R_{\mathfrak{p}}$. The last statement follows from the fact that "a module is 0" is a local property. □

Proposition 88.

$$\operatorname{Ext}_R^n(\bigoplus M_i, N) \cong \prod \operatorname{Ext}_R^n(M_i, N)$$
$$\operatorname{Ext}_R^n(M, \prod N_i) \cong \prod \operatorname{Ext}_R^n(M, N_i)$$

Remark 8. Ext does not commute with limits. For example, note that $\mathbb{Q} = \varinjlim \mathbb{Z}$ (homework 7 last semester) and $\operatorname{Ext}_{\mathbb{Z}}^1(\mathbb{Z}, \mathbb{Z}) = 0$ as $\mathbb{Z}$ is projective. However, $\operatorname{Ext}_{\mathbb{Z}}^1(\mathbb{Q}, \mathbb{Z})$ is not zero. In fact it is isomorphic to $\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Q}$ where $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$. This last group is deeply connected with number theory: $\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$ forms a locally compact Hausdorff topological ring called the finite adeles which is at the core of modern number theory.

Example 89. I claim that if A is a torsion abelian group then

$$\operatorname{Ext}_{\mathbb{Z}}^n(A, \mathbb{Z}) = \begin{cases} 0 & n \neq 1 \\ \operatorname{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}) & n = 1 \end{cases}$$

and the RHS in degree 1 is simply the dual group.

Proof. Consider $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. Since $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are divisible groups they are injective $\mathbb{Z}$-modules and so we immediately get vanishing of Ext in degree ≥ 2. The long exact sequence is

$$0 \to \operatorname{Hom}(A, \mathbb{Z}) \to \operatorname{Hom}(A, \mathbb{Q}) \to \operatorname{Hom}(A, \mathbb{Q}/\mathbb{Z}) \to \operatorname{Ext}^1(A, \mathbb{Z}) \to \operatorname{Ext}^1(A, \mathbb{Q}) = 0$$

Since A is torsion any homomorphism into a torsion-free group must be trivial. Thus $\operatorname{Hom}(A, \mathbb{Q}) = 0$ and $Ext_{\mathbb{Z}}^0(A, \mathbb{Z}) = \operatorname{Hom}(A, \mathbb{Z}) = 0$. The exact sequence then implies $\operatorname{Ext}_{\mathbb{Z}}^1(A, \mathbb{Z}) \cong \operatorname{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$. □

Proposition 90. *Suppose R is commutative and Noetherian and M is finitely generated. Then*

$$\operatorname{Ext}^n_R(M,N)_{\mathfrak{p}} \cong \operatorname{Ext}^n_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}, N_{\mathfrak{p}})$$

As a result if M is finitely generated then $\operatorname{Ext}^n_R(M,N) = 0$ is a local property, as in the case of Tor.

3.4.5 Intersection numbers

Suppose we want to answer the following question: how many points of intersection do two plane curves have? We'd like an answer that is algebraically formulated in sufficient generality that it can account for multiple points of intersection (for example $y^2 = x^2(x+1)$ and $x = 0$ intersecting at the origin in a double point) as well as curves with multiplicity (e.g., the double line $x = 0$ intersects the triple line $y = 0$ in 6 points).

The answer is provided by the following theorem.

Theorem 91. *Suppose R is a localization of $\mathbb{C}[x_1, \ldots, x_n]$ in which case it is a local Noetherian ring with maximal ideal $\mathfrak{m}$ (more generally R is allowed to be any regular local ring). Let $I, J \subset \mathfrak{m}$ be ideals such that $I + J$ contains some power of $\mathfrak{m}$. Let $k = R/\mathfrak{m}$ be the residue field.*

1. *Then $\operatorname{Tor}^R_n(R/I, R/J)$ is a finite dimensional k-vector space.*
2. *The expression*
$$I \cdot J = \sum (-1)^n \dim_k \operatorname{Tor}^R_n(R/I, R/J)$$
is a finite sum called the intersection number of I and J.

Example 92. 1. Let's compute $(x) \cdot (y)$ in $R = \mathbb{C}[x,y]_{(x,y)}$. We already know that

$$\operatorname{Tor}^R_n(R/(x), R/(y)) = \begin{cases} R/(x) \otimes_R R/(y) & n = 0 \\ (R/(y))[x] & n = 1 \\ 0 & n \geq 2 \end{cases}$$

since the ideals are principal. But $(R/(y))[x] = 0$ since a polynomial times x is divisible by y iff the polynomial is divisible by y ($\mathbb{C}[x,y]$ is a UFD). Also $R/(x) \otimes_R R/(y)$ is the cokernel of $R/(x) \xrightarrow{\times y} R/(x)$ (tensor with $R/(x)$ the exact sequence $0 \to R \to R \to R/(y) \to 0$) and so the tensor product is $R/(x,y) \cong k$. Thus the intersection number is 1.

2. Let's compute $(x^2) \cdot (y^3)$ (the double vertical axis intersecting the triple horizontal axis). Again the higher Tor groups all vanish and

$$(x^2) \cdot (y^3) = \dim_k R/(x^2) \otimes_R R/(y^3) = \dim_k R/(x^2, y^3)$$

But $R/(x^2, y^3)$ consists of polynomials with no x^2 or y^3 and visibly this is 6-dimensional over $k = \mathbb{C}$. Thus $(x^2) \cdot (y^3) = 6$.

Lecture 16
2015-02-18

---

3. How many times do $y^2 = x^2(x+1)$ and $x = 0$ intersect at the origin? Let's take again R to be $\mathbb{C}[x,y]_{(x,y)}$, $I = (y^2 - x^2(x+1))$ and $J = (x)$. Again all Tor groups vanish so we have

$$(f) \cdot (g) = \dim_{\mathbb{C}} R/(y^2 - x^2(x+1), x) = \dim_{\mathbb{C}} R/(x, y^2) = \dim_{\mathbb{C}} \mathbb{C}[y]/(y^2) = 2$$

Proof of Theorem. (1): Note that $\mathrm{Tor}_1^R(R/I, R/J)$ is the kernel of multiplication $R/J \otimes_R I \to R/J$ and so is annihilated by I and similarly by J. We'll show that in fact $\mathrm{Tor}_n^R(R/I, R/J)$ is annihilated by both I and J. Suppose $a \in J$. Then for a module M multiplication by a is the zero map on $M \otimes_R R/J \to M \otimes_R R/J$. Let $P^\bullet \to M \to 0$ be a projective resolution. We already know that the multiplication by a map on M extends to maps on $P^\bullet$ which has to be chain homotopic to the natural multiplication by a map on $P^\bullet$. Thus multiplication by a on M yields multiplication by a on the cohomology of the complex $P^\bullet \otimes_R R/J$. But $a = 0$ in R/J so this multiplication by a map is the 0 map on the complex and thus on the cohomology of the complex. Thus multiplication by a annihilates $H^n(P^\bullet \otimes_R R/J) = \mathrm{Tor}_n^R(M, R/J)$.

Thus $\mathrm{Tor}_n^R(R/I, R/J)$ is annihilated by $I + J$ and thus by a power $\mathfrak{m}^n$ for some n. It is also finitely generated over R and thus there is a surjection from a finite power of $R/\mathfrak{m}^n$, and so it is a finite dimensional k-vector space.

(2): This would require too much extra work. Suffices to say that localizations of $\mathbb{C}[x_1, \ldots, x_n]$ and regular local rings in general have finite global dimension which implies that $\mathrm{Tor}_n^R(M, N) = 0$ for n large enough. □

Lemma 93. *Suppose R is a commutative Noetherian ring and M, N finitely generated R-modules. Then $\mathrm{Tor}_n^R(M, N)$ are finitely generated R-modules.*

Proof. I'll prove this by induction on n. Consider $0 \to K \to R^n \to M \to 0$ be an exact sequence which exists as M is finitely generated. Then $\mathrm{Tor}_1^R(M, N) \subset K \otimes_R N$.

Now R^n is Noetherian since R is a Noetherian ring so $K \subset R^n$ is Noetherian. This implies that it is finitely generated so $K \otimes_R N$ is finite generated and thus Noetherian. Again Tor_1, being a submodule of a Noetherian module must be Noetherian and thus finitely generated.

Finally, for $n \geq 2$, the long exact sequence gives $\mathrm{Tor}_n^R(M, N) \cong \mathrm{Tor}_{n-1}^R(K, N)$. Since K and N are finitely generated this yields the inductive step. □

3.5 Representable functors

Suppose $\mathcal{C}$ is a **locally small** category by which I mean any category such that $\mathrm{Hom}_\mathcal{C}(X, Y)$ is a set for any two objects X and Y. Then given a fixed $X \in \mathrm{Ob}(\mathcal{C})$ the functor $F = \mathrm{Hom}_\mathcal{C}(X, -)$ is a covariant functor $F : \mathcal{C} \to \mathrm{Sets}$. There so-called Hom functors are very useful because instead of being abstract functors one can think of them as the object X. This is particularly useful in geometry.

In order to study these Hom functors and their special role in category theory we first define natural transformations of functors which play the role of morphisms of functors.

Definition 94. If $F, G : \mathcal{A} \to \mathcal{B}$ are two covariant functors a **natural transformation** $\Phi : F \to G$ is a collection of morphisms $\{\Phi_X : F(X) \to G(X) | X \in \mathrm{Ob}(\mathcal{A})\}$ such that if $f : X \to Y$ is any morphism in $\mathcal{A}$ then the following diagram commutes:

$$\begin{array}{ccc} F(X) & \xrightarrow{F(f)} & F(Y) \\ \downarrow{\scriptstyle \Phi_X} & & \downarrow{\scriptstyle \Phi_Y} \\ G(X) & \xrightarrow{G(f)} & G(Y) \end{array}$$

Example 95. I forgot, please remind me.

Theorem 96 (Yoneda's lemma)**.** *Suppose $F : \mathcal{C} \to$ Sets is any covariant functor. Then for any object $X \in \mathcal{C}$ there is a bijection between the set $F(X)$ and the set of natural transformations from the functor $\mathrm{Hom}_\mathcal{C}(X, -)$ to the functor F.*

Proof. Given an element $u \in F(X)$ one defines Φ as a natural transformation from the functor $\mathrm{Hom}_\mathcal{C}(X, -)$ to the functor F as follows. For each object Y we need to give a morphism $\Phi_Y : \mathrm{Hom}_\mathcal{C}(X, Y) \to F(Y)$. Since $f : X \to Y$ then $F(f) : F(X) \to F(Y)$ and we define $\Phi_Y(f) = F(f)(u)$. I leave it a diagram chasing exercise to check that this yields a natural transformation.

Given a natural transformation Φ we note that $\Phi_X : \mathrm{Hom}_{\mathcal{C}}(X, X) \to F(X)$ is a morphism and we attach to Φ the element $\Phi_X(\mathrm{id}_X) \in F(X)$. This is well-defined.

I leave it as an exercise that these two constructions are inverses to each other and thus yield bijections. □

Remark 9. If F were contravariant then the same result holds if we replace $\mathrm{Hom}_{\mathcal{C}}(X, -)$ with $\mathrm{Hom}_{\mathcal{C}}(-, X)$. (This is what happens in geometry.)

Lecture 17
2015-02-20

Definition 97. A covariant functor $F : \mathcal{C} \to \mathrm{Sets}$ is said to representable if there exists an object $X \in \mathrm{Ob}(\mathcal{C})$ and $u \in F(X)$ such that the natural transformation $\mathrm{Hom}_{\mathcal{C}}(X, -) \to F$ attached to u is a natural bijection. In other words for each Y we want $\mathrm{Hom}_{\mathcal{C}}(X, Y) \to F(Y)$ attaching to $f : X \to Y$ the element $F(f)(u)$ to be a bijection of sets. In this case we say that F is represented by (X, u) which is then the universal object.

Example 98. From now on Rings is the category of rings where homomorphisms take 1 to 1.

1. Consider the forgetful functor $F : \mathrm{Groups} \to \mathrm{Sets}$ sending the group G to the underlying set G. Then F is a covariant functor which is represented by $(\mathbb{Z}, 1)$. Indeed, we note that if $f : \mathbb{Z} \to G$ is a group homomorphism then $F(f) = f$ as a function of sets $\mathbb{Z} \to G$. We need to check that $\mathrm{Hom}_{\mathrm{Groups}}(\mathbb{Z}, G) \to G$ sending f to $f(1)$ is a bijection. Note that $f(n) = f(1)^n$ for all n so the map is bijective.

2. Consider the forgetful functor $F : \mathrm{Rings} \to \mathrm{Sets}$ sending the ring R to the set R. Then F is represented by $(\mathbb{Z}[X], X)$. Again if $f : \mathbb{Z}[X] \to R$ then $F(f) = f$ as a function of sets. We need to check that $\mathrm{Hom}_{\mathrm{Rings}}(\mathbb{Z}[X], R) \to R$ sending f to $f(X)$ is a bijection. Since $f(1) = 1$ it follows that for every polynomial $P(X)$ we have $f(P(X)) = P(f(X))$ so f is uniquely defined by $f(X)$ and so the natural transformation is a bijection.

3. Consider the functor $F : \mathrm{Rings} \to \mathrm{Sets}$ sending the ring R to the set of units $R^\times$. We already know that this is a covariant functor. It is represented by $(\mathbb{Z}[X, X^{-1}], X)$. Again $F(f) = f$ for any ring homomorphism f. We need to check that $\mathrm{Hom}_{\mathrm{Rings}}(\mathbb{Z}[X, X^{-1}], R) \to R$ sending f to $f(X)$ yields a bijection. First, $X \in \mathbb{Z}[X, X^{-1}]^\times$ and so $f(X) \in R^\times$. Moreover, if $P(X, X^{-1})$ is any polynomial then, as $f(1) = 1$, we have $f(P(X, X^{-1})) = P(f(X), f(X)^{-1})$ and so f is uniquely defined by $f(X)$. We deduce the natural transformation yields a bijection.

4. If R is a commutative ring and M and N are R-modules then the functor $F : \mathrm{Mod}_R \to \mathrm{Sets}$ sending P to the set of R-bilinear maps $M \times N \to P$ yields a covariant functor $\mathrm{Bil}_R(M \times N, -)$. It is represented by $M \otimes_R N$ and the natural bilinear map $M \times N \to M \otimes_R N$ sending $m \times n \mapsto m \otimes n$. Indeed, we know that $\mathrm{Hom}_R(M \otimes_R N, P) \cong \mathrm{Bil}_R(M \times N, P)$ not only as sets but also as R-modules.

5. The functor attaching to P the set of k-linear maps $M^k \to P$ is represented by $M^{\otimes k}$.

6. The functor attaching to P the set of symmetric k-linear maps $M^k \to P$ is represented by $\mathrm{Sym}^k M$.

7. The functor attaching to P the set of skew-symmetric k-linear maps $M^k \to P$ is represented by $\wedge^k M$.

8. The functor Nil : Rings $\to$ Sets attaching to R the set $\mathrm{Nil}(R)$ of nilpotents in not representable. Suppose it were, by a ring R and a universal nilpotent element $u \in \mathrm{Nil}(R)$. Then for some n one has $u^n = 0$. Since Nil is represented by (R, u) for any ring S one has $\mathrm{Hom}_{\mathrm{Rings}}(R, S) \to \mathrm{Nil}(S)$ sending $f : R \to S$ to $f(u)$ is a bijection. Take $S = \mathbb{Z}[x]/(x^{n+1})$. Then $x \in S$ is clearly nilpotent and so for some $f : R \to S$ one has $f(u) = x$. But then $x^n = f(u)^n = f(u^n) = f(0) = 0$ which is not true in S.

9. Consider the matrix $T_0 = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$ over $\mathbb{C}$. Recall from homework that the functor Def attaching to a $\mathbb{C}$-algebra R with residue field $\mathbb{C}$ the set of rank 2 free R-modules V and endomorphisms $T \in \mathrm{End}_R(V)$

such that $T \otimes_R \mathrm{id}_{\mathbb{C}} = T_0$ is a covariant functor. I claim it is represented by the universal object $(R, V = R^2, T)$ where $R = \mathbb{C}[x,y,z,t]_{(x,y,z,t)}$ and $T = \begin{pmatrix} 1+x & 1+y \\ z & 1+t \end{pmatrix}$. First, note that R is local with maximal ideal $\mathfrak{m}_R = (x,y,z,t)$ and residue field $R/\mathfrak{m}_R = \mathbb{C}$ and $T \otimes_R R/\mathfrak{m}_R = T_0$. We need to check that for any $\mathbb{C}$-algebra S with residue field $\mathbb{C}$ there is a bijection $\mathrm{Hom}_{\mathbb{C}}(R,S) \to \mathrm{Def}(S)$ sending f to $f(T)$. Next, every $\mathbb{C}$-algebra homomorphism f is uniquely determined by $f(x), f(y), f(z), f(t)$ so the assignment $f \mapsto f(T)$ uniquely defines f. Finally, if $T_S \in \mathrm{End}_S(S^2)$ is such that $T_S \otimes_S S/\mathfrak{m}_S = T_0$ then $T_S = \begin{pmatrix} 1+b & 1+b \\ c & a+d \end{pmatrix}$ for some $a,b,c,d \in \mathfrak{m}_S$ and so setting $f(x) = a, f(y) = b, f(z) = c, f(t) = d$ yields a unique homomorphism $f : R \to S$ with $f(T) = T_S$. Thus the map $f \mapsto f(T)$ is a bijection.

Lecture 18
2015-02-23

---

4 Fields

4.1 Basics

Proposition 99. *Let K be a field. Consider the natural map $\mathbb{Z} \to K$. Either this map is injective in which case we say K has characteristic 0 or there is a unique prime p such that $p = 0$ in K in which case we say that K has characteristic p.*

Proof. Consider the kernel $0 \to \ker \to \mathbb{Z} \to K$. Then $\mathbb{Z}/\ker \subset K$ is an integral domain and so ker is a prime ideal of $\mathbb{Z}$. Thus it is either (0) or (p) for some prime p. □

Definition 100. An extension of fields L/K is simply a containment $L \supset K$. If L/K is an extension then L is a K-vector space and we define $[L:K] = \dim_K L$.

Example 101.
1. $[\mathbb{C} : \mathbb{R}] = 2$.
2. If K is a finite field then there exists a prime p and $n \geq 1$ such that $|K| = p^n$. Indeed, since K is finite $\mathbb{Z}$ cannot inject into K so K has characteristic p for some prime p. Then $\mathbb{F}_p = \mathbb{Z}/(p) \subset K$ and $K/\mathbb{F}_p$ is a finite extension of fields. Let $[K : \mathbb{F}_p] = n$. Then K as an $\mathbb{F}_p$-vector space is $\mathbb{F}_p^n$ so it has cardinality p^n.

Proposition 102. *If $L/M/K$ are field extensions then $[L:K] = [L:M][M:K]$.*

Proof. Done in class. See Dummit and Foote Theorem 12 on page 523. □

4.2 Algebraic extensions

Definition 103. An element α is said to be algebraic over a field K if it is integral over K. An extension L/K is said to be algebraic if it is integral. The algebraic closure of a field K in a field L is its integral closure. The field K is said to be integrally closed in L if every element of L algebraic over K is in K.

Proposition 104. *Let K be a field. For any α denote $K[\alpha]$ as the ring of polynomial expressions in α with K-coefficients. Denote $K(\alpha) = \mathrm{Frac}\, K[\alpha]$.*

1. *If α, β are algebraic over K then $\alpha + \beta$ and $\alpha\beta$ are algebraic over K.*
2. *If α is algebraic over K then $K[\alpha] = K(\alpha)$.*
3. *If L/M is algebraic and M/K is algebraic then L/K is algebraic.*
4. *If L/K is an extension then the algebraic closure of K in L is a field M which is algebraically closed in L.*

5. *Every finite extension L/K is algebraic.*

6. *Every algebraic extension L/K can be written as a union $L = \cup L_i$ where L_i/K is finite.*

Proof. (1): Follows from the analogous statement for integral extensions.

(2): Suppose $P(\alpha) \in K[\alpha]$ is nonzero. We need to show that $1/P(\alpha) \in K[\alpha]$. By (1) $\beta = P(\alpha)$ is algebraic and so it satisfies a polynomial equation $Q(\beta) = 0$ of smallest degree n of the form $a_n\beta^n + \cdots + a_1\beta + a_0 = 0$. We may assume that $a_0 \neq 0$ because otherwise, since $\beta \neq 0$, we can divide by β to obtain an equation of smaller degree. But then

$$\frac{1}{\beta} = -\frac{a_1}{a_0} - \frac{a_2\beta}{a_0} - \cdots - \frac{a_n\beta^{n-1}}{a_0}$$

Thus $\beta^{-1} \in K[\beta] \subset K[\alpha]$.

(3): Follows from the analogous statement for integral extensions.

(4): Suppose $\alpha \in L$ is algebraic over K satisfying $P(X) = 0$, with $\alpha \neq 0$. Then $1/\alpha$ satisfies $X^{\deg P}P(1/X) = 0$ and so $1/\alpha \in L$ is again algebraic over K. Thus M is a field. That it is algebraically closed in L follows from the analogous statement for integral extensions.

(5): If $\alpha \in L$ then $K(\alpha) \subset L$ is also finite over K since sub vector spaces of finite dimensional vector spaces are again finite dimensional. Thus α is integral and thus algebraic over K.

(6): If L/K is algebraic then

$$L = \cup_{\alpha \in L} K(\alpha)$$

and $K(\alpha)/K$ is finite since α is algebraic.

□

Lecture 19
2015-02-25

Lemma 105. *Let $\phi : F_1 \to F_2$ be a homomorphism between two fields with no restriction on $\phi(1)$. Then either $\phi = 0$ or ϕ is injective. If ϕ is surjective then it is an isomorphism.*

Proof. Consider the ideal $\ker \phi \subset F_1$. It is either (0) in which case ϕ is injective, or it is F_1 in which case $\phi = 0$. If ϕ is surjective then $\phi \neq 0$ and so it is also injective. □

Definition 106. Let α be algebraic over K. Then the set $I_\alpha = \{P(X) \in K[X] | P(\alpha) = 0\}$ is an ideal of $K[X]$. It is principal generated by $m_\alpha(X) \in K[X]$ which is uniquely defined if assumed to be monic. The polynomial m_α is the minimal polynomial of α.

Proposition 107. *If α is algebraic over K then*

1. *$m_\alpha(X)$ is irreducible.*

2. *$K(\alpha) \cong K[X]/(m_\alpha(X))$.*

Proof. (1): It suffices to show that I_α is a prime ideal. If $PQ \in I_\alpha$ then $P(\alpha)Q(\alpha) = 0$ so one of $P(\alpha)$ and $Q(\alpha)$ is 0 which implies that P or Q is in I_α. Thus I_α is prime.

(2): The map $K[X] \to K[\alpha] = K(\alpha)$ is surjective. Moreover, since $m_\alpha(\alpha) = 0$ it follows that the map factors through the homomorphism of fields $K[X]/(m_\alpha(X)) \to K(\alpha)$. This is again surjective and thus an isomorphism by the previous lemma. □

We have seen that if $P(X)$ is an irreducible polynomial in $K[X]$ then $K[X]/(P(X))$ is a finite extension of K which contains some root of $P(X)$. The next result shows that the root does not matter.

Proposition 108. *Suppose $\phi : K \xrightarrow{\cong} K'$ is a field isomorphism and $P(X) \in K[X]$ is an irreducible polynomial. The polynomial $P'(X) = \phi(P(X)) \in K'[X]$ is clearly irreducible. If α is a root of P and β is a root of P' then there exists a commutative diagram*

$$\begin{array}{ccc} K & \xrightarrow[\cong]{\phi} & K' \\ \downarrow & & \downarrow \\ K(\alpha) & \xrightarrow{\cong} & K'(\beta) \end{array}$$

In particular any two roots of an irreducible polynomial over K generate isomorphic extensions of K.

Proof. Note that since $\phi(P) = P'$ the map $\phi : K[X] \to K'[X]$ yields an isomorphism of fields $K[X]/(P) \to K'[X]/(P')$ which extends $K \cong K'$. Since P is irreducible it follows that $P = m_\alpha$ and similarly $P' = m_\beta$. The previous result then shows that $K(\alpha) \cong K[X]/(P) \cong K'[X]/(P') \cong K'(\beta)$ as desired. □

Example 109. For example $X^3 - 2$ is irreducible over $\mathbb{Q}$ and so $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\zeta_3\sqrt[3]{2})$ as fields.

4.3 Algebraically closed fields

Definition 110. 1. A field K is said to be algebraically closed if every algebraic element over K is in K.

2. An algebraic closure of a field K is an algebraically closed field which is algebraic over K.

Lemma 111. *If every polynomial in $K[X]$ has a root in K then K is algebraically closed.*

Proof. Suppose α is algebraic over K. Let m_α be its minimal polynomial. By assumption m_α has a root in K. Since m_α is irreducible it follows that m_α is linear and therefore $\alpha \in K$ as desired. □

Theorem 112. *Let K be any field.*

1. *There exists an algebraically closed field L containing K.*
2. *For any algebraically closed field L containing K the algebraic closure of K in L is an algebraic closure of K.*

Proof. (1): Done in class. See Dummit and Foote Proposition 30 on page 544. It uses the previous lemma.
(2): Let $\overline{K}$ be the algebraic closure of K in L. This is a field from a previous result and by definition it is algebraic over K. Suppose now that α is algebraic over $\overline{K}$. Then $\overline{K}(\alpha)/\overline{K}$ is algebraic and so $\overline{K}(\alpha)/K$ is also algebraic which implies that α is algebraic over K. Since L is algebraically closed we deduce that $\alpha \in L$ and so by definition α is in the algebraic closure $\overline{K}$ of K in L. □

Example 113. The field $\mathbb{C}$ is algebraically closed by the fundamental theorem of algebra which we'll prove later using Galois theory. Thus the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ in $\mathbb{C}$ is an algebraic closure of $\mathbb{Q}$.

Lecture 20
2015-02-27

Proposition 114. *Let K be a field.*

1. *If $i : K \hookrightarrow L$ is an injection such that $L/i(K)$ is algebraic then any field homomorphism $K \to M$ where M is algebraically closed extends to a homomorphism $L \to M$.*
2. *Any two algebraic closures of K are isomorphic as fields.*

Proof. (1): Let $\mathcal{S}$ be the collection of pairs (T, f) where $L/T/K$ is a subextension and $f : T \to M$ is such that $f \circ i$ is the given homomorphism $K \to M$. We give the partial order on $\mathcal{S}$ by $(T, f) \leq (T', f')$ if $T \subset T'$ and $f' \circ i = f$. If $\mathcal{T} \subset \mathcal{S}$ is an increasing chain then let T be the union of the fields in $\mathcal{T}$. It's clear that $K \to M$ extends to $T \to M$ since every element of T is in some pair in $\mathcal{T}$. Thus $\mathcal{T}$ has a maximal element and Zorn's lemma implies that $\mathcal{S}$ has a maximal element (L', f').

To check that $L' = L$ suppose $\alpha \in L - L'$. It suffices to extend f' to $L'(\alpha) \to M$ because this would contradict the maximality of L'. Let β be any root of $f(P')$. Recall that we can find an isomorphism $L'(\alpha) \cong f(L')(\beta)$ making the diagram commute:

$$\begin{array}{ccc} L'(\alpha) & \longrightarrow & f(L')(\beta) \\ \uparrow & & \uparrow \\ L' & \xrightarrow{f'} & f(L') \end{array}$$

The result now follows because $f(L')(\beta) \subset M$.

(2): Let $i_j : K \to L_i$, $i = 1, 2$, be two algebraic closures of K. From (1) there exist maps $f : L_1 \to L_2$ such that $f \circ i_1 = i_2$. Then L_2 is a necessarily algebraic extension of $f(L_1)$ and since L_1 is algebraically closed and f must be an injection we deduce that $L_2 = f(L_1)$ and so f is an isomorphism. □

4.4 Composition of fields

Definition 115. If K_1 and K_2 are two subfields of a field L then the composite K_1K_2 is the smallest subfield of L containing K_1 and K_2. We denote the composite of $K(\alpha)$ and $K(\beta)$ as $K(\alpha, \beta)$.

Remark 10. If L_1, L_2 are subextensions of a big extension of K then L_1L_2 consists of all rational expressions in elements of L_1 and L_2.

Proposition 116. *Suppose $L_1, L_2/K$ are two finite subextensions of some big field.*

1. *Then $[L_1L_2 : K] \leq [L_1 : K][L_2 : K]$ with equality if and only if a basis of L_1/K stays independent over L_2.*
2. *$[L_1 : K]$ and $[L_2 : K]$ divide $[L_1L_2 : K]$.*
3. *If $[L_1 : K]$ and $[L_2 : K]$ are coprime then $[L_1L_2 : K] = [L_1 : K][L_2 : K]$.*

Proof. (1): Let u_i be a basis of L_1/K and v_j a basis of L_2/K. Then $L_1 = K(u_1, \ldots, u_m)$ and $L_2 = K(v_1, \ldots, v_n)$. But then $L_1L_2 = K(u_i, v_j)$ which is spanned by $u_1, \ldots, u_m$ over L_2. Thus $[L_1L_2 : K] = [L_1L_2 : L_2][L_2 : K] \leq mn$ as desired with equality iff the spanning set is also a basis.

(2): Follows from the fact that L_1 and L_2 are subextensions of L_1L_2 and degree is multiplicative.

(3): From (2) we deduce that $[L_1 : K][L_2 : K] = \text{lcm}([L_1 : K], [L_2 : K]) \mid [L_1L_2 : K]$ and from (1) we deduce equality. □

Example 117. $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$ as $\sqrt[3]{5}$ has minimal polynomial $X^3 - 5$. Similarly $[\mathbb{Q}(\zeta_3\sqrt[3]{5}) : \mathbb{Q}] = 3$. However the composite extendion $\mathbb{Q}(\zeta_3, \sqrt[3]{5})$ does not have degree 9 over $\mathbb{Q}$. Indeed, $\mathbb{Q}(\zeta_3, \sqrt[3]{5}) = \mathbb{Q}(\zeta_3)\mathbb{Q}(\sqrt[3]{5})$ is degree $6 = 2 \cdot 3$ over $\mathbb{Q}$ as 2 and 3 are coprime.

In the previous proposition part 1 this is because the basis $1, \sqrt[3]{5}, \sqrt[3]{25}$ of $\mathbb{Q}(\sqrt[3]{5})$ over $\mathbb{Q}$ satisfies

$$1 \cdot \zeta_3^2\sqrt[3]{25} + \sqrt[3]{5} \cdot \zeta_3\sqrt[3]{5} + \sqrt[3]{25} \cdot 1 = 0$$

over $\mathbb{Q}(\zeta_3\sqrt[3]{5})$.

Proposition 118. *If $[L_1L_2 : K] = [L_1 : K][L_2 : K]$ then $L_1 \cap L_2 = K$. The converse is not true.*

Proof. Suppose $[L_1L_2 : K] = [L_1 : K][L_2 : K]$. From the previous proposition we know that $[L_1L_2 : L_1 \cap L_2] \leq [L_1 : L_1 \cap L_2][L_2 : L_1 \cap L_2]$. But $[L_1L_2 : L_1 \cap L_2] = [L_1L_2 : L_1][L_1 : L_1 \cap L_2]$ and we deduce that $[L_1L_2 : L_1] \leq [L_2 : L_1 \cap L_2]$.

Now $[L_1L_2 : K] = [L_1L_2 : L_1][L_1 : K] = [L_1 : K][L_2 : K] = [L_1 : K][L_2 : L_1 \cap L_2][L_1 \cap L_2 : K]$ and so $[L_1L_2 : L_1] = [L_2 : L_1 \cap L_2][L_1 \cap L_2 : K]$. We also proved this is $\leq [L_2 : L_1 \cap L_2]$ and so $[L_1 \cap L_2 : K] \leq 1$. Thus $L_1 \cap L_2 = K$.

That the converse is not true follows from the previous example since $\mathbb{Q}(\sqrt[3]{5}) \cap \mathbb{Q}(\zeta_3\sqrt[3]{5}) = \mathbb{Q}$. □

4.5 Splitting fields and normal extensions

Definition 119. Let $P \in K[X]$ be a polynomial. The splitting field of P is any field L/K such that P splits as a product of linear terms over L but not so over any subextension of L. If the roots of $P(X)$ are $\alpha_1, \ldots, \alpha_n$ then the splitting field is $K(\alpha_1, \ldots, \alpha_n)$.

Example 120.

1. The splitting field of $X^3 - 5$ is $\mathbb{Q}(\zeta_3, \sqrt[3]{5})$.
2. The splitting field of $X^2 - 5$ is $\mathbb{Q}(\sqrt{5})$.
3. The splitting field of $X^2 + X + 1$ over $\mathbb{F}_2$ is a field with 4 elements.
4. If $K = \operatorname{Frac} \mathbb{Q}[\![x]\!]$ and $P(Y) \in K[Y]$ is $Y^2 - 2x - 1$ then the splitting field, by definition, is $K(\pm\sqrt{1+2x})$. However, the degree is not 2. In fact $K(\sqrt{1+2x}) = K$ since $\sqrt{1+2x} = \sum_{n \geq 0} \binom{1/2}{n} 2^n x^n \in K$.

Lecture 21
2015-03-02

Proposition 121. *Suppose $P(X)$ has degree n and splitting field L. Then $[L : K] \leq n!$.*

Proof. Done in class. See Dummit and Foote Proposition 26 on page 538. □

Proposition 122. *Let $P(X) \in K[X]$ be a polynomial. Suppose $\phi : K \xrightarrow{\cong} K'$ and $P' = \phi(P) \in K'[X]$. Let L be a splitting field of P and L' be a splitting field of P'. Then there exists an isomorphism $L \cong L'$ making the diagram commutative:*

$$\begin{array}{ccc} L & \xrightarrow{\cong} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow{\cong} & K' \end{array}$$

Proof. Done in class. See Dummit and Foote Theorem 27 on page 541. □

This proposition has the following corollary.

Definition 123. An extension L/K is said to be **normal** if any irreducible polynomial $P(X) \in K[X]$ that has one root in L has all roots in L.

Example 124.

1. For any field K the extension $\overline{K}/K$ is normal.
2. $\mathbb{C}/\mathbb{R}$ is normal.
3. $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$ is not normal.

Lemma 125. *Suppose L/K is a field extension and $\phi : L \to L$ is a field isomorphism such that $\phi|_K = \mathrm{id}_K$. If $P(X) \in K[X]$ has a root $\alpha \in L$ then $\phi(\alpha)$ is another root of $P(X)$.*

Proof. Note that $0 = \phi(0) = \phi(P(\alpha)) = P(\phi(\alpha))$ as ϕ is the identity on the coefficients of $P(X)$. □

Theorem 126. *A finite extension L/K is normal if and only if L is the splitting field of some polynomial in $K[X]$.*

Proof. Suppose L/K is normal. Note that the composite of two splitting fields in L is again a splitting field in L. Therefore we may choose $L/M/K$ the maximal subextension that is a splitting field over K, say of the polynomial $Q(X)$. If $M = L$ then we are done. Otherwise let $\alpha \in L - M$ with minimal polynomial $P(X)$ over K. Then the roots $\alpha_1 = \alpha, \ldots, \alpha_k$ of $P(X)$ all lie in L. Note that $M(\alpha_1, \ldots, \alpha_n) \subset L$ is the splitting field over K of the polynomial $P(X)Q(X)$ which contradicts the choice of M.

Now suppose $L = K(\alpha_1, \ldots, \alpha_n)$ is the splitting field of $P(X) \in K[X]$ with roots α_i. Suppose $Q(X) \in K[X]$ is an irreducible polynomial with root $\alpha \in L$. Let M be a splitting field of $P(X)Q(X)$ over L. Then clearly $L \subset M$. Let $\beta \in M$ by any other root of $Q(X)$. We'd like to show that $\beta \in L$. Since Q is irreducible we know there exists a field isomorphism $\phi : K(\alpha) \to K(\beta)$ sending α to β and being the identity on K.

The field M is a splitting field for $P(X)Q(X)$ over K but since M contains both $K(\alpha)$ and $K(\beta)$, M is the splitting field of $P(X)Q(X)$ over $K(\alpha)$ and of $P(X)Q(X) = \phi(P(X)Q(X))$ over $K(\beta)$. The previous proposition implies that we may extend ϕ to an isomorphism $\phi : M \to M$ which restricts to $\phi : K(\alpha) \to K(\beta)$. Let $\alpha_1, \ldots, \alpha_m$ be the roots of $P(X)$, all in L. Then $\alpha \in L$ must be a rational (in fact polynomial) expression in $\alpha_1, \ldots, \alpha_m$. But the previous lemma implies that $\phi(\alpha_i)$ is again a root of $P(X)$ and so $\phi(\alpha_1), \ldots, \phi(\alpha_m) \in L$. But then $\beta = \phi(\alpha) \in L$. □

4.6 Separable extensions

Definition 127. A polynomial $P(X) \in K[X]$ is said to be separable if it has no multiple root.

Example 128. $X^2 - Y \in \mathbb{F}_2(Y)[X]$ splits as $(X - \sqrt{Y})^2$ over the splitting field $\mathbb{F}_2(\sqrt{Y})$ but is irreducible over $\mathbb{F}_2(Y)$.

Proposition 129. *Let K be any field. For $P(X) = \sum_{i=0}^{n} a_i X^i$ define $P'(X) = \sum_{i=1}^{n} i a_i X^{i-1}$.*

1. *$(P + Q)' = P' + Q'$.*
2. *$(PQ)' = P'Q + PQ'$.*
3. *A root α if $P(X)$ is a multiple root if and only if $P'(\alpha) = 0$.*
4. *The polynomial $P(X)$ is separable if and only if P and P' are coprime.*
5. *If $P(X)$ is irreducible then P is separable unless $P' = 0$ in which case it is not separable.*

Proof. (1): Trivial by hand.

(2): Using (1) it suffices to check it for monomials. But $(aX^m bX^n)' = ab(m+n)X^{m+n-1} = ambX^{m-1}X^n + bnaX^m X^{n-1}$.

(3): If $P(X) = (X - \alpha)^2 Q(X)$ then $P'(X) = (X - \alpha)(Q'(X) + 2Q(X))$.

(4): Let L be a splitting field of $P(X)$ over K. If not separable then $X - \alpha \mid P, P'$. If P and P' are coprime over $K[X]$ then $P(X)A(X) + P'(X)B(X) = 1$ for some polynomials $A(X), B(X) \in K[X]$ which is impossible since $X - \alpha \nmid 1$.

(5): If P' is not zero then the only way P and P' can be not coprime, given that P is irreducible, is if $P \mid P'$ which contradicts that $\deg P > \deg P'$. If $P' = 0$ then every root of P is multiple. □

Example 130. $X^p + t$ is inseparable over $\mathbb{F}_p(t)$ but $X^2 + X + 1$ is separable over $\mathbb{F}_2$.

Lemma 131. *Let p be a prime and R any $\mathbb{F}_p$-algebra. Then $\phi(x) = x^p$ is a homomorphism $\phi : R \to R$. If R is reduced (e.g., if it is a field) then ϕ is injective.*

Proof. Done in class. See Dummit and Foote Proposition 35 on page 548. □

Lecture 22
2015-03-06

Definition 132. The $\mathbb{F}_p$-algebra R is said to be **perfect** if $\phi : R \to R$ is surjective.

Proposition 133. *Let K be a field and $P(X) \in K[X]$ be irreducible.*

1. *If K has characteristic 0 then P is separable.*
2. *If K has characteristic p a prime and P is not separable then there exists a separable polynomial $Q(X) \in K[X]$ and $k \neq 1$ such that $P(X) = Q(X^{p^k})$.*

Proof. (1): Note that $\deg P' = \deg P - 1$ since if $a_n \neq 0$ then $na_n \neq 0$ in characteristic 0.

(2): It suffices to show that if P is inseparable then $P(X) = Q(X^p)$ for some Q. Since $p \deg Q = \deg P$ after finitely many steps the procedure must stop, i.e., we reach a separable polynomial. The previous proposition implies that $P'(X) = 0$ so $\sum i a_i X^{i-1} = 0$ so $ia_i = 0$ for all i. This implies that $a_i = 0$ whenever $p \nmid i$ and taking $Q(X) = \sum a_{pi} X^i$ works. □

Definition 134. A field K is said to be **perfect** if either K has characteristic 0 or if it has characteristic p and it is perfect as an $\mathbb{F}_p$-algebra. An algebraic extension L/K is said to be **separable** if every element of L has separable minimal polynomial.

Proposition 135. *Suppose K is perfect. Then every algebraic extension is separable.*

Proof. Let $\alpha \in L$ with minimal polynomial $P(X)$. Since P is irreducible it is separable in characteristic 0. Suppose K has characteristic p. Then there exists a separable polynomial $Q(X)$ such that $P(X) = Q(X^{p^k})$.

Let $Q(X) = \sum q_i X^i$. Since K is perfect there exist $a_i \in K$ such that $q_i = a_i^{p^k}$. Then $Q(X^{p^k}) = \sum q_i X^{ip^k} = \sum (a_i X^i)^{p^k} = R(X)^{p^k}$ where $R(X) = \sum a_i X^i$. Thus, however, contradicts the fact that $P(X) = R(X)^{p^k}$ is irreducible. □

To study separable extensions more deeply we need the following criterion.

Theorem 136. *Let L/K be a finite extension of degree n and $\phi : K \to M$ a fixed injection field embedding (i.e., injection). Let $\mathcal{E}(L, \phi : K \hookrightarrow M) = \{\psi : L \hookrightarrow M | \psi|_K = \phi\}$.*

1. *$|\mathcal{E}(L, \phi : K \to M)| \leq [L : K]$.*
2. *If L/K is inseparable then $|\mathcal{E}(L, \phi : K \to M)| < [L : K]$.*
3. *If $L = K(\alpha_1, \ldots, \alpha_m)$ such that α_k is separable over $K(\alpha_1, \ldots, \alpha_{k-1})$ for all k. Then there exists a finite extension M' of M such that for any field N containing M', $|\mathcal{E}(L, \phi : K \to N)| = [L : K]$.*

Before proving the theorem I give an application.

Proposition 137.
1. *If $\alpha_1, \ldots, \alpha_m$ are such that for all k, α_k is separable over $K(\alpha_1, \ldots, \alpha_{k-1})$, then $K(\alpha_1, \ldots, \alpha_m)$ is separable over K.*
2. *If L/M and M/K are separable (not necessarily finite) then L/K is separable.*

Proof. (1): Part (3) of Theorem 136 implies that $|\mathcal{E}(L, K \hookrightarrow \overline{K})| = [L : K]$. Part (2) of the theorem then implies that L/K is separable.

(2): Suppose $\alpha \in L$. Then α is the root of a separable polynomial $X^n + b_{n-1}X^{n-1} + \cdots + b_1 X + b_0 = 0$ where $b_i \in M$. Since M/K is separable each b_i is separable and so α is separable over $K(b_0, \ldots, b_{n-1})$ which, in turn, is finite over K. Note that if b_k is separable over K then it is separable over $K(b_0, \ldots, b_{k-1})$ since its minimal polynomial over the finite extension divides the minimal polynomial over K. Thus $K(b_0, \ldots, b_n, \alpha)$ is separable by part (1). We conclude that α is separable over K. □

Proof of Theorem 136. First, let's show parts (1) and (2) inequality in the case of $L = K(\alpha)$. Let $P(X)$ be the minimal polynomial of α over K, of degree d. Then $K(\alpha)$ over K has basis $1, \alpha, \ldots, \alpha^{d-1}$ so $\psi \in \mathcal{E}(K(\alpha), \phi : K \hookrightarrow M)$ is uniquely determined by its value $\psi(\alpha)$. But $0 = \psi(P(\alpha)) = \psi(P)(\psi(\alpha)) = \phi(P)(\psi(\alpha)) = 0$ and so $\psi(\alpha)$ is a root of the polynomial $\phi(P)$ of degree d. Thus $\psi(\alpha)$ can take at most d values so $|\mathcal{E}(K(\alpha), \phi)| \leq d = [K(\alpha) : K]$ as desired. If $P(X)$ is inseparable then the number of roots of $P(X)$, and thus also the number of values of $\psi(\alpha)$, is $< \deg P(X)$ and so $|\mathcal{E}(K(\alpha), K \hookrightarrow M)| < [K(\alpha) : K]$.

(1): By induction on $[L : K]$. The base case $L = K$ is trivial. Suppose $\alpha \in L - K$. Note that if $\psi : L \to M$ is in $\mathcal{E}(L, K \hookrightarrow M)$ then $\psi|_{K(\alpha)} : K(\alpha) \to M$ is in $\mathcal{E}(K(\alpha), K \hookrightarrow M)$. In fact we get a partition

$$\boxed{\mathcal{E}(L, K \hookrightarrow M) = \bigsqcup_{\eta \in \mathcal{E}(K(\alpha), K \hookrightarrow M)} \mathcal{E}(L, \eta : K(\alpha) \hookrightarrow M)}$$

which is the main combinatorial tool in the proof.

From the case $K(\alpha)/K$ we know that $|\mathcal{E}(K(\alpha), K \hookrightarrow M)| \leq [K(\alpha) : K]$ and from the inductive hypothesis (since $[L : K(\alpha)] < [L : K]$) we know that $|\mathcal{E}(L, \eta : K(\alpha) \hookrightarrow M)| \leq [L : K(\alpha)]$. Thus

$$\begin{aligned}
|\mathcal{E}(L, \phi)| &= \sum_{\eta \in \mathcal{E}(K(\alpha), K \hookrightarrow M)} |\mathcal{E}(L, \eta : K(\alpha) \hookrightarrow M)| \\
&\leq \sum_{\eta \in \mathcal{E}(K(\alpha), K \hookrightarrow M)} [L : K(\alpha)] \\
&= [L : K(\alpha)] |\mathcal{E}(K(\alpha), K \hookrightarrow M)| \\
&\leq [L : K(\alpha)][K(\alpha) : K] \\
&= [L : K]
\end{aligned}$$

(2): If L/K is inseparable, for some $\alpha \in L$ the extension $K(\alpha)/K$ is inseparable. Thus $|\mathcal{E}(K(\alpha), K \hookrightarrow M)| < [K(\alpha) : K]$ and in the above formula we get strict inequality.

Lecture 23
2015-03-16

---

(3): Again, let's first do it in the case when $L = K(\alpha)$. Let $P(X)$ be the minimal polynomial of α over K. Let N be any extension of M containing the splitting field M' over M of the polynomial $\phi(P(X)) \in M[X]$. Let $\alpha_1, \ldots, \alpha_d \in N$ be the roots of this splitting field, all distinct as $P(X)$ is separable. We know that any $\psi \in \mathcal{E}(K(\alpha), K \hookrightarrow N)$ is uniquely defined by $\psi(\alpha)$ which has to be a root of $\phi(P(X))$. Any of the d roots α_i yields $\psi_i : K(\alpha) \hookrightarrow N$ and so we get equality $|\mathcal{E}(K(\alpha), K \hookrightarrow N)| = [K(\alpha) : K]$.

We proceed by induction on the number of α_i in L. For simplicity write $L_i = K(\alpha_1, \ldots, \alpha_i)$. Suppose $|\mathcal{E}(L_i, K \hookrightarrow M_i)| = [L_i : K]$ for some M_i/M finite. Let M_{i+1} be the splitting field over M_i of $\phi(P_{i+1}(X))$ where $P_{i+1}(X)$ is the minimal polynomial over L_i of α_{i+1}. Then $|\mathcal{E}(L_{i+1}, L_i \hookrightarrow M_{i+1}) = [L_{i+1} : L_i]$. Moreover, since M_{i+1} contains M_i the inductive hypothesis gives $|\mathcal{E}(L_i, K \hookrightarrow M_{i+1})| = [L_i : K]$. Finally the boxed combinatorial formula yields $|\mathcal{E}(L_{i+1}, K \hookrightarrow M_{i+1})| = [L_{i+1} : L_i][L_i : K] = [L_{i+1} : K]$. □

Definition 138. If L/K is any field extension let $\mathrm{Aut}(L/K) = \{f : L \xrightarrow{\cong} L | f|_K = \mathrm{id}_K\}$.

The following application of Theorem 136 is useful in Galois theory.

Proposition 139. *Let L/K.*

1. *If $\alpha \in L$ is algebraic over K with minimal polynomial $P(X)$ and $\phi \in \mathrm{Aut}(L/K)$ then $\phi(\alpha)$ is also a root of $P(X)$.*
2. *If L/K is finite then $|\mathrm{Aut}(L/K)| \leq [L : K]$.*

3. *If L/K is finite separable and normal then $|\operatorname{Aut}(L/K)| = [L : K]$.*

4. *If L/K is finite separable and normal and $L/M/K$ is any subextension then the number of embeddings $M \hookrightarrow L$ restricting to the identity on K is $[M : K]$.*

Proof. (1): This we already proved in the proof of Theorem 136.

(2): Note that $\operatorname{Aut}(L/K) = \mathcal{E}(L, K \hookrightarrow L)$ where $K \hookrightarrow L$ is a fixed inclusion. Then the statement follows from the theorem.

(3): Follows from (4).

(4): The set of such embeddings is $\mathcal{E}(M, K \hookrightarrow L)$. Suppose $M = K(\alpha)$. Let $P(X)$ be the minimal polynomial of α over K. Since L/K is normal, $P(X)$ splits over L and so the theorem implies that $|\mathcal{E}(K(\alpha), K \hookrightarrow L)| = [K(\alpha) : K]$. Thereafter the result follows by induction as in the theorem, part 3. □

Example 140. 1. Let $\zeta = \zeta_3$ and $u = \sqrt[3]{5}$. Then ζ has minimal polynomial $X^2 + X + 1$ and u has minimal polynomial $X^3 - 5$ over $\mathbb{Q}$. Both are separable and so Theorem 136 implies that $L = \mathbb{Q}(\zeta, u)$ is separable over $\mathbb{Q}$. The previous proposition implies that $\operatorname{Aut}(L/\mathbb{Q})$ has $[L : \mathbb{Q}] = 6$ elements. We know that every $f \in \operatorname{Aut}(L/\mathbb{Q})$ takes ζ to either ζ or ζ^2 and u to one of $u, \zeta u, \zeta^2 u$ (α goes to a root of its minimal polynomial).

   For $i \in \{1, 2\}$, $j \in \{0, 1, 2\}$ let $f_{i,j}$ be the unique homomorphism $L \to L$ taking $\zeta \mapsto \zeta^i$ and $u \mapsto \zeta^j u$. Since $L/\mathbb{Q}$ has basis $1, u, u^2, \zeta, \zeta u, \zeta u^2$ it follows that $f_{i,j}$ is uniquely defined by these two conditions. All 6 choices $f_{i,j}$ are clearly distinct and so $\operatorname{Aut}(L/\mathbb{Q}) = \{f_{i,j}\}$.

2. Consider $\mathbb{Q}(u)/\mathbb{Q}$. It is finite and separable but not normal. Any $f \in \operatorname{Aut}(\mathbb{Q}(u)/\mathbb{Q})$ takes u to one of $u, \zeta u, \zeta u^2$. At the same time $f(u) \in \mathbb{Q}(u) \subset \mathbb{R}$ and so $f(u) = u$ is the only choice. Finally, a basis of $\mathbb{Q}(u)/\mathbb{Q}$ is $1, u, u^2$ and so $f = \mathrm{id}$. Thus $\operatorname{Aut}(\mathbb{Q}(u)/\mathbb{Q}) = \{\mathrm{id}\}$.

Proposition 141. *If L/K is finite separable then $L = K(\alpha)$ for some $\alpha \in L$.*

Example 142. Continuing the previous example, I claim that $L = \mathbb{Q}(\zeta, u) = \mathbb{Q}(\zeta + u)$. Let $x = \zeta + u$. Certainly $\mathbb{Q}(\zeta, u) \supset \mathbb{Q}(x)$. Note that $x - \zeta = u$ so $(x - \zeta)^3 = u^3 = 5$. since $\zeta^2 = -\zeta - 1$ and $\zeta^3 = 1$ we deduce

$$\zeta = \frac{x^3 - 3x - 6}{3x^2 + 3x} \in \mathbb{Q}(x)$$

and also $u = x - \zeta \in \mathbb{Q}(x)$. Thus $\mathbb{Q}(\zeta, u) \subset \mathbb{Q}(x)$ and equality follows.

Proof of Proposition 141. If K is a finite field then so is L. We'll see in the next section that $L^\times$ is a cyclic group, generated by some g in which case $L = K(g)$.

Lecture 24

2015-03-18

Suppose that K is infinite. Since L/K is finite we may write $L = K(\alpha_1, \ldots, \alpha_n)$ with minimal n. We'd like to show that $n = 1$. Suppose $n > 1$. By induction it suffices to check that if $K(\alpha, \beta)/K$ is separable then $K(\alpha, \beta) = K(\gamma)$ for some γ.

For $c \in K$ the field $K(\alpha + c\beta) \subset K(\alpha, \beta)$ is separable over K. If $K(\alpha + c\beta) \subsetneq K(\alpha, \beta)$ then $[K(\alpha + c\beta) : K] < [K(\alpha, \beta) : K]$. Fix an embedding $K \hookrightarrow \overline{K}$ into an algebraic closure. The theorem implies there are $[K(\alpha, \beta) : K]$ extensions to $K(\alpha, \beta) \hookrightarrow \overline{K}$ and $[K(\alpha + c\beta) : K]$ extensions to $K(\alpha + c\beta) \hookrightarrow \overline{K}$. There are more of the former than the latter which implies that for two distinct embeddings $\phi, \psi : K(\alpha, \beta) \hookrightarrow \overline{K}$, they restrict to the same embeddings $K(\alpha + c\beta) \hookrightarrow \overline{K}$. But both extensions ϕ and ψ extend $K \hookrightarrow \overline{K}$ and so $\phi(c) = \psi(c) = c$ which implies that $\phi(\alpha) + c\phi(\beta) = \phi(\alpha + c\beta) = \psi(\alpha + c\beta) = \psi(\alpha) + c\psi(\beta)$.

Choose $c \neq 0$. Then $\phi(\alpha) = \psi(\alpha)$ iff $\phi(\beta) = \psi(\beta)$ in which case $\phi = \psi$ on $K(\alpha, \beta)$. Thus $c = (\phi(\alpha) - \psi(\alpha))/(\psi(\beta) - \phi(\beta))$. However, over all distinct embeddings $\phi, \psi : K(\alpha, \beta) \hookrightarrow \overline{K}$ there are finitely many such expressions. Since K is infinite we may choose c not equal to any such value in which case we get a contradiction.

□

Example 143. 1. $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

2. $\mathbb{Q}(\zeta_3, \sqrt[3]{5}) = \mathbb{Q}(\zeta_3 + \sqrt[3]{5})$.

Proposition 144. *Suppose L/K is an algebraic extension of fields such that K is an imperfect field of characteristic p, a prime. Let $M = \{x \in L | K(x)/K \text{ is separable}\}$.*

1. *M is a field called the separable closure of K in L.*
2. *M/K is separable.*
3. *L/M is* **purely inseparable**, *i.e., every element of L not in M has inseparable minimal polynomial.*
4. *If L/K is normal then M/K is also normal.*

Proof. (1): If α has separable minimal polynomial $P(X)$ then $1/\alpha$ has necessarily separable minimal polynomial $X^{\deg P(X)}P(1/X)$. If α, β are separable then $K(\alpha,\beta)/K$ is separable and therefore $\alpha+\beta, \alpha\beta$ are both separable.

(2): By definition.

(3): If $\alpha \in L$ is separable over M then $M(\alpha)$ is separable over M which, in turn, is separable over K. Thus $M(\alpha)$ is separable over K.

(4): Suppose $P(X) \in K[X]$ is irreducible with a root $\alpha \in M$. Then $P(X)$ has all roots in L. At the same time it is the minimal polynomial of $\alpha \in M$ so it is separable which implies that all the other roots are in fact in M. □

Remark 11. One can also show that if M is the separable closure of K in L then

1. If L/K is finite then $[L:M]$ is a power of p. (One calls $[L:M]$ the inseparable degree of L/K and $[M:K]$ the separable degree.)
2. In fact, the minimal polynomial of every $x \in L$ over M is of the form $X^{p^k} - a$.

4.7 Finite fields

Proposition 145. *Let p be a prime and K a field with p^n elements.*

1. *The splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$ has p^n elements.*
2. *The field K is perfect.*
3. *The field K is the splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$.*
4. *All finite field with p^n elements are isomorphic.*
5. *The group $K^\times$ is cyclic.*

The (unique up to isomorphism) finite field with p^n elements is denoted $\mathbb{F}_{p^n}$.

Proof. (1): If α and β are roots of $P(X) = X^{p^n} - X$ then $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha+\beta$ is again such a root and $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$ is a root. Moreover $P'(X) = -1$ so P is separable. Thus $P(X)$ has p^n distinct roots and let F be the set of roots. It is stable under addition, multiplication and also clearly inverses so F is a field with p^n elements.

(2): $\phi : K \to K$ is an injection of finite sets so it is also surjective.

(3): If $\alpha \in K - 0$ then α is an element of the finite group $K^\times$ with $p^n - 1$ elements. Thus $\alpha^{p^n-1} = 1$ and so α is a root of $P(X)$. Thus all of K consists of roots of $P(X)$.

(4): Follows from uniqueness of splitting fields.

Lecture 25
2015-03-20

(5): Thr group $K^\times$ is finite abelian so it is of the form $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ with $n_1 \mid \ldots \mid n_r$. Pick $g \in K^\times$ to be the identity in $\mathbb{Z}/n_r\mathbb{Z}$. Note that every $h \in K^\times$ visibly has order dividing n_r (as $n_i \mid n_r$ for all i). Thus $h^{n_r} = 1$ where $n_r \mid p^n - 1$. This implies that every element $h \in K^\times$ is a root of $X^{n_r} - 1$ which has at most $n_r \mid p^n - 1$ roots. We deduce that $n_r = p^n - 1$ and so $K^\times = \langle g \rangle$ as desired. □

Proposition 146. *Let p be a prime and $n \geq 2$. There exists an irreducible polynomial $P(X) \in \mathbb{F}_p[X]$ of degree n and $\mathbb{F}_{p^n} \cong \mathbb{F}_p[X]/(P(X))$.*

Proof. Let $g \in \mathbb{F}_{p^n}$ (which we know to exist) a generator of $\mathbb{F}_{p^n}^\times$. Let $P(X)$ be the minimal polynomial of g over $\mathbb{F}_p$, of degree m. Then $\mathbb{F}_{p^n} = \mathbb{F}_p(g) \cong \mathbb{F}_p[X]/(P(X))$ has degree $n = \deg P(X)$ over $\mathbb{F}_p$. □

Corollary 147. *Let p be a prime. Denote $\mathcal{P}_d$ the set of irreducible monic polynomials of degree d in $\mathbb{F}_p[X]$.*

1. *$X^{p^n} - X$ is the product of all polynomials in $\mathcal{P}_d$ as $d \mid n$.*
2. *$p^n = \sum_{d|n} d|\mathcal{P}_d|$.*

Proof. (1): If P is an irreducible factor of $X^{p^n} - X$ of degree d then the splitting field $\mathbb{F}_{p^d}$ of $P(X)$ is a subfield of the splitting field $\mathbb{F}_{p^n}$ of $X^{p^n} - X$ and so $d \mid n$. Since $X^{p^n} - X$ is separable each irreducible factor appears once. Finally, suppose $P(X)$ is an irreducible polynomial of degree $d \mid n$. If α is a (nonzero) root of $P(X)$ then $\alpha \in \mathbb{F}_{p^d}$ and so $\alpha^{p^d - 1} = 1$. Since $d \mid n$ we have $p^d - 1 \mid p^n - 1$ and so α is also a root of $X^{p^n} - X$. This is true for every root of $P(X)$ and so $P \mid X^{p^n} - X$ as desired.

(2): Take degrees in (1). □

Proposition 148 (Möbius inversion)**.** *Define $\mu : \mathbb{Z}_{\geq 1} \to \{-1, 1\}$ by $\mu(n) = 0$ if n is not square free and $\mu(n) = (-1)^k$ if n is a product of k distinct primes. If $f, g : \mathbb{Z}_{\geq 1} \to \mathbb{C}$ are functions such that $f(n) = \sum_{d|n} g(d)$ for all n then*

$$g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d)$$

Proof. Let $\mathcal{S} = \{f : \mathbb{Z}_{\geq 1} \to \mathbb{C}\}$ which is an abelian group with respect to addition. Define the binary operation $*$ on $\mathcal{S}$ by $(f * g)(n) = \sum_{d|n} f(d)g(n/d)$. It's easy to check that $*$ is associative and distributive with respect to addition. Let $e \in \mathcal{S}$ such that $e(1) = 1$ and $e(n) = 0$ for $n > 1$. Then clearly $f * e = e * f = f$. The set $\mathcal{S}$ with $+, *$ and unit e is a commutative ring.

If $u = 1$ is the constant function in $\mathcal{S}$ then $u * \mu = \mu * u = e$. The condition in the problem is that $f = u * g$. Then $f * \mu = g$ as desired. □

Corollary 149. *There are $\frac{1}{n}\sum_{d|n} \mu(n/d)p^d$ irreducible polynomials of degree n in $\mathbb{F}_p[X]$. In particular the probability that a randomly chosen polynomial in $\mathbb{F}_p[X]$ of degree n is irreducible is at least $\frac{1}{pn} - \frac{\log_2(n)}{p^{n/2+1}}$.*

Remark 12. This is useful in computer science. The way to construct $\mathbb{F}_{p^n}$ is to choose an irreducible polynomial in $\mathbb{F}_p[X]$ of degree n and then store $\mathbb{F}_p[X]/(P(X))$ in the computer. Choosing such P can be done randomly. Choosing randomly polynomials, if one had an irreducibility criterion, would yield an irreducible polynomial in expected time n. I did this in detail in class.

Lecture 26
2015-03-23

4.8 Cyclotomic fields

Definition 150. The n-th cyclotomic field is the splitting field of $X^n - 1$ over $\mathbb{Q}$. Let μ_n be the n-th roots of unity. Then μ_n is cyclic, generated by $e^{2\pi i/n}$. A primitive n-th root of unity is any generator of μ_n.

Proposition 151. *Let $\zeta \in \mu_n$ be a primitive root.*

1. *The set of primitive roots is $\Psi_n = \{\zeta^k | (k,n) = 1\}$ and has order $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.*
2. *The n-th* **cyclotomic polynomial** *defined as*

$$\Phi_n(X) = \prod_{\zeta \in \Psi_n} (X - \zeta)$$

   is in $\mathbb{Z}[X]$ and has degree $\varphi(n)$.
3. *$X^n - 1 = \prod_{d|n} \Phi_d(X)$.*
4. *$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}$.*

Proof. (1): We know that the order of ζ^k is $n/(k,n)$ and the result is immediate.

(2): We see that the coefficients of $\Phi_n(X)$ are algebraic integers. Moreover, from (4) it follows that it has rational coefficients. Since $\mathbb{Z}$ is integrally closed we deduce that it has integer coefficients.

(3): It suffices to show that every n-th root of unity appears exactly once in some $\Phi_d(X)$. Suppose $\zeta \in \mu_n$ has order $d \mid n$. Then ζ is a root of $\Phi_d(X)$. Moreover, every root of $\Phi_d(X)$ is an n-th root and must have order d. Thus Φ_d are all coprime and so each n-th root appears exactly once in the RHS.

(4): Follows from Möbius inversion applied to $\log(X^n - 1) = \sum_{d|n} \log \Phi_d(X)$. □

Theorem 152. *For each $n \geq 2$ the polynomial $\Phi_n(X)$ is irreducible over $\mathbb{Q}$ and thus $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.*

Proof. Done in class. See Dummit and Foote Theorem 41 on page 554. □

Lecture 27
2015-03-25

---

5 Galois theory

5.1 Automorphisms

Definition 153. An algebraic extension L/K is said to be **Galois** if L/K is both separable and normal. In that case we denote the group $\mathrm{Aut}(L/K)$ by $\mathrm{Gal}(L/K)$.

Remark 13.
1. We've seen that if L/K is finite Galois then $|\operatorname{Gal}(L/K)| = [L : K]$.
2. The main tool in computing Galois groups is the observation, used before, that if $\sigma \in \mathrm{Aut}(L/K)$ and $\alpha \in L$ is algebraic over K then $\sigma(\alpha)$ is another root of the minimal polynomial of α over K.

Example 154. I worked these out in detail in class.

1. $\mathrm{Aut}(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. The automorphisms are id and $a + b\sqrt{5} \mapsto a - b\sqrt{5}$.
2. $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}) = 1$.
3. From homework, $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = 1$, but the extension is not algebraic.
4. From homework, $\mathrm{Aut}(K(t)/K) \cong \mathrm{PGL}(2, K)$, but the extension is not algebraic.

5. Consider the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$. It is separable as $\mathbb{F}_p$ is perfect and normal, being the splitting field of X^{p^n}. Recall that Frobenius $\phi(x) = x^p$ is an automorphism. Fermat's little theorem implies that $\phi|_{\mathbb{F}_p} = \mathrm{id}$ and so $\phi \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Since $\mathbb{F}_{p^n}$ is the splitting field of $X^{p^n} - X = \phi^n - \mathrm{id}$ we deduce that $\phi^n = \mathrm{id}$ on $\mathbb{F}_{p^n}$ and $\phi^r \neq \mathrm{id}$ for $0 < r < n$. Thus $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \{\mathrm{id}, \phi, \phi^2, \ldots, \phi^{n-1}\}$ which, as a group, is $\cong \mathbb{Z}/n\mathbb{Z}$ by comparing cardinalities as $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.

6. $\mathbb{C}/\mathbb{R}$ is Galois with Galois group $\cong \mathbb{Z}/2\mathbb{Z}$ consisting of the identity and complex conjugation.

7. If $[L : K] = 2$ then L is the splitting field over K of a quadratic and therefor is normal. If K has characteristic not 2 then the extension L/K is always separable and therefore Galois. In characteristic 2, e.g., $\mathbb{F}_2(\sqrt{x})/\mathbb{F}_2(x)$ is quadratic, normal but not separable. If separable then $\mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}$ as this is the only group of cardinality 2.

8. For example $K(x)/K(x + 1/x)$ is degree 2. Indeed, if $y = x + 1/x$ then $x^2 - xy + 1 = 0$. It is Galois in characterstic not 2.

9. The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois, being the splitting field of $X^n - 1$. Its Galois group is $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. To $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ one get the automorphism σ_k taking ζ_n to ζ_n^k. Done in class, see Dummit and Foote Theorem 26 on page 596.

10. Let $p > 2$ be a prime. Then $\mathbb{Q}(\zeta_p, \sqrt[p]{2})$ is Galois over $\mathbb{Q}$. Any automorphism must take ζ_p to ζ_p^a for some $0 < a < p$ and $\sqrt[p]{2}$ to $\zeta_p^b \sqrt[p]{2}$ for some $0 \leq b < p$. Define $m(a, b) = \begin{pmatrix} a & b \\ & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F}_p)$ and $\sigma_{m(a,b)}$ as the automorphism taking ζ_p to ζ_p^a and $\sqrt[p]{2}$ to $\zeta_p^b \sqrt[p]{2}$. Since a basis of $\mathbb{Q}(\zeta_p, \sqrt[p]{2})$ over $\mathbb{Q}$ is given by $\zeta_p^i \sqrt[p]{2^j}$ for $0 \leq i \leq p-2$ and $0 \leq j \leq p-1$, $\sigma_{m(a,b)}$ is uniquely defined by a and b. This yields a homomorphism. Note that
$$\sigma_{m(a,b)} \circ \sigma_{m(a',b')} = \sigma_{m(a,b)m(a',b')}$$
and $\sigma_{m(1,0)} = \mathrm{id}$. Thus $\sigma_{m(a,b)}$ and $\sigma_{m(a,b)^{-1}} = \sigma_{m(a^{-1}, -a^{-1}b)}$ are inverses to each other and so $\sigma_{m(a,b)}$ is an automorphism.

    Finally, $\{\sigma_{m(a,b)}\} \subset \mathrm{Gal}(\mathbb{Q}(\zeta_p, \sqrt[p]{2})/\mathbb{Q})$ is a subgroup of order $p(p-1)$ which is also the order of the extension and thus of the Galois group. We deduce that
$$\mathrm{Gal}(\mathbb{Q}(\zeta_p, \sqrt[p]{2})/\mathbb{Q}) \cong \{\begin{pmatrix} a & b \\ & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F}_p)\} \cong \mathbb{Z}/p\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^\times$$

11. When $p = 3$ we get $\mathrm{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}) \cong S_3$ with $\sigma_{m(2,0)}$ being a transposition and $\sigma_{m(0,1)}$ being a 3-cycle.

12. $\mathbb{Q}(i, \sqrt[4]{2})$ is Galois over $\mathbb{Q}$ being the splitting field of $X^4 - 2$. The Galois group is $\cong D_8$ taking F to complex conjugation and R to the automorphism which takes i to i and $\sqrt[4]{2}$ to $i\sqrt[4]{2}$.

Lecture 28
2015-03-27

5.2 The main theorem of Galois theory

Definition 155. Suppose $H \subset \mathrm{Aut}(L/K)$ is a subgroup. Define $L^H = \{x \in L | \sigma(x) = x, \forall h \in H\}$.

The following proposition is immediate.

Proposition 156. *Let L/K be an extension.*

1. *If $H \subset \mathrm{Aut}(L/K)$ then L^H is a field, called the fixed field of H.*
2. *If $H_1 \subset H_2 \subset \mathrm{Aut}(L/K)$ then $L^{H_1} \supset L^{H_2}$.*

3. *If* $K \subset M_1 \subset M_2 \subset L$ *then* $\mathrm{Aut}(L/M_1) \subset \mathrm{Aut}(L/M_2)$.

The goal of this section is to prove the following two main theorems of Galois theory:

Theorem 157 (Main theorem A)**.** *Let* L/K *be a finite Galois extension.*

1. *If* $L/M/K$ *is a subextension then* L/M *is Galois.*
2. $L^{\mathrm{Gal}(L/M)} = M$.
3. *If* $H \subset \mathrm{Gal}(L/K)$ *is a subgroup then* $H = \mathrm{Gal}(L/L^H)$.
4. *There is a bijection between subgroups* $H \subset \mathrm{Gal}(L/K)$ *and subextensions* $L/M/K$ *sending* H *to* L^H *and* M *to* $\mathrm{Gal}(L/M)$.

Theorem 158 (Main theorem B)**.** *Let* L/K *be a finite Galois extension.*

1. *If* $\sigma \in \mathrm{Gal}(L/K)$ *and* H *is a subgroup of* $\mathrm{Gal}(L/K)$ *then* $\sigma(L^H) = L^{\sigma H \sigma^{-1}}$.
2. *A subextension* M *of* L/K *is Galois over* K *iff* $\sigma(M) = M$ *for all* $\sigma \in \mathrm{Gal}(L/K)$.
3. *In the bijection above* H *is normal if and only if* L^H/K *is Galois as well. Equivalently,* M/K *is Galois iff* $\mathrm{Gal}(L/M)$ *is normal in* $\mathrm{Gal}(L/K)$.
4. *In this case* $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$ *or equivalently* $\mathrm{Gal}(L^H/K) \cong \mathrm{Gal}(L/K)/H$.

5.2.1 Examples

Example 159. Examples for Theorem A.

1. Consider $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ containing the subgroup $H = \{-1, 1\}$. What is $\mathbb{Q}(\zeta_n)^H$? The group H fixes $\zeta_n + \zeta_n^{-1}$ and so $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subset \mathbb{Q}(\zeta_n)^H$. The main theorem then tells us that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n)^H] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$ and so $\mathbb{Q}(\zeta_n)^H = \mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\cos(2\pi/n)) \subset \mathbb{R}$. It is the largest real subfield of $\mathbb{Q}(\zeta_n)$.
2. We've seen that if $K = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$ then $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$. This group has the following subgroups: S_3, 1, A_3 and 3 transpositions. A_3 is generated by $\sigma_{m(0,1)}$ while the three transpositions are $\sigma_{m(2,b)}$ for $0 \leq b \leq 2$. What are the corresponding subextensions?
   (a) S_3: The subextension is $L^{S_3} = \mathbb{Q}$.
   (b) A_3: Note that ζ_3 is fixed by $\sigma_{m(0,1)}$ and so $\mathbb{Q}(\zeta_3) \subset L^{A_3}$. Then $[L : \mathbb{Q}(\zeta_3)] = 3 = |A_3| = [L : L^{A_3}]$ and so $L^{A_3} = \mathbb{Q}(\zeta_3)$.
   (c) Transposition $\sigma_{m(2,b)}$. Note that $\zeta_3^b \sqrt[3]{2}$ is fixed by $\sigma_{m(2,b)}$ and so $\mathbb{Q}(\zeta_3^b \sqrt[3]{2}) \subset L^{\langle \sigma_{m(2,b)} \rangle}$. A comparison of degree, as in the case of A_3, yields equality.

In class I also did one of these computations by brute force.

Lecture 29
2015-03-30

Example 160. Examples for Theorem B.

1. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is abelian it follows that any subgroup is normal and therefore any subextension is Galois over $\mathbb{Q}$.

2. We know from last semester's homework that the normal subgroups of $\{\begin{pmatrix} a & b \\ & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F}_p)\}$ are all of the form $H_c = \{\begin{pmatrix} a & b \\ & 1 \end{pmatrix} | a \in \langle c \rangle \subset \mathbb{F}_p^\times\}$. Since $H_1 \subset H_c$ we conclude that every subextension of $K = \mathbb{Q}(\zeta_p, \sqrt[p]{2})$ which is Galois over $\mathbb{Q}$, being of the form K^{H_c}, must be contained in K^{H_1}. Note that ζ_p is fixed by H_1 and so $\mathbb{Q}(\zeta_p) \subset K^{H_1}$. At the same time comparing degrees we deduce that $\mathbb{Q}(\zeta_p) = K^{H_1}$. We deduce that every subextension of K Galois over $\mathbb{Q}$ is in fact contained in $\mathbb{Q}(\zeta_p)$, all of whose subextensions are Galois over $\mathbb{Q}$.

5.2.2 Two technical results

The main tools in proving the main theorems of Galois theory are combinatorics and linear algebra.

Proposition 161 (Linear independence of characters)**.** *Suppose G is a finite group and L is a field. Let $\chi_1, \ldots, \chi_n : G \to L^\times$ are distinct characters, i.e., group homomorphisms. Then $\chi_1, \ldots, \chi_n$ are linearly independent over L, i.e., if $\sum a_i \chi_i(g) = 0$ for all g then $a_1 = \ldots = a_n = 0$.*

Proof. Done in class. See Dummit and Foote Theorem 7 on page 569. □

This uses combinatorics, specifically the fact that minimal linear dependences exist. This is in the same flavor as the proof of the fact that vector spaces have bases.

Proposition 162. *Let L/K be any extension and $H \subset \mathrm{Aut}(L/K)$ be any finite subgroup. Then $|H| = [L : L^H]$.*

Proof. Let $H = \{\sigma_1, \ldots, \sigma_n\}$ and $\{u_i\}$ a basis for L over L^H.

Suppose that $|H| > [L : L^H]$. Then L has basis $u_1, \ldots, u_m$ over L^H with $m < n$. Then linear algebra yields a nontrivial solution to the system

$$\begin{cases} \sum_{i=1}^n \sigma_i(u_1) x_i = 0 \\ \vdots \\ \sum_{i=1}^n \sigma_i(u_m) x_i = 0 \end{cases}$$

with $x_i \in L$. For every $\alpha \in L^H$ have $\sigma_i(\alpha) = \alpha$ so $\sum_i \sigma_i(\alpha u_j) x_i = 0$ for all j. Any $u \in L$ can be written as $u \sum a_j u_j$ with $a_j \in L^H$ and so $\sum_i \sigma_i(u) x_i = 0$ for all u. But then $\sigma_i : L \to L$ multiplicative are linearly dependent over L which contradicts the previous proposition.

Therefore $|H| \leq [L : L^H]$. Suppose that in fact we can find linearly independent (over L^H) vectors $u_1, \ldots, u_m$ in L. I.e., we are assuming that $|H| < [L : L^H]$.

Lecture 30
2015-04-01

The system

$$\begin{cases} \sum_{i=1}^m \sigma_1(u_i) x_i = 0 \\ \vdots \\ \sum_{i=1}^m \sigma_n(u_i) x_i = 0 \end{cases}$$

has a nontrivial solution with $x_i \in L$. Among all these solutions we can choose one with the smallest number of nonzero x_i and, reordering, we may assume that $x_1, \ldots, x_r$ are nonzero. Dividing by x_r we may further assume that $x_r = 1$. We get

$$\begin{cases} \sigma_1(u_1) x_1 + \cdots + \sigma_1(u_{r-1}) x_{r-1} + \sigma_1(u_r) = 0 \\ \vdots \\ \sigma_n(u_1) x_1 + \cdots + \sigma_n(u_{r-1}) x_{r-1} + \sigma_n(u_r) = 0 \end{cases}$$

If $x_1, \ldots, x_{r-1} \in L^H$ then take the equation for $\sigma_1 = 1 \in H$, namely, $u_1x_1 + \cdots + u_rx_r = 0$. This would be a linear dependence over L^H contradicting the choice of u_i. Let's assume that $x_1 \notin L^H$. This implies there exists $\sigma \in H$ such that $\sigma(x_1) \neq x_1$. For each i we have

$$\sum_j \sigma\sigma_i(u_j)\sigma(x_j) = \sigma(\sum_j \sigma_i(u_j)x_j) = 0$$

Since H is a group multiplication by σ permuted H and so we deduce that for each i (writing σ_i instead of $\sigma\sigma_i$),

$$\sum_j \sigma_i(u_j)\sigma(x_j) = 0$$

from which we subtract

$$\sum_j \sigma_i(u_j)x_j = 0$$

But $x_r = 1$ so $\sigma(x_r) = x_r$ so we obtain

$$\sum_{j=1}^{r-1} \sigma_i(u_j)(x_j - \sigma(x_j)) = 0$$

which contradicts the minimality of r.

□

5.2.3 The proof of the main theorems

Proof of Main Theorem A. (1): Since L/K is separable so is L/M. If L/K is normal and finite it is the splitting field over K of a separable polynomial in $K[X]$. L is then also the splitting field of the same polynomial but now over M. Thus L is normal over M.

(2): By definition $M \subset L^{\mathrm{Gal}(L/M)}$ and we know that $|\operatorname{Gal}(L/M)| = [L : M]$. But $[L : L^{\mathrm{Gal}(L/M)}] = |\operatorname{Gal}(L/M)|$ and so we deduce that $M = L^{\mathrm{Gal}(L/M)}$.

(3): By definition H fixes L^H so $H \subset \mathrm{Gal}(L/L^H)$. The two groups have equal orders but the proposition and so they are the same.

(4): The maps $M \mapsto \mathrm{Gal}(L/M)$ and $H \mapsto L^H$ are mutual inverses by (2) and (3) and therefore yield bijections between subextensions and subgroups of the Galois group. □

Proof of Main Theorem B. (1): Note that $x \in L^{\sigma H\sigma^{-1}}$ iff $\sigma h\sigma^{-1}(x) = x$ for all $h \in H$ iff $h(\sigma^{-1}(x)) = \sigma^{-1}(x)$ for all $h \in H$, iff $\sigma^{-1}x \in L^H$ iff $x \in \sigma(L^H)$.

(2): Note that M/K is separable as L/K is. If M/K is normal and $\alpha \in M$ let P be the minimal polynomial of α over K. Normality implies that all roots of P are in M. But also $\sigma(\alpha)$ is a root of P and therefore $\sigma(M) \subset M$. Comparing dimensions over K we deduce that $\sigma(M) = M$ for all $\sigma \in \mathrm{Gal}(L/K)$.

Suppose M/K is not normal. Then there exists an irreducible $P \in K[X]$ with one root $\alpha \in M$ and another root $\beta \notin M$. Necessarily $\beta \in L$ as L/K is normal. We may extend the identity on K to an isomorphism $K(\alpha) \xrightarrow{\cong} K(\beta)$ sending α to β. Since L is the splitting field over K of a polynomial in $K[X]$ and L contains both α and β we may extend the isomorphism $K(\alpha) \to K(\beta)$ to an isomorphism $\sigma : L \to L$. Since $\sigma|_K = \mathrm{id}$ we get that $\sigma \in \mathrm{Gal}(L/K)$ and $\sigma(\alpha) = \beta$. But $\alpha \in M$ while $\beta = \sigma(\alpha) \notin M$.

(3): By (2) L^H/K is Galois iff $\sigma(L^H) = L^H$ for all $\sigma \in \mathrm{Gal}(L/K)$. (1) then yields that $L^H = L^{\sigma H\sigma^{-1}}$. Main Theorem A then shows that $H = \sigma H\sigma^{-1}$. These are all equivalences so L^H/K is Galois iff H is normal in $\mathrm{Gal}(L/K)$. Taking $H = \mathrm{Gal}(L/M)$ yields the equivalent statement.

(4): If M/K is Galois, part (2) shows that for $\sigma \in \mathrm{Gal}(L/K)$ we get $\sigma : M \to M$ is also an automorphism. So $\sigma \mapsto \sigma|_M$ yields a homomorphism $\Phi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$. Its kernel is, by definition, $\mathrm{Gal}(L/M)$. Thus $\mathrm{Gal}(L/K)/\operatorname{Gal}(L/M) \cong \operatorname{Im}\Phi \subset \mathrm{Gal}(M/K)$. Comparing orders of groups we deduce that $\operatorname{Im}\Phi = \mathrm{Gal}(M/K)$ as desired. □

5.3 Galois groups of composite fields

Proposition 163. *Suppose $L, L'/K$ are extensions such that L/K is finite Galois.*

1. *Then LL'/L' is Galois and* $\mathrm{Gal}(LL'/L') \cong \mathrm{Gal}(L/L \cap L')$.
2. *If L'/K is finite then* $[LL' : K] = [L : K][L' : K]/[L \cap L' : K]$.

Proof. Done in class. See Dummit and Foote Proposition 19 on page 591. □

Proposition 164. *Suppose $L, L'/K$ are finite Galois extensions.*

1. *Then LL'/K and $L \cap L'/K$ are Galois.*
2. $$\mathrm{Gal}(LL'/K) \cong \{(\sigma, \tau) \in \mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K) | \sigma|_{L\cap L'} = \tau|_{L\cap L'}\}$$
3. *If $L \cap L' = K$ then* $\mathrm{Gal}(LL'/K) \cong \mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K)$.

Proof. Done in class. See Dummit and Foote Proposition 21 on page 592. □

Example 165. $\mathbb{F}_{p^m}\mathbb{F}_{p^n} = \mathbb{F}_{p^{[m,n]}}$. The proposition then says that $\mathbb{Z}/[m, n]\mathbb{Z} \cong \{(a, b) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} | a \equiv b \pmod{(m, n)}\}$ which follows from the Chinese Remainder Theorem.

Example 166. $\mathrm{Gal}(\mathbb{Q}(\zeta_n, \sqrt[n]{2}, \sqrt[n]{3})/\mathbb{Q}) \cong \{\left(\begin{pmatrix} a & b \\ & 1 \end{pmatrix}, \begin{pmatrix} a' & b' \\ & 1 \end{pmatrix}\right) | a = a' \in (\mathbb{Z}/n\mathbb{Z})^\times, b, b' \in \mathbb{Z}/n\mathbb{Z}\}$.

5.4 Solvability of polynomials and Galois groups

Definition 167. We say that a polynomial $P(X) \in K[X]$ is solvable by radicals if its roots can be expressed using $\sqrt[n]{\cdot}$ radicals. Equivalently if the splitting field of P over K is contained in a field of the form $K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_k]{a_k})$ where $a_i \in K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_{i-1}]{a_{i-1}})$ for each i.

Example 168.

1. Quadratics, cubics and quartics are all solvable by radicals.
2. $X^n - a$ is solvable by radicals.
3. $X^6 - 6X^4 - 12X^2 - 12 = (X^2 - 2)^3 - 4$ is solvable by radicals over $\mathbb{Q}$.
4. Any $P(X)$ over a finite field is solvable by radicals. Indeed, elements of finite fields are all roots of unity.

The main goal of this section is the following result.

Theorem 169. *Let K be a field of characteristic 0 and $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$.*

1. *If $a_0, \ldots, a_{n-1} \in K$ then P is solvable by radicals if and only if its splitting field L/K has solvable Galois group* $\mathrm{Gal}(L/K)$.
2. *If $a_0, \ldots, a_{n-1}$ are formal variables and $P(X) \in K(a_0, \ldots, a_{n-1})[X]$ then $P(X)$ is not solvable by radicals when $n \geq 5$.*

Remark 14. In part (2) we know solvability by radicals when $n \leq 4$ due to the quadratic formula, Cardano's formula and a similar formula for quartics.

Example 170. We know that $X^n - 2$ is solvable by radicals. Its Galois group is $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ which has as normal subgroup $\mathbb{Z}/n\mathbb{Z} \rtimes 1$ and therefore is solvable.

Lecture 32
2015-04-10

Proposition 171. *Suppose K has characteristic not dividing n. Then L/K is Galois with cyclic Galois group of order $\mid n$ iff $L = K(\sqrt[n]{a})$ for some $a \in K$.*

Proof. Done in class. See Dummit and Foote Propositions 36 and 37 on pages 625-626. □

Proof of Theorem 169. Done in class. See Dummit and Foote Theorem 39 on page 628. We used something we'll prove soon namely that in part (2) the Galois group is S_n which is not solvable when $n \geq 5$. □

Example 172. 1. $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is cyclic so solvable.

2. $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic and so solvable. To see directly note that $\mathbb{F}_{p^n}$ is the splitting field of $X^{p^n-1} - 1$.

5.5 Galois groups of polynomials and symmetric polynomials

Definition 173. Let $P(X) \in K[X]$ be a separable polynomial. The Galois group $\mathrm{Gal}(P)$ of P is the Galois group over K of the splitting field of P.

Remark 15. The previous section shows the importance of studying Galois groups of polynomials.

Definition 174. For variables $x_1, \ldots, x_n$ define the k-th symmetric polynomial

$$s_k = \sum_{1 \leq i_1 < \ldots < i_k \leq n} x_{i_1} \cdots x_{i_k}$$

Theorem 175. *Consider the extension $K(x_1, \ldots, x_n)/K(s_1, \ldots, s_n)$.*

1. *The extension is Galois.*
2. *$\mathrm{Gal}(K(x_1, \ldots, x_n)/K(s_1, \ldots, s_n)) \cong S_n$.*
3. *Every symmetric polynomial is a polynomial in the symmetric polynomials $s_1, \ldots, s_n$.*

Proof. (1): The variables $x_1, \ldots, x_n$ are the distinct roots of $X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n \in K(s_1, \ldots, s_n)[X]$. Thus the extension is a splitting field.

(2): A permutation $\sigma \in S_n$ acts on rational functions as follows: if $P(x_1, \ldots, x_n) \in K(x_1, \ldots, x_n)$ then $\sigma(P(x_1, \ldots, x_n)) = P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ and these are clearly automorphisms in $\mathrm{Gal}(K(x_1, \ldots, x_n)/K(s_1, \ldots, s_n))$. But $[K(x_1, \ldots, x_n) : K(s_1, \ldots, s_n)] \leq n!$ (from the section on splitting fields) and so we get equality comparing cardinalities.

(3): The main theorem of Galois theory yields $K(x_1, \ldots, x_n)^{S_n} = K(s_1, \ldots, s_n)$. □

Corollary 176. *Every finite group is a Galois group of a finite Galois extension.*

Proof. If G has order n then $G \subset S_n$ and so $\mathrm{Gal}(K(x_1, \ldots, x_n)/K(x_1, \ldots, x_n)^G) = G$. □

Lecture 33
2015-04-13

The main tool in computing the Galois group of a polynomial is the following:

Lemma 177. *Let K be any field and $P(X) \in K[X]$ a separable polynomial.*

1. *If $P(X)$ is irreducible of degree n then $\mathrm{Gal}(P) \subset S_n$ and has order divisible by n.*
2. *If $P(X) = P_1(X) \cdots P_k(X)$ where P_i is irreducible of degree n_i then the splitting field of P is the composite of the splitting fields of P_i and therefore $\mathrm{Gal}(P) \subset S_{n_1} \times \cdots \times S_{n_k}$.*

3. *If $Q(X) \in K[X]$ is any separable irreducible that splits over the splitting field of P then* $\mathrm{Gal}(P)$ *acts transitively on the roots of* $Q(X)$.

Proof. (1) and (2): $\mathrm{Gal}(P)$ permutes the roots of irreducible polynomials and so $\mathrm{Gal}(P)$ acts on the roots of P_i so we get a homomorphism $\mathrm{Gal}(P) \to S_{n_1} \times \cdots \times S_{n_k}$. Every automorphism in $\mathrm{Gal}(P)$ is uniquely defined by what it does on the roots of $P(X)$ and so this homomorphism is injective. Adjoining one root of P_i shows that $n_i \mid |\mathrm{Gal}(P)|$.

(3): Again $\mathrm{Gal}(P)$ acts on the roots of Q. If α, β are two roots of Q then there exists an isomorphism $K(\alpha) \cong K(\beta)$ extending the identity on K. From the section on splitting field this extends to an automorphism of the splitting field which is then an element of $\mathrm{Gal}(P)$. □

Definition 178. The discriminant of a polynomial $P(X) \in K[X]$ is the expression

$$D = \mathrm{disc}(P) = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

where $\alpha_1, \ldots, \alpha_n$ are all the roots of $P(X)$. Clearly $D \neq 0$ iff P is separable.

Proposition 179. *Suppose $P(X) \in K[X]$ is a separable polynomial and $D = \mathrm{disc}(P)$.*

1. *$D \in K$ and*
$$D = (-1)^{\binom{n}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j) = (-1)^{\binom{n}{2}} \prod_i P'(\alpha_i)$$
2. *Suppose K has characteristic different from 2. Let $\sigma \in \mathrm{Gal}(P)$ thought of as an element of S_n by letting σ permute the set of roots $\{\alpha_1, \ldots, \alpha_n\}$. Then $\sigma \in A_n$ iff $\sigma(\sqrt{D}) = \sqrt{D}$.*
3. *Suppose K has characteristic different from 2.* $\mathrm{Gal}(P) \subset A_n$ *iff* $\sqrt{D} \in K$.

Proof. Done in class. See Dummit and Foote Propositions 33 and 34 on pages 610 and 611. □

Example 180.
1. $\mathrm{disc}(X^2 + aX + b) = a^2 - 4b$. Clearly Gal is either $1 = A_2$ or S_2 according to whether the discriminant is a square or not.
2. $\mathrm{disc}(X^3 + aX + b) = -4a^3 - 27b^2$. If the cubic is irreducible then Gal has order divisible by 3 so is either A_3 or S_3.
3. From homework $\mathrm{disc}(X^n + aX + b) = (-1)^{\binom{n}{2}} n^n q^{n-1} + (-1)^{\binom{n-1}{2}} (n-1)^{n-1} p^n$.

Theorem 181 (Galois groups over $\mathbb{Q}$)**.** *Let $P(X) \in \mathbb{Z}[X]$ be an irreducible polynomial of degree n. Suppose $p \nmid \mathrm{disc}(P)$ is a prime number and*

$$P(X) \equiv \overline{P}_1(X) \cdots \overline{P}_k(X) \pmod{p}$$

is the factorization mod p. Then there exists $\sigma \in \mathrm{Gal}(P)$ whose cycle type is $(\deg P_1, \ldots, \deg P_k)$.

Proof. Hard, uses algebraic number theory. □

Example 182. This theorem works with large Galois groups.

1. $X^5 + 20X + 16$ has discriminant $2^{16} \cdot 5^6$ so $\mathrm{Gal} \subset A_5$. Mod 3 it is irreducible so there exists a 5-cycle in Gal. Mod 7 it splits as a linear times a linear times a cubic so there exists a 3-cycle. But A_5 is generated by a 3-cycle and a 5-cycle and so $\mathrm{Gal} = A_5$.
2. $X^5 + 20X + 15$. Mod 3 get that Gal contains a transposition and mod 13 the polynomial is irreducible so Gal contains a 5-cycle. We deduce that $\mathrm{Gal} = S_5$ which confirms that the discriminant $5^5 \cdot 257 \cdot 1217$ is not a square.

Lecture 34
2015-04-15

5.6 The fundamental theorem of algebra

Theorem 183. *The field $\mathbb{C} = \mathbb{R}(i)$ is algebraically closed.*

Proof. Done in class. See Dummit and Foote Theorem 35 on page 616. □

5.7 Infinite Galois theory

Example 184. 1. The extension $\overline{K}/K$ is Galois when K is perfect.

2. More generally if K has characteristic p and is not perfect then K^{sep}/K is Galois.

3. If $L_1 \subset L_2 \subset \ldots$ are all Galois over K and $L = \cup L_i$ then L/K is Galois.

Proposition 185. *Suppose L/K is infinite Galois.*

1. *Let $\mathcal{I} = \{L/M/K | M/K$ finite Galois$\}$ with $M \prec M'$ if $M \subset M'$. Then $\mathcal{I}$ is a directed set.*

2. *Consider $\{\mathrm{Gal}(M/K)\}_{M\in\mathcal{I}}$ with maps $\pi_{M',M} : \mathrm{Gal}(M'/K) \to \mathrm{Gal}(M/K)$ sending $\sigma \mapsto \sigma|_M$ if $M \prec M'$. Then $\{\mathrm{Gal}(M/K)\}_{M\in\mathcal{I}}$ is an inverse system and*

$$\mathrm{Gal}(L/K) \cong \varprojlim \mathrm{Gal}(M/K)$$

3. *Suppose $L/N/K$ such that N/K is (possibly infinite) Galois. Then under the isomorphism $\mathrm{Gal}(L/K) \cong \varprojlim \mathrm{Gal}(M/K)$ we have the identification*

$$\mathrm{Gal}(L/N) = \varprojlim \mathrm{Gal}(M/N \cap M)$$

taking $\mathrm{Gal}(M/N \cap M)$ as a subgroup of $\mathrm{Gal}(M/K)$.

Proof. (1): If $M, M'/K$ are finite Galois then MM'/K is finite Galois and so $\mathcal{I}$ is a directed set.

(2): Consider the map $\phi_M : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ sending $\sigma \mapsto \sigma|_M$. If $M \prec M'$ then $(\sigma|_{M'})|_M = \sigma|_M$ and so $\pi_{M',M} \circ \phi_{M'} = \phi_M$. The universal property of inverse limits yields $\phi : \mathrm{Gal}(L/K) \to \varprojlim \mathrm{Gal}(M/K)$ such that $\phi_M = \pi_M \circ \phi$ where $\pi_M : \varprojlim \mathrm{Gal}(M/K) \to \mathrm{Gal}(M/K)$ is projection onto the M-th coordinate.

(Recall that $\varprojlim G_u = \{(g_u) \in \prod G_u | g_u = \pi_{v,u}(g_v), \forall u \prec v\}$.)

Suppose $\phi(\sigma) = 1$. If $\alpha \in L$ let M be the splitting field of the minimal polynomial of α. Then $\phi_M(\sigma) = 1$ implies $\sigma|_M = \mathrm{id}_M$ and so $\sigma(\alpha) = \alpha$. We deduce $\sigma = 1$ and so ϕ is injective. Reciprocally, if $(\sigma_M) \in \varprojlim \mathrm{Gal}(M/K)$ define $\sigma : L \to L$ by $\sigma(\alpha) = \sigma_M(\alpha)$ for any M containing α (there is always one such M, namely the splitting field of the minimal polynomial of α). This is well-defined as $\sigma_M(\alpha) = \sigma_{M'}(\alpha)$ for any $M \subset M'$. The map σ is clearly a homomorphism, its inverse corresponds by the same procedure to (σ_M^{-1}) and clearly fixes K as each σ_M does. Thus $\sigma \in \mathrm{Gal}(L/K)$ and $\phi(\sigma) = (\sigma_M)$. So ϕ is also surjective.

(3): This is identical to (2). □

Example 186. 1. Remark that $\overline{\mathbb{F}}_p = \cup \mathbb{F}_{p^n}$. The proposition implies that

$$\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \varprojlim \mathbb{Z}/n\mathbb{Z} =: \widehat{\mathbb{Z}} = \prod_q \mathbb{Z}_q$$

where recall that $\mathbb{Z}_q = \varprojlim \mathbb{Z}/q^n\mathbb{Z}$.

2. Suppose p is a prime. Then

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}_p^\times$$

and the composition

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^\times$$

is called the p-cyclotomic character. It governs the behavior of Hodge theory of smooth projective varieties over $\mathbb{Q}_p$.

When $p > 2$ we can say a little more as $(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}$ so

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \varprojlim \mathbb{Z}/p^{n-1}\mathbb{Z} \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$$

3. Going slightly further, let $\mathbb{Q}(\mu_\infty) = \cup\mathbb{Q}(\mu_n)$. Then

$$\mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) \cong \varprojlim(\mathbb{Z}/n\mathbb{Z})^\times \cong \widehat{\mathbb{Z}}^\times \cong \prod_q \mathbb{Z}_q^\times$$

This is the main theorem of Class Field Theory for $\mathbb{Q}$. For finite extensions of $\mathbb{Q}$ it is considerably more difficult as one needs suitable replacements of μ_n which can be found in the torsion of formal groups.

4. Consider the subfield $\mathbb{Q}_\infty$ of $\mathbb{Q}(\mu_{p^\infty})$ fixed under $\mathbb{Z}/(p-1)\mathbb{Z}$. Then $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$. It turns out that $\mathbb{Q}_\infty$ is the only Galois extension of $\mathbb{Q}$ with Galois group $\mathbb{Z}_p$. Leopoldt's conjecture states that if K is the splitting field over $\mathbb{Q}$ of an irreducible polynomial $P(X)$ with r pairs of complex conjugate roots then there are exactly $1 + r$ independent extensions of K with Galois group $\mathbb{Z}_p$. This is still open.

Lecture 35
2015-04-17

Theorem 187 (Main theorem of Galois theory)**.** *Let L/K be infinite Galois. Endow* $\mathrm{Gal}(L/K)$ *with the profinite topology.*

1. *There is a bijection between the set of subextensions $L/M/K$ and the set of (topologically) closed subgroups H of* $\mathrm{Gal}(L/K)$*. The correspondence is the usual $M \mapsto \mathrm{Gal}(L/M)$ and $H \mapsto L^H$.*
2. *M/K is Galois if and only if* $\mathrm{Gal}(L/M) \triangleleft \mathrm{Gal}(L/K)$ *in which case* $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$.
3. *If H is open (and thus also closed) then L^H/K is finite.*

Proof. (1): First we check that $\mathrm{Gal}(L/M)$ is closed in $\mathrm{Gal}(L/K)$ and then show that the two maps are inverses to each other.

Note that $\mathrm{Gal}(L/M) \cong \varprojlim \mathrm{Gal}(N/M \cap N)$ as N/K is finite Galois, from the previous proposition. Since each $\mathrm{Gal}(N/M\cap N)$ is a subgroup of $\mathrm{Gal}(N/K)$ it suffices to show that if H_u is a subgroup of the finite group G_u then $\varprojlim H_u$ is a closed subgroup of $\varprojlim G_u$. It is clearly a subgroup. If $(g_u) \notin \varprojlim H_u$ then $g_{u_0} \notin H_{u_0}$ for some u_0. Consider $U = \{g_{u_0}\} \times \prod_{v \neq u_0} G_v$ which is an open neighborhood of (g_u) clearly disjoint from $\varprojlim H_u$. Thus $\varprojlim H_u$ is closed in $\varprojlim G_u$.

Next, let $\alpha \in L^{\mathrm{Gal}(L/M)}$. Let N be the splitting field of the minimal polynomial of α over K. Then $N/M \cap N$ is finite Galois. Since $\mathrm{Gal}(L/M)$ projects onto $\mathrm{Gal}(N/M \cap N)$ it follows that $\alpha \in N^{\mathrm{Gal}(N/M\cap N)}$ and so $\alpha \in M \cap N$. Thus $L^{\mathrm{Gal}(L/M)} = M$.

Finally, suppose $H \subset \mathrm{Gal}(L/K)$ is a closed subgroup. We want to show that $\mathrm{Gal}(L/L^H) = H$. For M/K finite Galois we have $\pi_M : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$, surjective. Let $H_M = \pi_M(H)$, a subgroup of $\mathrm{Gal}(M/K)$. From the universal property get a homomorphism $H \to \varprojlim H_M$. It is injective using the explicit description of $\varprojlim$ as compatible sequences. Finally, suppose $(\sigma_M) \in \varprojlim H_M$ is a compatible sequence. If $(\sigma_M) \notin H$ then there exists an open neighborhood U of (σ_M) contained in the complement of H. The open set U can be chosen of the form $\prod_{M \prec M_0} \{\sigma_M\} \times \prod_{M \not\prec M_0} \mathrm{Gal}(M/K)$ (simply by choosing M_0 large enough). Let $\sigma \in H$ mapping to σ_{M_0} in H_{M_0} (by definition such a σ exists). Then $\sigma \in U$ as $\pi_M(\sigma) = \sigma_M$ for all $M \prec M_0$, contradicting the fact that $U \cap H = \emptyset$.

What is H_M? Every $\pi_M(\sigma) \in H_M$ fixes $L^H \cap M$ and so $H_M \subset \mathrm{Gal}(M/L^H \cap M)$ whenever M/K is finite Galois. But $L^H \cap M = M^{H_M}$ by definition of H_M and so $\mathrm{Gal}(M/L^H \cap M) = H_M$ by the main theorem of finite Galois theory. We deduce that $H = \varprojlim H_M = \varprojlim \mathrm{Gal}(M/L^H \cap M) = \mathrm{Gal}(L/L^H)$ as desired.

(2): The proof from the finite case carries over.
(3): H open has finite index in $\mathrm{Gal}(L/K)$ (proved this on a homework last semester) and so $\mathrm{Gal}(L^H/K) \cong \mathrm{Gal}(L/K)/H$ is finite. □

Example 188. Let $L/K = \mathbb{Q}(\mu_{p^\infty}, \sqrt[p^\infty]{2})/\mathbb{Q}$. Then $\mathrm{Gal}(L/K) \cong \{\begin{pmatrix} a & b \\ & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}_p)\}$. Indeed, choose ζ_{p^n} such that $\zeta_{p^m}^{p^{m-n}} = \zeta_{p^n}$. Then $\zeta_{p^n} \mapsto \zeta_{p^n}^{a \bmod p^n}$ for all n and $\sqrt[p^n]{2} \mapsto \zeta_{p^n}^{b \bmod p^n} \sqrt[p^n]{2}$ for all n is the automorphism attached to the matrix $\begin{pmatrix} a & b \\ & 1 \end{pmatrix}$.

The Galois group has as nonclosed subgroup $H = \{\begin{pmatrix} 1 & b \\ & 1 \end{pmatrix} | b \in \mathbb{Z}\}$. What is the fixed subfield? Certainly $\mathbb{Q}(\mu_{p^\infty})$ is contained in the fixed field. Then $\mathrm{Gal}(L/L^H)$ is closed and necessarily contains H. However, the smallest closed subgroup containing H is $\{\begin{pmatrix} 1 & b \\ & 1 \end{pmatrix} | b \in \mathbb{Z}_p\}$ with fixed subfield $\mathbb{Q}(\mu_{p^\infty})$ and so $L^H = \mathbb{Q}(\mu_{p^\infty})$.

Lecture 36
2015-04-20

---

6 Representation theory

6.1 G-modules

Definition 189. Let R be a commutative ring. A G-module over R is an R-module M with an action of G such that the action of G is R-linear.

When $R = \mathbb{Z}$ we simply say that M is a G-module.

When $R = F$ is a field we say that M is a representation of G over the field F as M is then automatically an F-vector space.

Proposition 190. *A G-module over R is the same as an $R[G]$-module.*

Proof. If M is a G-module over R define scalar multiplication $\sum a_g[g] \cdot m := \sum a_g g(m)$ which turns M into an $R[G]$-module. Reciprocally, if M is an $R[G]$-module then it is also an R-module. The group G acts on M via $g(m) := [g] \cdot m$. □

Example 191.

1. Let R be any commutative ring.
   (a) S_n acts on R^n by permuting coordinates. Then R^n is an S_n-module over R.
   (b) $R^{n-1} = \{(x_1, \ldots, x_n) \in R^n | \sum x_i = 0\}$ is also an S_n-module over R. This is called the standard representation of S_n over R.
   (c) $\mathrm{GL}(n, R)$ acts on R^n by matrix multiplication and so R^n is a $\mathrm{GL}(n, R)$-module over R. This is called the standard representation of $\mathrm{GL}(n, R)$ over R.
   (d) $\mathrm{GL}(n, R)$ acts on $M_{n \times n}(R)$ by $g \cdot X := gXg^{-1}$. This is called the adjoint of the standard representation.
2. Let L/K be a Galois extension and $G = \mathrm{Gal}(L/K)$.
   (a) Then G acts on both L and $L^\times$ and L and $L^\times$ are then G-modules.
   (b) If $\mu_n \subset L$ then μ_n is a G-module.
3. If G is any group and $\chi : G \to R^\times$ is any homomorphism then consider the $R[G]$-module $R(\chi)$ defined as follows: it is the ring R considered as an $R[G]$-algebra with respect to the homomorphism $R[G] \to R$ given by $\sum a_g[g] \mapsto \sum a_g \chi(g)$.

4. Two special examples.
   (a) μ_n is a D_{2n}-module via symmetries.
   (b) $\mathbb{C}^2$ is a Q_8 module as follows. Writing $Q_8 = \langle I, J\rangle$ let I act on $\mathbb{C}^2$ via the matrix $\begin{pmatrix} i & \\ & -i \end{pmatrix}$ and J via the matrix $\begin{pmatrix} & -1 \\ 1 & \end{pmatrix}$.

There are two goals that we'll pursue:

1. Study $M^G = \{m \in M | g(m) = m, \forall g \in G\}$. We've already seen that if $G = \mathrm{Gal}(L/K)$ and $M = L$ then $M^G = K$ is the main theorem of Galois theory. It is nontrivial and consequential. The ability to compute M^G is very useful.
2. We'd like to classify the finitely generated G-modules over R. For example, when $R = F$ is a field and G is cyclic then $F[G]$ is a quotient of $F[X, X^{-1}]$ and, since $F[X]$ is a PID, we can classify the finitely generated $F[G]$-modules. Over algebraically closed fields, i.e., the study of representation theory over algebraically closed fields, this may be done.

To pursue the first goal we'll study the derived functors of $(-)^G$: group cohomology. To pursue the second goal we'll study the structure of noncommutative rings.

6.2 Group cohomology

6.2.1 Basic examples

Proposition 192. *The map $M \mapsto M^G$ is a functor from G-modules over R to R-modules. This functor is covariant left-exact.*

Proof. Consider R as an $R[G]$-module via $R[G] \to R$ sending $\sum a_g[g]$ to $\sum a_g$. Then $\mathrm{Hom}_{R[G]}(R, M)$ is uniquely defined by where $1 \in R$ goes. Such a homomorphism takes 1 to $m \in M$ such that $m = f(1) = f(g(1)) = g(f(1)) = g(m)$ for all $g \in G$ as G acts trivially on R. Thus $f(1) \in M^G$ and any choice of $f(1) = m \in M^G$ will yield a homomorphism $f(r) = rf(1) \in \mathrm{Hom}_{R[G]}(R, M)$.
Thus $(-)^G = \mathrm{Hom}_{R[G]}(R, -)$ and so we get a covariant left-exact functor. □

Lecture 37
2015-04-22

Definition 193. Let $H^k(G, -)$ be the k-th right derived functor of the left-exact covariant functor $(-)^G$. The previous proposition shows that

$$H^k(G, M) = \mathrm{Ext}^k_{\mathbb{Z}[G]}(\mathbb{Z}, M)$$

Proposition 194. *If $0 \to M' \to M \to M'' \to 0$ is an exact sequence of G-modules then there is a long exact sequence of abelian groups*

$$0 \to (M')^G \to M^G \to (M'')^G \to H^1(G, M') \to H^1(G, M) \to H^1(G, M'') \to H^2(G, M') \to \dots$$

Proof. Follows from the long exact sequence for $\mathrm{Ext}^\bullet_{\mathbb{Z}[G]}(\mathbb{Z}, -)$. □

Example 195. If $G = 1$ is the trivial group then $\mathbb{Z}[G] = \mathbb{Z}$ and so $\mathbb{Z}$ is a free $\mathbb{Z}[G]$-module. Thus

$$H^k(1, M) = \mathrm{Ext}^k_{\mathbb{Z}}(\mathbb{Z}, M) = 0$$

for all $k \geq 1$ while $H^0(1, M) = M^1 = M$.

In the previous example we used that $\mathrm{Ext}(M,N)$ vanishes when M is projective of N is injective. More generally we may compute $H^k(G,M) = \mathrm{Ext}^k_{\mathbb{Z}[G]}(\mathbb{Z},M)$ using either a projective resolution of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module or an injective resolution of M as a $\mathbb{Z}[G]$-module. We will use projective resolutions.

Example 196. Suppose $G \cong \mathbb{Z}/n\mathbb{Z}$ is cyclic generated by $\phi \in G$ and suppose M is a G-module. This general example is problem D1 on the midterm. Note that $\mathbb{Z}[G] = \mathbb{Z}[\mathbb{Z}/n\mathbb{Z}] \cong \mathbb{Z}[X]/(X^n-1)$. Under this isomorphism we get a commutative diagram of exact sequences

$$\begin{array}{ccccccccccccccc}
\ldots & \xrightarrow{\phi-1} & \mathbb{Z}[G] & \xrightarrow{N} & \mathbb{Z}[G] & \xrightarrow{\phi-1} & \mathbb{Z}[G] & \xrightarrow{N} & \mathbb{Z}[G] & \xrightarrow{\phi-1} & \mathbb{Z}[G] & \xrightarrow{\sum} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow\cong & & \downarrow\cong & & \downarrow\cong & & \downarrow\cong & & \downarrow\cong & & \| & & \\
\ldots & \xrightarrow{\cdot(X-1)} & \frac{\mathbb{Z}[X]}{(X^n-1)} & \xrightarrow{\cdot\sum X^i} & \frac{\mathbb{Z}[X]}{(X^n-1)} & \xrightarrow{\cdot(X-1)} & \frac{\mathbb{Z}[X]}{(X^n-1)} & \xrightarrow{\cdot\sum X^i} & \frac{\mathbb{Z}[X]}{(X^n-1)} & \xrightarrow{\cdot(X-1)} & \frac{\mathbb{Z}[X]}{(X^n-1)} & \xrightarrow{P\mapsto P(1)} & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

where the map $\mathbb{Z}[G] \to \mathbb{Z}$ is $\sum a_g[g] \mapsto \sum a_g$ which turns $\mathbb{Z}$ into the trivial $\mathbb{Z}[G]$-module and $N = [1] + [\phi] + \cdots + [\phi^{n-1}] \in \mathbb{Z}[G]$.

This can be checked to be exact and yields a free and therefore projective resolution. Therefore $H^k(G,M)$ can be computed as the k-th cohomology of the image of the above resolution under the covariant functor $\mathrm{Hom}_{\mathbb{Z}[G]}(-,M)$, i.e.,

$$H^k(G,M) = H^k\left(\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],M) \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],M) \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],M) \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],M) \to \ldots\right)$$

Since $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],M) \cong M$ we get

$$H^k(G,M) \cong H^k\left(M \xrightarrow{\phi-1} M \xrightarrow{N} M \xrightarrow{\phi-1} \ldots M \xrightarrow{N} M \to\right)$$

where now $N = 1 + \phi + \cdots + \phi^{n-1} \in \mathrm{End}_{\mathbb{Z}}(M)$ and $\phi - 1 = \phi - \mathrm{id} \in \mathrm{End}_{\mathbb{Z}}(M)$. Immediately we get

$$H^k(G,M) \cong \begin{cases} M^G = M^{\phi=1} & k = 0 \\ M^{N=0}/(\phi-1)(M) & k \geq 1 \text{ odd} \\ M^{\phi=1}/N(M) & k \geq 2 \text{ even} \end{cases}$$

where $M^{\phi=1} = \{m \in M | \phi(m) = m\}$ and $M^{N=0} = \{m \in M | N(m) = 0_M\}$. Here 0_M is the identity in the abelian group M. When M is written multiplicatively then all additions become multiplications and $O_M = 1$ is the multiplicative unit.

1. We now do some explicit computations. Let $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ and $M = \mathbb{C}^\times$. Then $G = \langle c \rangle$ is generated by complex conjugation and so $N(z) = \text{“}1 + c\text{”}(z) = z \cdot c(z) = |z|^2$ while $\text{“}c - 1\text{”}(z) = c(z)/z = \overline{z}/z$ as the group M is written multiplicatively. We compute

$$\begin{aligned} M^{c=1} &= \{z \in \mathbb{C}^\times | z = \overline{z}\} = \mathbb{R}^\times \\ (c-1)(M) &= \{\overline{z}/z | z \in \mathbb{C}^\times\} = \{e^{-2i\theta} | 0 \leq \theta < 2\pi\} = S^1 \\ M^{N=0} &= \{z \in \mathbb{C}^\times | |z|^2 = 1\} = S^1 \\ N(M) &= \{|z|^2 | z \in \mathbb{C}^\times\} = (0,\infty) \end{aligned}$$

   Therefore

$$H^k(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times) = \begin{cases} \mathbb{R}^\times & k = 0 \\ 1 & k \geq 1 \text{ odd} \\ \{\pm 1\} & k \geq 2 \text{ even} \end{cases}$$

2. Again let $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ but now take $M = \mu_n \subset \mathbb{C}^\times$. We compute

$$M^{c=1} = \{z \in \mu_n | z = \overline{z}\} = \mu_n \cap \mathbb{R} = \begin{cases} 1 & n \text{ odd} \\ \pm 1 & n \text{ even} \end{cases}$$

$$(c-1)(M) = \{\overline{z}/z | z \in \mu_n\} = \{e^{-4\pi i k/n}\} = \begin{cases} \mu_n & n \text{ odd} \\ \mu_n/\pm 1 & n \text{ even} \end{cases}$$

$$M^{N=0} = \{z \in \mu_n | |z|^2 = 1\} = \mu_n$$
$$N(M) = \{|z|^2 | z \in \mu_n\} = 1$$

Putting everything together we see that for every $k \geq 0$

$$H^k(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mu_n) = \begin{cases} 1 & n \text{ odd} \\ \pm 1 & n \text{ even} \end{cases}$$

3. On the homework you'll have to show that if $G = \mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) \cong \mathbb{Z}/d\mathbb{Z}$ generated by the Frobenius automorphism $\phi(x) = x^q$ and $M = \mathbb{F}_{q^d}^\times$ then

$$H^k(\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q), \mathbb{F}_{q^d}^\times) = 0$$

whenever $k \geq 1$.

6.2.2 Computing group cohomology in general: cocycles and coboundaries

When G was finite cyclic we saw an explicit simple projective resolution of $\mathbb{Z}$ by free $\mathbb{Z}[G]$-modules. When G is a general finite group we can still find an explicit, albeit more complicated, free resolution.

Consider $\mathbb{Z}[G^k]$, the group ring of $G^k = G \times G \times \cdots \times G$, as a $\mathbb{Z}[G]$-module under the ring homomorphism $\mathbb{Z}[G] \to \mathbb{Z}[G^k]$ defined on basis elements by $[g] \mapsto [(g, g, \ldots, g)]$. Then $\mathbb{Z}[G^k] \cong \bigoplus_{G^k/G} \mathbb{Z}[G]$ is a free $\mathbb{Z}[G]$-module.

Proposition 197. *The following is a free resolution of $\mathbb{Z}[G]$-modules:*

$$\ldots \to \mathbb{Z}[G^3] \xrightarrow{d} \mathbb{Z}[G^2] \xrightarrow{d} \mathbb{Z}[G] \xrightarrow{\sum} \mathbb{Z} \to 0$$

where $d : \mathbb{Z}[G^k] \to \mathbb{Z}[G^{k-1}]$ is defined on basis elements by

$$d(g_1, \ldots, g_k) = \sum_{i=1}^{k} (-1)^{i-1} (g_1, \ldots, \widehat{g_i}, \ldots, g_k)$$

Proof. Explicit computations. For example if $x \in \mathbb{Z}[G]$ is in the kernel of $\sum$ then $x = \sum a_g[g]$ and $\sum a_g = 0$. But then $x = x - \sum a_g[1] = d \sum a_g[(g, 1)]$. □

As a corollary

$$H^k(G, M) = H^k\left(\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], M) \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^2], M) \to \ldots\right)$$

which explicitly means

$$H^k(G, M) = \frac{\ker\left(\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{k+1}], M) \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{k+2}], M)\right)}{\mathrm{Im}\left(\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^k], M) \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{k+1}], M)\right)}$$

Theorem 198. *Let $Z^1(G,M) = \{f : G \to M \text{ any function} | f(gh) = g(f(h)) + f(g), \forall g,h \in G\}$ (the cocycles) and $B^1(G,M) = \{f_m | m \in M\}$ (the coboundaries) where for $m \in M$ the function $f_m : G \to M$ is defined by $f_m(g) = m - g(m)$. Then $B^1(G,M) \subset Z^1(G,M)$ and*

$$H^1(G,M) = Z^1(G,M)/B^1(G,M)$$

Proof. Note that $f \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^k], M)$ is uniquely defined by what it does on basis elements. Let $(g_1, \ldots, g_k) \in G^k$ in which case we only need to specify $f([(g_1, \ldots, g_k)])$. But f is G-linear and so $f([(g_1, \ldots, g_k)]) = f([g_1][(1, g_1^{-1}g_2, \ldots, g_1^{-1}g_k)]) = g_1(f([(1, g_1^{-1}g_2, \ldots, g_1^{-1}g_k)]))$ and so f is uniquely defined by what it does on elements of the form $(1, x_2, \ldots, x_k)$. We conclude that

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^k], M) \cong \mathrm{Maps}(G^{k-1}, M)$$

and we fix an isomorphism by sending $f : \mathbb{Z}[G^k] \to M$ to the map $\phi(g_1, \ldots, g_{k-1}) := f([(1, g_1, g_1g_2, \ldots, g_1g_2 \cdots g_{k-1})])$. This seems peculiar and there are many isomorphisms but this choice makes the formulae for the differential maps particularly nice.

In particular $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], M) \cong M$, $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^2], M) \cong \mathrm{Maps}(G, M)$ and $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^3], M) \cong \mathrm{Maps}(G^2, M)$. We only need to make explicit the differential maps. The map $d : M \to \mathrm{Maps}(G, M)$ is the map $d : \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], M) \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^2], M)$ given by composing with $d([g,h]) = [g] - [h]$. Thus d sends $m \in M \cong \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], M)$ to the map $\phi_m \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^2], M)$ that sends $[(g,h)]$ to $g(m) - h(m)$. To this map we associate $g \mapsto \phi_m([(1,g)]) = f_m$ in $\mathrm{Maps}(G, M)$.

Similarly $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^2], M) \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^3], M)$ is given by composing with $[(g,h,k)] \mapsto [(h,k)] - [(g,k)] + [(g,h)]$. Thus if $\phi \in \mathrm{Maps}(G, M)$ corresponds to $f \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^2], M)$ (i.e., $\phi(g,h) = f([(1, g, gh)])$) then $d\phi$ corresponds to df which takes $[(g,h,k)]$ to $f([(h,k)]) - f([(g,k)]) + f([(g,h)])$. To this map is associated $d\phi \in \mathrm{Maps}(G^2, M)$ defined by

$$d\phi(g,h) = (df)([(1,g,gh)]) = f([(g,gh)]) - f([(1,gh)]) + f([(1,g)]) = g(\phi(h)) - \phi(gh) + \phi(g)$$

We deduce that

$$\ker(\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^2], M) \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^3], M)) = Z^1(G,M)$$

and

$$\mathrm{Im}(\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], M) \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^2], M)) = B^1(G,M)$$

and the theorem follows. □

Lecture 38
2015-04-24

Corollary 199. *If G acts trivially on M then $H^1(G,M) \cong \mathrm{Hom}_{\mathrm{Groups}}(G, M)$.*

Proof. Since G acts trivially on M, $m - g(m) = 0$ so $B^1(G,M) = 0$. Also $Z^1(G,M) = \{f : G \to M | f(gh) = f(h) + f(g)\} = \mathrm{Hom}(G, M)$. □

Proposition 200. *Let H be a subgroup of G and M a G-module. For each $k \geq 0$ there exist homomorphisms*

$$\mathrm{res}^k : H^k(G,M) \to H^k(H,M)$$

and

$$\mathrm{cor}^k : H^k(H,M) \to H^k(G,M)$$

such that $\mathrm{cor}^k \circ \mathrm{res}^k$ is multiplication by $[G:H]$ on $H^k(G,M)$.

Proof. This uses the notion of universal delta functors from homological algebra, which we didn't cover, but let me just say that $\mathrm{res}^0 : M^G \to M^H$ is usual inclusion, res^1 is given by restriction $\mathrm{Maps}(G,M) \to \mathrm{Maps}(H,M)$ and $\mathrm{cor}^0 : M^H \to M^G$ is the averaging map $\mathrm{cor}^0(m) = \sum_{g \in G/H} g(m)$. Then clearly $\mathrm{cor}^0 \circ \mathrm{res}^0 = |G/H| = [G:H]$. □

Corollary 201. *If G is finite and M is a G-module over a vector space of characteristic which does not divide $|G|$ then $H^k(G,M)=0$ for all $k\geq 1$. E.g., $H^k(G,M)=0$ for $k\geq 1$ whenever M is a divisible abelian group.*

Proof. Consider $\mathrm{res}^k : H^k(G,M) \to H^k(1,M)=0$ and $\mathrm{cor}^k : H^k(1,M)=0 \to H^k(G,M)$. Then $\mathrm{cor}^k \circ \mathrm{res}^k = 0$ is multiplication by $|G|$ on the vector space $H^k(G,M)$. Since $|G|$ is invertible in the field this can only happen if the vector space has dimension 0, i.e., if $H^k(G,M)=0$. □

Corollary 202 (Useful in ramification theory)**.** *Let G act trivially on $\mathbb{Z}$. Then*

$$H^2(G,\mathbb{Z}) \cong G^\vee$$

the Pontryagin dual of G.

Proof. Consider the exact sequence $0\to\mathbb{Z}\to\mathbb{Q}\to\mathbb{Q}/\mathbb{Z}\to 0$ which gives

$$H^1(G,\mathbb{Q}) \to H^1(G,\mathbb{Q}/\mathbb{Z}) \to H^2(G,\mathbb{Z}) \to H^2(G,\mathbb{Q})$$

and the previous result yields $H^2(G,\mathbb{Z}) \cong H^1(G,\mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}) = G^\vee$. □

6.2.3 Hilbert 90 and Kummer theory

We've seen that $H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}),\mathbb{C}^\times)=0$ and $H^1(\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q),\mathbb{F}_{q^d}^\times)=0$. In fact this is true for all finite Galois extensions L/K.

Theorem 203 (Hilbert's theorem 90)**.** *If L/K is a finite Galois extension of fields then*

$$H^1(\mathrm{Gal}(L/K),L^\times)=0$$

The same is true if we replace $L^\times$ with L.

Proof. Uses linear independence of characters. □

More generally, when G is a profinite group, e.g., a Galois group, then one can still study group cohomology $H^k(G,M)$ as long as the action of G on M is continuous. This means that $M=\bigcup_{U\subset G} M^U$ as U varies through the open subgroups of G. In that case one defines

$$H^k(G,M) = \varinjlim_{U\subset G} H^k(G/U, M^U)$$

For example when L/K is Galois then

$$H^k(\mathrm{Gal}(L/K),L^\times) \cong \varinjlim_{L/M/K} H^k(\mathrm{Gal}(M/K),M^\times)$$

as M/K is finite Galois. This follows from the fact that $\mathrm{Gal}(L/K)=\varprojlim \mathrm{Gal}(M/K)$ while $L^\times=\bigcup M^\times$. Crucially $H^k(G,-)$ is still the right-derived functor of $(-)^G$ and so one has long exact sequences attached to short exact ones.

Corollary 204. *If L/K is infinite Galois (e.g., $\overline{K}/K$ when K is perfect) then*

$$H^1(\mathrm{Gal}(L/K),L^\times)=0$$

Proof. $H^1(\mathrm{Gal}(L/K),L^\times) = \varinjlim_{L/M/K} H^1(\mathrm{Gal}(M/K),M^\times) = \varinjlim 0 = 0$. □

Proposition 205. *If $\zeta_n\in K$ then $H^1(\mathrm{Gal}(\overline{K}/K),\mu_n)\cong K^\times/(K^\times)^n$. (E.g., we already saw that $H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}),\mu_2) = \mathbb{R}^\times/(0,\infty)=\pm 1$.)*

Proof. Consider the exact sequence $1 \to \mu_n \to \overline{K}^\times \to \overline{K}^\times \to 1$ which gives the long exact sequence (as $\overline{K}^{\mathrm{Gal}(\overline{K}/K)} = K$)

$$K^\times \xrightarrow{x \mapsto x^n} K^\times \to H^1(\mathrm{Gal}(\overline{K}/K), \mu_n) \to H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times)$$

Hilbert 90 shows that $H^1(\mathrm{Gal}(\overline{K}/K), \mu_n)$ is then the cokernel of the n-th power map on $K^\times$, as desired. □

Proposition 206. *Suppose K is a field of characteristic 0 and $\zeta_n \in K$. Then the set of finite cyclic Galois extensions L/K of order dividing n is in bijection with $K^\times/(K^\times)^n$. (E.g., extensions of $\mathbb{Q}$ of degree 1 or 2 are of the form $\mathbb{Q}(\sqrt{d})$ and are in bijection with $d \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, two extensions $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{d'})$ being the same iff d and d' differ by a square factor.)*

Proof. Such extensions L are in bijection, according to Galois theory, with open subgroups of $\mathrm{Gal}(\overline{K}/K)$ which are cyclic and have order dividing n. In other words they are in bijection with homomorphisms $\mathrm{Gal}(\overline{K}/K) \to \mathbb{Z}/n\mathbb{Z}$ associating the such a homomorphism the fixed field of $\overline{K}$ under the kernel of the homomorphism.

Therefore we need to compute $\mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mathbb{Z}/n\mathbb{Z})$. Since $\zeta_n \in K$ then $\mathrm{Gal}(\overline{K}/K)$ acts trivially on $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$ so we need to compute

$$\begin{aligned}\mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mathbb{Z}/n\mathbb{Z}) &= \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mu_n) \\ &\cong H^1(\mathrm{Gal}(\overline{K}/K), \mu_n) \\ &\cong K^\times/(K^\times)^n\end{aligned}$$

□

Remark 16. This yields another proof of the fact that cyclic extensions of K of order dividing n are of the form $K(\sqrt[n]{a})$.

Remark 17. How does one make explicit the isomorphism $\mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mu_n) \cong K^\times/(K^\times)^n$. Suppose $a \in K^\times/(K^\times)^n$. Choose $\sqrt[n]{a}$, which is unique up to an element of μ_n. To this is attached the homomorphism $\mathrm{Gal}(\overline{K}/K) \to \mu_n$ sending σ to $\sigma(\sqrt[n]{a})/\sqrt[n]{a}$. Note that even if this cohomology class seems to be a coboundary, it is not. A coboundary is of the form $\sigma \mapsto \sigma(b)/b$ for $b \in K^\times$ whereas $\sqrt[n]{a} \in K^\times$ iff $a = 1$ in $K^\times/(K^\times)^n$.

Lecture 39
2015-04-27

6.3 A little noncommutative algebra

Definition 207. Let R be a noncommutative ring and M a left R-module. The module M is said to be **simple** if there are no proper sub-R-modules. The module is said to be **semisimple** if it is a direct sum of simple modules.

A ring R is said to be simple/semisimple if it is so as a module over itself.

The fundamental theorem of noncommutative algebra is the following:

Theorem 208 (Wedderburn)**.** *Let K be a field. Every simple K-algebra is of the form $M_{n\times n}(D)$ where D is a division K-algebra.*

Proof. Take for granted. □

Example 209.

1. Every extension L/K is a division K-algebra and so $M_{n\times n}(L)$ is a simple K-algebra.
2. If $K = \mathbb{R}$ let $\mathbb{H} = \mathbb{R} \oplus i\mathbb{R} \oplus j\mathbb{R} \oplus k\mathbb{R}$ with the algebra structure $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$. This is the ring of real quaternions. It is a division ring because

$$(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$$

and so every nonzero element of the algebra is invertible. It is clearly not a field.

Definition 210. A simple K-algebra A is said to be central if $Z(A) = K$.

Proposition 211. *Let K be a field. If A and B are two central simple algebras then $A \otimes_K B$ is a central simple K-algebra.*

Proof. Take for granted. □

Corollary 212. *Let $\mathrm{Br}(K)$ be the set of all central (necessarily simple) division K-algebras. Then $\mathrm{Br}(K)$ is naturally a group, called the* **Brauer group**.

Proof. Suppose $A, B \in \mathrm{Br}(K)$. Then $A \otimes_K B$ is simple and therefore Wedderburn's theorem implies there exists a division K-algebra C such that $A \otimes_K B \cong M_{n\times n}(C)$. Centrality implies that $K = Z(A \otimes_K B) = Z(M_{n\times n}(C)) \cong Z(C)$ and so C is a central division K-algebra. □

Theorem 213. *If K is a field then*

$$\mathrm{Br}(K) \cong H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times)$$

Example 214.

1. Let K be any algebraically closed field, e.g., $K = \mathbb{C}$. Then $\mathrm{Br}(K) \cong H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times) = H^2(1, K^\times) = 0$ and so K itself is the only central division K-algebra, in this case a field. Remark that every extension of K, algebraic or not, is a division K-algebra, but it is not central.

2. Let $K = \mathbb{R}$. Then $\mathrm{Br}(\mathbb{R}) \cong H^2(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times)$ which we already computed to be $\{\pm 1\}$. The field $\mathbb{R}$ is itself in $\mathrm{Br}(\mathbb{R})$ as well as the quaternions $\mathbb{H}$ described above. One consequence of this computation is that $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \cong M_{4\times 4}(\mathbb{R})$. Indeed, $(-1)^2 = 1$ so the group structure shows that the tensor product is a matrix algebra over $\mathbb{R}$. A comparison of dimension yields 4×4.

3. If $\mathbb{F}_q$ is a finite field then $\mathrm{Br}(\mathbb{F}_q) \cong H^2(\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q), \overline{\mathbb{F}}_q^\times) = \varinjlim H^2(\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q), \mathbb{F}_{q^d}^\times) = \varinjlim 0 = 0$. This implies that $\mathbb{F}_q$ is the only central division $\mathbb{F}_q$-algebra.

Corollary 215 (Wedderburn's little theorem)**.** *Every finite division ring is a field.*

Proof. Let D be a finite division ring and let $F = Z(D)$. Then F is stable under addition, multiplication and division and so is a division sub-algebra. It is commutative by definition so it is a finite field, $F = \mathbb{F}_q$. Thus D is a (necessarily) central division $\mathbb{F}_q$-algebra and so $D \cong M_{n\times n}(\mathbb{F}_q)$ as $\mathrm{Br}(\mathbb{F}_q) = 0$. But D is a division ring so $n = 1$ and thus $D = \mathbb{F}_q$, a field. □

Corollary 216. *If K is algebraically closed, e.g., if $K = \mathbb{C}$, then K is the only finite dimensional division K-algebra.*

Proof. Let R be a finite dimensional division K-algebra and let $L = Z(R)$ be the center, necessarily a finite field extension of K. Since K is algebraically closed $L = K$ and so R is a central division K-algebra. Then use $\mathrm{Br}(K) = 0$ to deduce that $R = K$. □

Example 217. Let p be a prime and $\mathbb{Q}_p$ the fraction field of $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. Local class field theory yields $\mathrm{Br}(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$ so the central division $\mathbb{Q}_p$-algebras are in bijection with the divisible group $\mathbb{Q}/\mathbb{Z}$.

If D is a central division $\mathbb{Q}$-algebra then tensoring with $\mathbb{R}$ and $\mathbb{Q}_p$ yields again central division algebras. Global class field theory yields an exact sequence

$$0 \to \mathrm{Br}(\mathbb{Q}) \to \mathrm{Br}(\mathbb{R}) \oplus \bigoplus \mathrm{Br}(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z} \to 0$$

and thus

$$\mathrm{Br}(\mathbb{Q}) \cong \ker\left(\frac{1}{2}\mathbb{Z}/\mathbb{Z} \oplus \bigoplus_{\text{countable}} \mathbb{Q}/\mathbb{Z} \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z}\right)$$

6.4 Representation theory of finite groups

Let G be a finite group and F a field. We would like to study the category of representations of G over F, in other words G-modules over F. A representation is thus a pair (ρ, V) where V is an F-vector space while $\rho : G \to \mathrm{Aut}_F(V)$ is the action homomorphism.

Theorem 218 (Mashke's theorem)**.** *If the characteristic of F is $p \nmid |G|$ then every finite dimensional representation of G over F is semisimple.*

Proof. I decided to skip the proof. I had already written it though.

It suffices to show that if $W \subset V$ is a subrepresentation then $V \cong W \oplus U$ for some subrepresentation U. Then inductively we can write V as a direct sum of simple modules as the process has to terminate by dimension considerations.

Suppose $W \subset V$ is a sub-F-vector space which is stable under the action of G. Let $\pi : V \to W$ be any vector space projection, i.e., any vector space homomorphism such that $\pi|_W = \mathrm{id}_W$ and $\pi^2 = \pi$. Define

$$\widetilde{\pi}(v) = \frac{1}{|G|} \sum_{g \in G} g^{-1}(\pi(g(v)))$$

which is clearly a vector space homomorphism $V \to W$ as $\pi(g(v)) \in W$ and W is stable under G. Moreover,

$$\widetilde{\pi}(h(v)) = \frac{1}{|G|} \sum g^{-1}(\pi(g(h(v)))) = h(\widetilde{\pi}(v))$$

and so $\widetilde{\pi} : V \to W$ is a $F[G]$-module homomorphism. It's also clear that $\widetilde{\pi}^2 = \widetilde{\pi}$ and $\widetilde{\pi}|_W = \mathrm{id}_W$. The natural inclusion $W \to V$ is an $F[G]$-linear section to $\widetilde{\pi}$ and so $V \cong W \oplus \ker \widetilde{\pi}$ as $F[G]$-modules. □

From now on we restrict to representations of G on complex vector spaces. Mashke's theorem implies that every finite dimensional complex representation of G is a direct sum of irreducible representations. It is therefore desirable to determine the set of all irreducible representations.

Proposition 219. $\mathbb{C}[G] \cong \oplus M_{n_i \times n_i}(\mathbb{C})$ *for* $1 \leq i \leq d$.

Proof. $\mathbb{C}[G]$ is a finite dimensional module over itself and therefore it is semisimple and thus a direct sum of simple $\mathbb{C}$-algebras. Recalling that $\mathbb{C}$ is the only finite dimensional division $\mathbb{C}$-algebra, Wedderburn's theorem yields the result. □

Lecture 40
2015-04-29

I explained that

$$\mathbb{C}[G] \cong \oplus_V \mathrm{End}_{\mathbb{C}}(V)$$

where V ranges through the set of all irreducible finite dimensional complex representations of G, if G is finite.

Then I explained that the natural group ring structure on $\mathbb{C}[G]$ is isomorphic to the ring of functions $\mathrm{Maps}(G, \mathbb{C})$ with addition and the convolution product. The explicit isomorphism between $\mathrm{Maps}(G, \mathbb{C})$ and $\oplus \mathrm{End}_{\mathbb{C}}(V)$ is given by Fourier transforms.

We deduced that the Fourier transform of the convolution of two functions is the product of the Fourier transforms of the functions.

I finished with the following example. Suppose a cyllinder has a grid with m rows and n columns. The goal is two write reals in the $m \times n$ squares, not all 0, such that the real in each square is equal to the sum of the reals in the adjacent squares. I showed that this can be done if and only if there exist integers k and l such that $m + 1 \nmid k$ and

$$\cos\left(\frac{k\pi}{m+1}\right) + \cos\left(\frac{2l\pi}{n}\right) = \frac{1}{2}$$

Actually I only showed that if the cyllindrical table can be filled then there exist k and l satisfying the above formula.