Fixing the gap in Lemma 7.16

MRQ

April 28, 2017

In the proof of Lemma 7.16, it is asserted that

$$\alpha = \beta + \varepsilon(\beta\phi) + \varepsilon^2(\beta\phi^2) + \cdots + \varepsilon^{p-1}(\beta\phi^{p-1})$$

is an element such that $\alpha\phi \neq \alpha$ and $(\alpha^p)\phi = \alpha^p$. However, the justification of the first is that $\alpha\phi = \varepsilon^{-1}\alpha$ and that $\varepsilon \neq 1$, so that $\alpha\phi \neq \alpha$. The problem is that we don't necessarily know $\alpha \neq 0$ and without checking α is non-zero, the conclusion is invalid.

The fix is to use the following:

Lemma 1 *Let K be a finite normal extension of a field F of characteristic zero and suppose that* $\mathrm{Gal}(K/F)$ *is cyclic of order p generated by some element ϕ. Then there exists some $x \in K$ such that*

$$\alpha = x + \varepsilon(x\phi) + \varepsilon^2(x\phi^2) + \cdots + \varepsilon^{p-1}(x\phi^{p-1}) \neq 0.$$

We can then use this α in Lemma 7.16 and the rest of the argument will work.

Proof: We first claim that there exists there does not exist non-zero scalars $\lambda_0, \lambda_1, \ldots, \lambda_{p-1}$ in F such that

$$\lambda_0 x + \lambda_1(x\phi) + \cdots + \lambda_{p-1}(x\phi^{p-1}) = 0$$

for all $x \in K$. Suppose, for a contradiction, that such λ_i exist. Choose n to be as small as possible such that there exist non-zero $\lambda_0, \lambda_1, \ldots, \lambda_n \in F$ with

$$\lambda_0 x + \lambda_1(x\phi) + \cdots + \lambda_n(x\phi^n) = 0 \tag{1}$$

for all $x \in K$. Our assumption ensures $n \leqslant p-1$, while $n \geqslant 2$ since K contains non-zero elements.

Consider any non-zero y in K and substitute yx for x in the above equation and use the fact that the powers of ϕ are automorphisms to conclude:

$$\lambda_0 yx + \lambda_1(y\phi)(x\phi) + \cdots + \lambda_n(y\phi^n)(x\phi^n) = 0 \tag{2}$$

for all $x \in K$. Now multiply Equation (1) by $y\phi^n$ and subtract Equation (2) to conclude

$$\lambda_0(y\phi^n - y)x + \lambda_1(y\phi^n - y\phi)(x\phi) + \cdots + \lambda_{n-1}(y\phi^n - y\phi^{n-1})(x\phi^n) = 0$$

for all $x \in K$. Since $n \leqslant p-1$, ϕ^n is not the identity map and hence we can choose y such that $y\phi^n \neq y$. Hence we have an equation with fewer than n terms and with coefficients $\mu_i = \lambda_i(y\phi^n - y\phi^i)$, not all of which are zero, contrary to our minimality assumption on n.

In conclusion, there does not exist non-zero coefficients λ_i satisfying

$$\lambda_0 x + \lambda_1(x\phi) + \cdots + \lambda_{p-1}(x\phi^{p-1}) = 0$$

for all $x \in K$. In particular, specialising to $\lambda_i = \varepsilon^i$, there exists some $x \in K$ such that

$$x + \varepsilon(x\phi) + \cdots + \varepsilon^{p-1}(x\phi^{p-1}) \neq 0.$$

□