CATEGORY THEORY Lesson 0429 - Solutions
DR. PAUL L. BAILEY Friday, May 1, 2020

I don't see any uploads in the assignments I made in Microsoft Classroom. Please try to write the solutions to these problems and upload them by tomorrow. I took out the hard part.

Problem 1. Let E/F be a finite separable extension.

(a) Show that $|\mathrm{Aut}(E/F)| \leq [E : F]$.

(b) Show that if E/F is normal, then $|\mathrm{Aut}(E/F)| = [E : F]$.

Proof. Suppose E/F is finite and separable. Then E/F is primitive, so there exists $\alpha \in E$ such that $E = F[\alpha]$. Let $f \in F[X]$ be the minimum polynomial of α. Then $[E : F] = \deg(f)$, and there are at most $\deg(f)$ distinct roots of f in E. Let B denote the set of these roots, so $B \subset E$ and $|B| \leq \deg(f)$. Every automorphism of E preserves B as a set. Moreover, for each $\beta \in B$, there exists a unique isomorphism $\phi_\beta : F[\alpha] \to F[\beta]$ which preserves F pointwise and sends α to β.

Since $\beta \in E = F[\alpha]$, then $F[\beta] \subset F[\alpha]$, and since $[F[\beta] : F] = \deg(f) = [E : F]$, we must that $F[\beta] = F[\alpha] = E$. In this case, ϕ_β is an automorphism of E, and every automorphism of E is of this form. So there is one automorphism of E/F for each element in B; that is,

$$|\mathrm{Aut}(E/F)| = |B| \leq \deg(f) = [E : F].$$

This shows **(a)**.

If additionally E/F is a normal extension, then f splits in E, and since E/F is separable, f splits into distinct factors, so f has exactly $\deg(f)$ roots in E; thus

$$|\mathrm{Aut}(E/F)| = |B| = \deg(f) = [E : F].$$

This shows **(b)**. □

Problem 2 (Bilbo's Lemma)**.** Let E/F be a field extension. Let K be a subfield of E which contains F. Let $\alpha \in E$ be algebraic over F. Let $f \in F[X]$ be the minimum polynomial of α over F, and let $g \in K[X]$ be the minimum polynomial of α over K. Show that g divides f in $K[X]$.

Proof. We use the division algorithm; divide g into f to obtain $q, r \in K[X]$ such that

$$f = gq + r \quad \text{with} \quad \deg(r) < \deg(g).$$

Plug in α to get

$$f(\alpha) = g(\alpha)q(\alpha) + r(\alpha).$$

Since $f(\alpha) = g(\alpha) = 0$, we get $r(\alpha) = 0$. But g is a nonzero polynomial of minimal degree which annihilates α, and since $\deg(r) < \deg(g)$ and r annihilates α, we must have $r = 0$. Thus $f = gq$, and g divides f in $K[X]$. □

Problem 3. Let E/F be a field extension. Let K be a subfield of E which contains F. Show that if E/F is normal, then E/K is normal.

Proof. Suppose E/F is a normal extension. Let $g \in K[X]$ have a root α in E; we wish to show that g splits in E. Let f be the minimum polynomial of α over F. By Bilbo's Lemma, g divides f. Thus all of the roots of g are also roots of f. But E/F is normal, so those roots are all in E. Thus g splits in E, and E/K is normal. □

Let $H \leq \mathrm{Aut}(E)$. The *fixed field* of H is

$$\mathrm{Fix}(H) = \{x \in E \mid \phi(x) = x \text{ for all } \phi \in H\}.$$

Problem 4. Let E/F be a finite separable extension. Let $H \leq \mathrm{Aut}(E/F)$. Let $K = \mathrm{Fix}(H)$. Show that K is a subfield of E which contains F.

Proof. Let $\phi \in H$ and $x, y \in K$. Then $\phi(k) = k$ for every $k \in K$. Now

(S0) $\phi(1) = 1$, so $1 \in K$, so $1 \in K$.

(S1) $\phi(x + y) = \phi(x) + \phi(y) = x + y$, so $x + y \in K$.

(S2) $\phi(-x) = -\phi(x) = -x$, so $-x \in K$.

(S3) $\phi(xy) = \phi(x)\phi(y) = xy$, so $xy \in K$.

(S4) if $x \neq 0$, then $\phi(x^{-1}) = \phi(x)^{-1} = x^{-1}$, so $x^{-1} \in K$.

Thus K is a subfield of E. $\square$