Algebra II, Spring 2017

Solutions to Problem Set 5

1. Assume the transcendence degree of K/F is m. Since we have shown that every algebraically independent set of K over F can be extended to a transcendence basis, and since we know any transcendence basis of K/F has m elements, it follows that the transcendence degrees of E/F and K/F are finite.

Let $A = \{\alpha_1, \ldots, \alpha_n\}$ be a transcendence basis of E/F and $B = \{\beta_1, \ldots, \beta_m\}$ a transcendence basis of K/E. Then we show $A \cup B$ is a transcendence basis for K/F. If elements of $A \cup B$ are algebraically dependent, then there are polynomials $f_{d_1,\ldots,d_m} \in F[x_1, \ldots, x_n]$ not all equal to zero such that

$$\sum_{(d_1,\ldots,d_m)} f_{d_1,\ldots,d_m}(\alpha_1, \ldots, \alpha_n)\beta_1^{d_1} \ldots \beta_m^{d_m} = 0$$

But this contradicts the fact that the β_i are algebraically independent over E.

We also need to show K is algebraic over $F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$. This is true since K is algebraic over $E(\beta_1, \ldots, \beta_m)$ and $E(\beta_1, \ldots, \beta_m)$ is algebraic over $F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$.

2. (a) It is enough to show that if A is a finite subset of K which is algebraically independent over F, then A is algebraically independent over E. Assume to the contrary, and set $A = \{\alpha_1, \ldots, \alpha_n\}$. Then there is i such that $\{\alpha_1, \ldots, \alpha_i\}$ is algebraically independent over E but $\{\alpha_1, \ldots, \alpha_{i+1}\}$ is algebraically dependent over E. Then by the lemma proved in class, α_{i+1} is algebraic over $E(\alpha_1, \ldots, \alpha_i)$. But then since E is algebraic over F, $E(\alpha_1, \ldots, \alpha_i)$ is algebraic over $F(\alpha_1, \ldots, \alpha_i)$, so α_{i+1} is algebraic over $F(\alpha_1, \ldots, \alpha_i)$ contradicting the assumption that A is algebraically independent over F.

(b) Since K is finitely generated over F, it has a finite transcendence degree over F (we proved this in class.), and therefore E has also a finite transcendence degree over F. Let A be a finite transcendence basis for E over F. Then replacing F by $F(A)$ we can assume from the beginning that E is algebraic over F. (since if E is finitely generated over $F(A)$, it is also finitely generated over F.)

So assume E/F is algebraic. To show E/F is finitely generated, it is enough to show E/F is a finite extension. Let B a finite transcendence degree for K over F. Then $K/F(B)$ is algebraic and also finitely generated, therefore it is a finite extension. Assume $m = [K : F(B)]$. We show $[E : F] \leq m$. If $\gamma_1, \ldots, \gamma_r$ is a basis for E over F, then the γ_i are linearly independent as elements of K over $F(B)$: if $c_1\gamma_1 + \cdots + c_r\gamma_r = 0$, $c_i \in F(B)$, then after multiplying by the common denominator, we get a linear relation between the γ_i where the coefficients come from $F[B]$. But this implies that B is algebraically dependent over E which is not possible by part (a), so $r \leq m$.

3. $f(x) = x^4 + x + 1$ mod 2. Obviously this polynomial does not have any root in $\mathbf{F}_2$, and since the only irreducible polynomial of degree 2 in $\mathbf{F}_2$ is $x^2 + x + 1$ and $(x^2 + x + 1)^2 \neq x^4 + x + 1$, we conclude that $f(x)$ is irreducible modulo 2. Since $f'(x) = 1 \neq 0$, we conclude that the roots of $f(x)$ are distinct in $\overline{\mathbf{F}}_2$. So the Galois group contains a 4-cycle. On the other hand, $f(x) = x^4 + 2x^2 + x = x(x^3 + 2x + 1)$ mod 3, and $x^3 + 2x + 1$ is irreducible in $\mathbf{F}_3$ since it has no root mod 3, so the Galois group has a 3-cycle. (note that $(x^3 + 2x + 1)' \neq 0$, so the roots of $f(x)$ mod 3 are all distinct. The only subgroup of S_4 which contains a 3-cycle and a 4-cycle is S_4.

4. We have $f(x) = x(x - 1)(x + 1)(x + 2)(x^2 + 2)$ mod 5, and $x^2 + 2$ is irreducible with a non-zero derivative mod 5, so the roots of $f(x)$ are all distinct in $\overline{\mathbf{F}}_5$, so the Galois group contains a 2-cycle. On there other hand, $f(x) = x^6 + x^4 + x^2 + x + 1$ mod 2. We claim that $f(x)$ is irreducible mod 2. Clearly $f(x)$ has no root $\mathbf{F}_2$, so if it is irreducible, it has to have a factor of degree 2 or a factor of degree 3. The only irreducible polynomial of degree 2 mod 2 is $x^2 + x + 1$ and the only irreducible polynomials of degree 3 mod 2 are $x^3 + x + 1$ and $x^3 + x^2 + 1$, and it is easy to see that none of these 3 polynomials divide $f(x)$ mod 2, so $f(x)$ is irreducible, and therefore the Galois group contains a 6-cycle.

5. Let $\sigma_1, \sigma_2 \in \mathrm{Aut}(\bar{\mathrm{F}}/\mathrm{F})$ and $\alpha \in \bar{F}$. Then α is algebraic over F, so $F(\alpha)$ is a finite extension of F. Since every finite extension of a finite field is a Galois extension, $F(\alpha)$ is a Galois extension of F, and therefore, σ_1 and σ_2 give automorphisms of $F(\alpha)$. (in other words, every element β of $F(\alpha)$ should be mapped to another element of $F(\alpha)$ by σ_1 and σ_2 since the minimal polynomial of β splits in $F(\alpha)$.) Since the Galois group of every finite extension of a finite field is abelian, $\sigma_1\sigma_2(\alpha) = \sigma_2\sigma_1(\alpha)$.