

The purpose of these notes is to prove the following theorem.

Theorem 1. *Let F be a field containing a primitive n -th root of unity ζ . Let E/F be a cyclic extension of degree n . Then $E = F[\beta]$ for some β with $\beta^n \in F$.*

Note that we have already proved the converse. Also, both the theorem and the converse are proved in Milne's text.

We will use the normal basis theorem.

Theorem 2. *Let E/F be a finite Galois extension with $G = \text{Gal}(E/F)$. Then there exists $\alpha \in E$ such that $\{g\alpha \mid g \in G\}$ is an F -basis for E .*

Proof of Theorem 1. Let $G := \text{Gal}(E/F)$ be generated by γ . Using Theorem 2, let $\{\gamma^i \alpha \mid i = 0, \dots, n-1\}$ be a basis for E over F . Then set

$$\beta = \sum_{i=0}^{n-1} \zeta^i \gamma^i(\alpha).$$

Note that $\gamma(\beta) = \sum_{i=0}^{n-1} \zeta^i \gamma^{i+1} \alpha = \sum_{i=1}^n \zeta^{i-1} \gamma^i \alpha = \sum_{i=1}^{n-1} \zeta^{i-1} \gamma^i \alpha = \zeta^{-1} \beta$. Therefore, for all $k \in \mathbf{Z}$, $\gamma^k \beta = \zeta^{-k} \beta$. Set $N\beta = \prod_{g \in G} g\beta$. Then clearly $N\beta \in E^G = F$. On the other hand, we compute that $N\beta = \beta^n \prod_{i=0}^{n-1} \zeta^{-i}$. Therefore, $\beta^n \in F$.

Now set $L = F[\beta]$. We have $\text{Gal}(E/L) = \{g \in G \mid g\beta = \beta\}$. But, for $i = 0, 1, \dots, n-1$, we have $\gamma^i \beta = \zeta^{-i} \beta = \beta \Leftrightarrow i = 0$. Therefore $\text{Gal}(E/L) = \{1\}$. Therefore $E = L$. Q.E.D.

Now, we need Theorem 2 only in the case that E/F is a cyclic extension. To prove this, I am going to use a result that is very important in its own right, namely, the theorem on independence of characters. Let Λ be a group and E a field. A *character* of Λ into E is simply a group homomorphism $\chi : \Lambda \rightarrow E^\times$. Write Λ^\vee for the set of all characters. We can consider Λ^\vee as a subgroup of the group $\text{Hom}_{\text{Sets}}(\Lambda, E^\times)$ of all functions $f : \Lambda \rightarrow E^\times$. Here the multiplication on functions $f, g \in \text{Hom}_{\text{Sets}}(\Lambda, E^\times)$ is given by $fg(\lambda) = f(\lambda)g(\lambda)$. We can, in turn, consider $\text{Hom}_{\text{Sets}}(\Lambda, E^\times)$ as a subset of the vector space $\text{Hom}_{\text{Sets}}(\Lambda, E)$.

Theorem 3. *Let Λ be a group, E a field and let $\{\chi_1, \dots, \chi_n\}$ be a finite set of characters. Then the χ_i are linear independent in $\text{Hom}_{\text{Sets}}(\Lambda, E)$.*

Proof. Suppose the theorem is false. Let n be the minimum cardinality for which it fails and let $\sum_{i=1}^n \alpha_i \chi_i = 0$ be a dependence relation (for a group Λ , a field E and a non-negative integer n). Clearly, $n > 1$ and, by the minimality of n , all the α_i are non-zero. We can therefore assume $\alpha_1 = 1$. If χ is any character of Λ , then $\sum_{i=1}^n \alpha_i (\chi \chi_i)(\lambda) = \chi(\lambda) \sum_{i=1}^n \alpha_i \chi_i(\lambda) = 0$. Therefore, $\sum_{i=1}^n \alpha_i \chi \chi_i = 0$ as well. We may therefore assume that $\chi_1 = 1$. Now, since the χ_i we started with were distinct, $\chi_2 \neq 1$. Therefore, there exists $\mu \in \Lambda$ such that $\chi_2(\mu) \neq 1$. Now, for all $\lambda \in \Lambda$ we have

$$\sum_{i=1}^n \alpha_i \chi_i(\lambda \mu) = \sum_{i=1}^n \alpha_i \chi_i(\mu) \chi_i(\lambda) = 0.$$

It follows that

$$\sum_{i=1}^n \alpha_i (1 - \chi_i(\mu)) \chi_i = \sum_{i=2}^n \alpha_i (1 - \chi_i(\mu)) \chi_i = 0.$$

Since $\chi_2(\mu) \neq 0$, this is a non-trivial dependence relation. However, it has $n-1$ terms and this contradicts our assumption on the minimality of n .

Proof of Theorem 2 in the cyclic case. Suppose G is generated by $\gamma \in G$. Then, γ is an F -linear transformation of E and, by the homework, we can find γ -cyclic F subspaces V_i of E and polynomials $p_i \in F[t]$ such that $p_i(\gamma) = 0$, $p_1 | p_2 | \dots | p_r$, $\deg p_i = \dim V_i$ and $E = \bigoplus_{i=1}^r V_i$. Now $\gamma^n - 1 = 0$ on E . It follows that all of the p_i divide the polynomial $x^n - 1$. Thus $p_r | x^n - 1$. If $p_r = x^n - 1$ then $r = 1$ since $\deg p_i = 1$. Otherwise, we have $\deg p_r < n$. This implies that the characters $g^i : E^\times \rightarrow E^\times$ as i ranges from 0 to $n-1$ are linearly dependent contradicting Theorem 3. Thus we must have $r = 1$, and V itself is cyclic. Thus we can find an $\alpha \in E$ such that $v, gv, g^2v, \dots, g^{n-1}v$ span V . Q.E.D.