Math 30820 Honors Algebra 4
Homework 5

Andrei Jorza

Due Wednesday, 2/22/2017

Do 4 of the following questions. Some questions may be obligatory. Artin a.b.c means chapter a, section b, exercise c. You may use any problem to solve any other problem.

Throughout this problem set R is an **integral domain**, unless otherwise specified.

1. (You must do this problem. It's a more streamlined version of the proof I presented in class.) Suppose K/F is the splitting field of $P(X) \in F[X]$ and $Q(X) \in F[X]$ is an irreducible polynomial with roots α, β.

   (a) Show that $K(\alpha)$ (respectively $K(\beta)$) is the splitting field of $P(X)$ over $F(\alpha)$ (respectively $F(\beta)$).

   (b) Show that $K(\alpha) \cong K(\beta)$.

   (c) Deduce that K/F is a normal extension.

   Proof. (a): Suppose P has roots $u_1, \dots, u_n$. Then the splitting field of P over any field S that contains F is $S(u_1, \dots, u_n)$. Over F this is $K = F(u_1, \dots, u_n)$ while over $F(\alpha)$ it is $F(\alpha, u_1, \dots, u_n) = K(\alpha)$.

   (b): Since Q is irreducible there is an isomorphism $f : F(\alpha) \to F(\beta)$ such that $f|_F = \mathrm{id}_F$ and $f(\alpha) = \beta$. As $P \in F[X]$ it follows that $f(P(X)) = P(X)$. From class we know that there exists an isomorphism ϕ between the splitting field $K(\alpha)$ of P over $F(\alpha)$ and the splitting field $K(\beta)$ of P over $F(\beta)$ such that $\phi|_{F(\alpha)} = f$.

   (c): If $\alpha \in K$ then $K = K(\alpha) \cong K(\beta)$ and so $[K(\beta) : K] = 1$ which implies $K(\beta) = K$ so $\beta \in K$. This implies that if Q has a root in K then all its roots are in K as desired. ☐

2. (You must do this problem.) Let k be a field and $k(x)$ be the field of rational functions in the variable x. Let $t = \dfrac{P(x)}{Q(x)} \in k(x)$ with P and $Q \neq 0$ coprime in $k[x]$. Denote by $k(t)$ the subextension of $k(x)$ generated by t.

   (a) Show that the polynomial $R(Y) = P(Y) - tQ(Y) \in k(t)[Y]$ is irreducible over $k(t)$ and $R(x) = 0$. [Hint: Use Gauss' lemma and show that $R(Y)$ is irreducible over $k[t, Y]$.]

   (b) Show that the degree of $R(Y)$ as a polynomial in Y is the maximum of the degrees of $P(x)$ and $Q(x)$ as polynomials in x.

   (c) Show that $[k(x) : k(t)] = \max(\deg P(x), \deg Q(x))$.

   Proof. (a): Gauss' lemma implies that we only need to show that $R(Y)$ is irreducible in $k[t, Y] = k[Y][t]$. But $P(Y) - tQ(Y) \in (k[Y])[t] \subset k(Y)[t]$ is linear in t and so is irreducible over the field $k(Y)$ which immediately implies it is irreducible over the PID $k[Y]$. By definition of t we have $R(x) = 0$.

   (b): Let $n = \max(\deg P, \deg Q)$ and write $P(Y) = aY^n + \text{lower}$ and $Q(Y) = bY^n + \text{lower}$ where at least one of a, b is nonzero. Then $R(Y) = (a + bt)Y^n + \text{lower}$ and since $a + bt \neq 0$ if $a, b \neq 0$ it follows that $\deg R = n$.

(c): The minimal polynomial of x over $k(t)$ is $R(Y)$ from part (a). Therefore $[k(x) : k(t)] = \deg R(Y)$ and the conclusion follows. $\square$

3. Let K/F and L/F be field extensions. Suppose you are given subextensions $K/K_i/F$ and $L/L_j/F$ for i and j in partially ordered index sets I and J such that if $i \leq i'$ and $j \leq j'$ then $K_i \subset K_{i'}$ and $L_j \subset L_{j'}$. Further assume that I and J satisfy the following property: any two elements of the partially ordered set have an upper bound in the partially ordered set. If $K = \bigcup_{i \in I} K_i$ and $L = \bigcup_{j \in J} L_j$. Show that $KL = \bigcup_{(i,j) \in I \times J} K_i L_j$. [Hint: Show that the RHS is the smallest field that contains K and L.]

   Proof. Since $K_i L_j \subset KL$ because $K_i \subset K$ and $L_j \subset L$ it suffices, as in the hint, to show that $T = \bigcup_{(i,j)} K_i L_j$ is a field. Suppose $x, y \in T$. Then $x \in K_i L_j$ and $y \in K_{i'} L_{j'}$. By hypothesis we may choose $u \in I$ and $v \in J$ such that $u \geq i, i'$ and $v \neq j, j'$. The $K_i, K_{i'} \subset K_u$ and $L_j, L_{j'} \subset L_v$ and so $x, y \in K_u L_v$. Since $K_u L_v$ is a field it follows that $x + y, xy, x/y \in K_u L_v \subset T$ and so T is a field. $\square$

4. Show that if K/F and L/F are algebraic extensions then KL/F is also an algebraic extension. [Hint: Use the previous problem and the result for finite extensions in class to show that if $\{u_i\}$ is a basis of K/F and $\{v_j\}$ are a basis of L/F then $\{u_i v_j\}$ span KL/F.]

   Proof. Let $\mathcal{B}_K = (u_i)$ be a basis for K/F and $\mathcal{B}_L = (v_j)$ be a basis for L/F. Let I be the set of finite subsets of $\mathcal{B}_K$, partially ordered with respect to inclusion, and similarly let J be the set of finite subsets of $\mathcal{B}_L$, partially ordered with respect to inclusion. Simply by taking unions of finite sets we deduce that any two finite sets in I (or J) have an upper bound in I (J).

   For $S \in I$ define $K_S = K(u \mid u \in S)$ and similarly L_T for $T \in J$. Since K/F is algebraic it follows that u is algebraic over F for all $u \in S$. The result from class then shows that K_S/F, being the composite of finitely many finite extensions over F, is then finite and therefore algebraic. As $S \leq S'$ implies that $S \subset S'$ we deduce that $K_S \subset K_{S'}$, and the analogous statement for L_T. From the previous problem $KL = \bigcup K_S L_T$. As K_S/F and L_T/F are finite extensions it follows that so is $K_S L_T$ and so every element of KL, being in some $K_S L_T$, will have to be algebraic over F. $\square$

5. Show that if L/F and K/F are finite extensions such that $[KL : F] = [K : F][L : F]$ then $K \cap L = F$.

   Proof. Let $K \cap L = M$. Then $[KL : F] = [KL : M][M : F] \leq [K : M][L : M][M : F]$. But the LHS is $[K : F][L : F] = [K : M][L : M][M : F]^2$. Combining we deduce that $[M : F] \leq 1$ and so $M = F$. $\square$

6. Artin 15.3.7 on page 473.

   Proof. (a): Suppose $i \in F = \mathbb{Q}(\sqrt[4]{-2})$. Then $\sqrt{-2} = i\sqrt{2} \in F$ and so $\sqrt{2} \in F$. Note $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ have only $\mathbb{Q}$ in common (otherwise their degrees being 2 it would mean $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{2})$ and the RHS $\subset \mathbb{R}$ whereas $i \notin \mathbb{R}$) and they have degree 2 the problem on the exam implies $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4$. But $\mathbb{Q}(\sqrt[4]{-2}) : \mathbb{Q}] = 4$ so we'd have $\mathbb{Q}(\sqrt[4]{-2}) = \mathbb{Q}(i, \sqrt{2})$. Now $\sqrt[4]{-2} = \frac{1+i}{\sqrt{2}} \sqrt[4]{2}$ and since $i, \sqrt{2} \in F$ it would follow that $\sqrt[4]{2} \in F$ as well. But since $\mathbb{Q}(\sqrt[4]{2})$ has degree 4 over $\mathbb{Q}$, it would follow that $\mathbb{Q}(\sqrt[4]{-2}) \supset \mathbb{Q}(\sqrt[4]{2})$ would have to be an equality. But then $F = \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ whereas $i \notin \mathbb{R}$.

   (b): Write $\alpha = \sqrt[3]{2}$ and $\zeta = \zeta_3$. Suppose $\beta = \sqrt[3]{5} \in \mathbb{Q}(\alpha) \subset K = \mathbb{Q}(\zeta, \alpha)$, the latter field being the splitting of $X^3 - 2 \in \mathbb{Q}[X]$. Consider the field isomorphism $f : \mathbb{Q}(\alpha) \to \mathbb{Q}(\zeta\alpha)$ being the identity on $\mathbb{Q}$ and sending $\alpha \mapsto \zeta\alpha$. This can be done as α and $\zeta\alpha$ are roots of $X^3 - 2$. From class we can find an isomorphism $\phi : K \to K$ such that $\phi|_{\mathbb{Q}(\alpha)} = f$.

   Note $\beta \in K$ is a root of $X^3 - 5$ and from class we know that then $\phi(\beta)$ is another root of $X^3 - 5$ so it would have to be $\xi\beta$ where $\xi \in \{1, \zeta, \zeta^2\}$. Writing $\beta = a + b\alpha + c\alpha^2$ (as $1, \alpha, \alpha^2$ are a $\mathbb{Q}$-basis for $\mathbb{Q}(\alpha)$) if $\phi(\beta) = \xi\beta$ then

$$a\xi + b\alpha\xi + c\alpha^2\xi = \xi\beta = \phi(\beta) = \phi(a + b\alpha + c\alpha^2) = a + b\zeta\alpha + c\zeta^2\alpha^2$$

From class we know that $[\mathbb{Q}(\zeta,\alpha):\mathbb{Q}]=6$ so $[\mathbb{Q}(\alpha,\zeta):\mathbb{Q}(\alpha)]=2$ and so again from class the $\mathbb{Q}$-basis $1,\alpha,\alpha^2$ is independent over $\mathbb{Q}(\zeta)$. But then the relation

$$a(1-\xi)+b(\zeta-\xi)\alpha+c(\zeta^2-\xi)\alpha^2=0$$

with coefficients $a(1-\xi), b(\zeta-\xi), c(\zeta^2-\xi)\in\mathbb{Q}(\zeta)$ would have to have all coefficients equal to 0. We deduce that 2 of a,b,c must be 0 and so

$$\beta=\sqrt[3]{5}\in\{\sqrt[3]{2},\zeta\sqrt[3]{2},\zeta^2\sqrt[3]{2}\}$$

This can't be because then $\sqrt[3]{5/2}\in\mathbb{Q}(\zeta)$ and β/α has degree 3 over $\mathbb{Q}$ whereas $\mathbb{Q}(\zeta)$ is quadratic over $\mathbb{Q}$. $\square$