

Normal basis theorem

math center

The familiar normal basis theorem states that:

Theorem 0.1. Let $L|K$ be a finite Galois extension with Galois group G . Then $L \simeq K[G]$ as left G -modules.

In other words, L viewed as a representation is isomorphic to the regular representation of G . It then follows that

$$H^r(G, L) = H^r(G, K[G]) = H^r(G, \text{Ind}_{\{1\}}^G(K)) = 0,$$

for all $r > 0$, where the last equality is Shapiro's lemma.

1 Field theoretic proof

Let's only sketch this proof because it's somewhat long, although being quite elegant otherwise.

Lemma 1.1 (Linear independence of characters). If K is an integral domain and G is a monoid, then the set of characters $\text{Hom}_{\text{Mon}}(G, K^\times)$ is linear independent over K .

Of course, we only need the case of K a field and G a group.

Proof. Let χ_1, \dots, χ_n be characters. Consider the set

$$\mathcal{S} := \{(c_1, \dots, c_n) \in K^n \setminus 0 : c_1\chi_1 + \dots + c_n\chi_n = 0\}$$

Let (a_1, \dots, a_n) be an element of \mathcal{S} such that $n := |\{i : a_i \neq 0\}|$ is minimal. Because $\chi(1) = 1$ for any character χ , $n > 1$. Thus we may assume WLOG that $a_1, a_2 \neq 0$. Let $h \in G$ be a constant to be determined. Notice that

$$-a_1\chi_1(gh) = \sum_{i>1} a_i\chi_i(gh) = \sum_{i>1} a_i\chi_i(g)\chi_i(h),$$

and also

$$-a_1\chi_1(gh) = -a_1\chi_1(g)\chi_1(h) = \sum_{i>1} a_i\chi_i(g)\chi_1(h).$$

Pick $h \in G$ such that $\chi_1(h) \neq \chi_2(h)$. On subtracting the two equations, we obtain a nonzero linear relation which clearly contradicts the minimality of (a_i) . \square

We first prove the theorem for infinite K . This amounts to the following two facts.

- (I) Given that K is infinite, for any K -algebra A and $L|K$, the set $\text{Hom}_{K\text{-Alg}}(A, L)$ is algebraically independent over L .
- (II) Let $\{x_\sigma \in L : \sigma \in G\}$ be a set of elements indexed by G , then it is a basis if and only if $\det(\tau(x_\sigma))_{\sigma, \tau} \neq 0$.

Since there exists a basis indexed by G , the formal polynomial (modulo abuse of notation) $\det(\tau(X_\sigma))_{\sigma,\tau} \neq 0$. We may plug in $X_\sigma = \sigma(\cdot)$, and by (I), there must exist $x \in L$ such that $\det(\tau\sigma(x))_{\sigma,\tau} \neq 0$. We apply (II) one more time to see that $\{\sigma(x)\}$ is indeed a basis of L .

(II) follows from Lemma 1.1.

(I) is more tricky to prove. We need to show that $P(\chi_1, \dots, \chi_n) \neq 0$ for some nonzero polynomial $P \in L[X_1, \dots, X_n]$. The set

$$\{(\chi_1(a), \dots, \chi_n(a)) : a \in A\}$$

generates the L -vector space L^n by Lemma 1.1, hence there must exist a_1, \dots, a_n such that the matrix $(\chi_i(a_j))_{i,j}$ is invertible. Consider the map

$$\begin{aligned} K^n &\longrightarrow A \\ (k_1, \dots, k_n) &\longmapsto \sum_i k_i a_i \end{aligned}$$

composed with $P(\chi_1(\cdot), \dots, \chi_n(\cdot))$. This is non-zero as a formal polynomial because $P \neq 0$, thus it must also be non-zero as a function. Here we used that K is infinite. This concludes the proof of (I).

Now, suppose that $L|K$ is a cyclic extension, $G = \langle \sigma \rangle$. This clearly includes every finite K . In this scenario, we view L as a $K[X]$ -module via $X \rightsquigarrow \sigma$, and the structure theorem factorizes L as the sum of invariant subspaces

$$L \simeq \frac{K[X]}{(P_1)} \oplus \cdots \oplus \frac{K[X]}{(P_r)}, \quad P_1 | \cdots | P_r.$$

Since $L|K$ is finite, $P_i \neq 0$. By Lemma 1.1, we also can't have $0 < \deg(P_i) < [L : K]$. Thus the only possibility is $L \simeq K[X]/(X^{[L:K]} - 1)$. The basis $\{1, X, \dots, X^{[L:K]-1}\}$ pulls back along this isomorphism as a normal basis.

For more details, see Thm 9.5.6 [here](#).

2 Module theoretic proof

The idea is to use the following result.

Proposition 2.1. Let G be a group, and let $L|K$ be a finite extension of fields. Then the base change functor $L \otimes - : K[G]\text{-Mod} \longrightarrow L[G]\text{-Mod}$ is conservative, i.e., if two $K[G]$ -modules V, W satisfy $L \otimes V \simeq L \otimes W$, then $V \simeq W$. Here by “module” we always mean modules that are finite-dimensional over K .

The assumption that $L|K$ is finite can be dropped in this result; see end of this note.

Proof. Recall the Krull-Remak-Schmidt theorem: If M is a R -module of finite length, then there exists a unique (up to isomorphism and reordering) decomposition of M into indecomposable modules:

$$M \simeq \bigoplus_{i=1}^n M_i.$$

All modules have finite length under the assumption we noted.

If $L \otimes V \simeq L \otimes W$ as $L[G]$ -modules, they must be isomorphic as $K[G]$ -modules as well. The result then follows from

$$L \otimes V \simeq V^{\oplus [L:K]}, \quad \text{in } K[G]\text{-Mod},$$

and comparing the indecomposable components of both sides. \square

This easy fact from representation theory now allows us to give a proof without worrying about the finiteness of K . More specifically, we will establish the following isomorphisms of *right* $K[G]$ -modules¹

$$L \otimes_K \textcolor{red}{L} \xrightarrow{\sim} \prod_{\sigma \in G} L_\sigma \xleftarrow{\sim} L \otimes \textcolor{red}{K}[G]$$

where the actions are given by $l \cdot \tau := \tau^{-1}(l)$, $e_\sigma \cdot \tau := e_{\sigma\tau}$ and the right multiplication of $K[G]$, respectively.

2.1 The first isomorphism

This is given by

$$\begin{aligned} L \otimes_K L &\xrightarrow{\sim} \prod_{\sigma \in G} L_\sigma \\ l \otimes m &\longmapsto (l\sigma(m))_\sigma \end{aligned}$$

Evidently, this defines a homomorphism of right G -modules, so it suffices to prove this is a bijection. There are two ways to see this. The first idea is to use Lemma 1.1. Let b_1, \dots, b_d be a K -basis of L , then any element of $L \otimes_K L$ can be put in the form

$$\sum_{i=1}^d l_i \otimes b_i \longmapsto \left(\sum_{i=1}^d l_i \sigma(b_i) \right)_\sigma$$

Thus the matrix of this homomorphism is $(\sigma(b_i))_{\sigma,i}$, which is invertible precisely by the linear independence of characters. Hence the map is an isomorphism.

A completely different approach is given by the primitive element theorem. Let

$$L = K(\alpha) \simeq K[X]/(P), \quad \text{basis: } \{1, \alpha, \alpha^2, \dots\}.$$

Then

$$L \otimes_K L \simeq L \otimes K[X]/(P) = L[X]/(P) \xrightarrow[\text{CRT}]{} \prod_{\sigma} L_\sigma.$$

Since $P(X) = \prod_{\sigma} (X - \sigma(\alpha))$, we confirm this defines the same map as above.

Remark 2.2. I think it makes some sense to call this isomorphism “the normal basis theorem”, which is itself just primitive element thm + CRT. Galois!

Remark 2.3. If we write the RHS as $\text{Map}(G, L)$, then this isomorphism generalizes to infinite $L|K$, with an small extra smoothness condition.

¹They are of course also (left) L -linear, but we don't need it, as we saw in the proof of Proposition 2.1.

2.2 The second isomorphism

This is given by

$$\begin{aligned} L \otimes K[G] &\xrightarrow{\sim} \prod_{\sigma \in G} L_\sigma \\ l \otimes \sigma &\longmapsto le_\sigma \end{aligned}$$

It turns out that this map is natural, so there are a ton of ways to see it. For example, both sides are the induced module of the $K[G^{\text{op}}]$ -module L equipped with a trivial right G -action.

The End

As we noted,
Compiled on 2025/11/04.
[Home page](#)