Math 30820 Honors Algebra 4
Homework 6

Andrei Jorza

Due Wednesday, 3/1/2017

Do 6 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.

1. Show that every extension K/F with $[K:F]=2$ is a normal extension.

   Proof. Let $\alpha \in K \setminus F$. Then $K = F(\alpha)$ is quadratic over F and so α is a solution to the monic minimal polynomial $X^2 - aX + b \in F[X]$. The roots of this polynomial are α and $a - \alpha$ and so K is the splitting field of this polynomial and is therefore normal. □

2. Let $P \in F[X]$, of degree n, and K be the splitting field of P over F. Show that $[K:F] \mid n!$.

   Proof. Let α be a root of P. As in the proof in class of the fact that $[K:F] \le n!$ we have K is the splitting field over $F(\alpha)$ of $P(X)/(X-\alpha) \in F(\alpha)[X]$.

   We now prove by induction on n. Suppose we know this in degree $< n$ and consider P of degree n. If P is irreducible then $P(X)/(X-\alpha)$ has degree $n-1 < n$ and so the inductive hypothesis implies that $[K:F(\alpha)] \mid (n-1)!$ and so $[K:F] = [K:F(\alpha)][F(\alpha):F)] \mid (n-1)! \cdot n = n!$. If $P = AB$ is a product of coprime polynomials of degrees a and b with $n = a+b$ let L be the splitting field of A over F, in which case K is the splitting field of B over L. As A and B are coprime we deduce that $F \subsetneq L \subsetneq K$.

   Then the inductive hypothesis implies that $[L:F] \mid a!$ and $[K:L] \mid b!$ which gives

   $$[K:F] \mid a!b! \mid n!$$

   as $\dfrac{n!}{a!b!} = \binom{n}{a}$. □

3. Let F be a field, $P \in F[X]$ a *monic* polynomial and K a field that contains all the roots $\alpha_1, \ldots, \alpha_n$ of the polynomial $P(X)$, where n is the degree of $P(X)$. The **discriminant** of $P(X)$ is defined as

   $$\Delta = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$$

   Show that P is separable if and only if $\Delta \neq 0$ and that

   $$\Delta = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} P'(\alpha_i)$$

   Proof. The first part is clear as $\Delta \neq 0$ iff no two roots are equal.

For the second note that if $P(X) = \prod(X - \alpha_i)$ then $P'(\alpha_i) = \prod_{j \neq i}(\alpha_i - \alpha_j)$. Now

$$\begin{aligned}
\Delta &= \prod_{i<j}(\alpha_i - \alpha_j)^2 \\
&= (-1)^{\binom{n}{2}} \prod_{i \neq j}(\alpha_i - \alpha_j) \\
&= (-1)^{\binom{n}{2}} \prod_{i=1}^{n} \prod_{j \neq i}(\alpha_i - \alpha_j) \\
&= (-1)^{\binom{n}{2}} \prod_{i=1}^{n} P'(\alpha_i)
\end{aligned}$$

□

4. (Do one of the 2 parts)

   (a) Consider the polynomial $P(X) = X^5 + pX + q$. Show that it has discriminant

   $$\Delta = 5^5 q^4 + 4^4 p^5$$

   (b) (This part is worth 2 extra points) Consider the polynomial $P(X) = X^n + pX + q$. Show that it has discriminant

   $$\Delta = (-1)^{\binom{n}{2}} n^n q^{n-1} + (-1)^{\binom{n-1}{2}} (n-1)^{n-1} p^n$$

[Hint: Use the previous problem.]

Proof. (a): Follows from (b).
(b): From the previous problem we need to compute $\prod P'(\alpha_i)$. But $\alpha_i^n = -p\alpha_i - q$ and so

$$P'(\alpha_i) = n\alpha_i^{n-1} + p = n(-p - q\alpha_i^{-1}) + p = -(n-1)p - nq\alpha_i^{-1}$$

so

$$\prod P'(\alpha_i) = \prod(-(n-1)p - nq\alpha_i^{-1}) = \prod \frac{(n-1)p}{\alpha_i} \prod(-\alpha_i - \frac{nq}{(n-1)p}) = \frac{(n-1)^n p^n}{\prod \alpha_i} P(-\frac{nq}{(n-1)p})$$

Since $\prod \alpha_i = (-1)^n q$ we get

$$\begin{aligned}
\Delta &= (-1)^{\binom{n}{2}} \prod P'(\alpha_i) \\
&= (-1)^{\binom{n}{2}+n} \frac{(n-1)^n p^n}{q} \left(\left(-\frac{nq}{(n-1)p} \right)^n - p\frac{nq}{(n-1)p} + q \right) \\
&= (-1)^{\binom{n}{2}} n^n q^{n-1} + (-1)^{\binom{n-1}{2}} (n-1)^{n-1} p^n
\end{aligned}$$

□

5. Let $\alpha \in \mathbb{R}$ such that $\alpha^4 = 5$.

   (a) Is $\mathbb{Q}(i\alpha^2)$ normal over $\mathbb{Q}$?

   (b) Is $\mathbb{Q}(\alpha + i\alpha)$ normal over $\mathbb{Q}(i\alpha^2)$?

   (c) Is $\mathbb{Q}(\alpha + i\alpha)$ normal over $\mathbb{Q}$?

Proof. (a): The roots of X^2+5 are $\pm i\alpha^2$ and so this field is a splitting field and therefore normal over $\mathbb{Q}$.

(b): The roots of $X^2 - 2i\alpha^2 \in \mathbb{Q}(i\alpha^2)[X]$ are $\pm(\alpha + i\alpha)$ and so again $\mathbb{Q}(\alpha + i\alpha)$ is a splitting field and therefore normal over $\mathbb{Q}(i\alpha^2)$.

(c): Note that $\alpha + i\alpha$ is the root of $X^4 + 20$ which is irreducible over $\mathbb{Q}$ by Gauss and Eisenstein. If $F = \mathbb{Q}(\alpha + i\alpha)$ were normal over $\mathbb{Q}$, F would have to contain all the roots $\pm\alpha \pm i\alpha$ of $X^4 + 20$. But then $(\alpha + i\alpha) \pm (\alpha - i\alpha) \in F$ implies $\alpha, i\alpha \in F$ and so F contains α and i. But $[F : \mathbb{Q}] = 4$ and F contains the composite $\mathbb{Q}(\alpha)\mathbb{Q}(i)$. Now $\mathbb{Q}(\alpha)$ is degree 4 over $\mathbb{Q}$ and $\mathbb{Q}(i)$ is degree 2 over $\mathbb{Q}$. As the composite is inside F of degree 4 over $\mathbb{Q}$ it must be that $\mathbb{Q}(\alpha, i)$ has degree 4 over $\mathbb{Q}$. But then $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha, i)$ and so $i \in \mathbb{Q}(\alpha)$ which cannot be as $\mathbb{Q}(\alpha) \subset \mathbb{R}$. □

6. Let F be a field of characteristic p that is nor perfect, i.e., the Frobenius homomorphism $\phi : F \to F$ given by $\phi(x) = x^p$ is not surjective. Show that there exist inseparable irreducible polynomials in $F[X]$.

Proof. Let $a \in F$ such that $a \notin \operatorname{Im}\phi$ and consider the polynomial $X^p - a$. Let α be a root of this polynomial in $\overline{F}$ so $\alpha^p = a$. But then $P(X) = X^p - a = X^p - \alpha^p = (X-\alpha)^p$. Let $m(X)$ be the minimal polynomial of α over F. Then $m(X) \mid P(X) = (X-\alpha)^p$ and so $m(X) = (X-\alpha)^k$ for some $k \leq p$. This polynomial is irreducible and inseparable as long as $k \geq 1$. But if $k = 1$ then $m(X) = X - \alpha \in F[X]$ so $a = \alpha^p = \phi(\alpha)$ which contradicts the hypothesis on α. □

7. Let F be a field of characteristic p and let K/F be a finite extension with $p \nmid [K : F]$. Show that K/F is a separable extension, i.e., for every $\alpha \in K$ the minimal polynomial of α over F is a separable polynomial.

Proof. Suppose $\alpha \in K$ with minimal polynomial $P(X)$. If $P(X)$ is inseparable from class $P(X) = Q(X^p)$ for a polynomial Q. But then $[F(\alpha) : F] = \deg P = p \deg Q$. However as $\alpha \in K$ it follows that $p \deg Q = [F(\alpha) : F] \mid [K : F]$ contradicting the hypothesis. □

8. Let $F = k(x)$ be the field of rational functions in the variable x with coefficients in some field k. Suppose $\phi : F \to F$ is a field automorphism such that $\phi|_k = \operatorname{id}|_k$. Show that there exists $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, k)$ such that $\phi(x) = \dfrac{ax+b}{cx+d}$. [Hint: What is $[F : \operatorname{Im}\phi]$?]

Proof. Let $t = \phi(x) \in k(x)$. Since ϕ is an isomorphism it follows that $\operatorname{Im} phi = \phi(k(x)) = k(\phi(x)) = k(t)$ has to be all of $k(x)$. But then $[k(x) : k(t)] = 1$ and from the previous homework this degree is $\max(\deg P, \deg Q)$ where $t = P(x)/Q(x)$. Therefore P and Q are at most linear so $t = \dfrac{ax+b}{cx+d}$. It remains to check that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible. Otherwise either $(a, b) = \lambda(c, d)$ in which case $t = \lambda \in k$ and so $k(t) = k \neq k(x)$ or $(a, c) = \lambda(b, d)$ in which case $t = b/d$ again yielding a contradiction. □