D-MATH Algebra II FS 2014
Prof. Brent Doran

Solutions 9

Splitting fields, finite fields

1. Let F be a field of characteristic zero, and let g be an irreducible polynomial that is a common divisor of f and f'. Prove that g^2 divides f.

   Solution : Since g divides f, we may use the decomposition $f = gh$, and as g also divides f', it must divide $g'h + gh'$ hence in particular $g'h$. Since g is irreducible, it cannot divide g', which is of lower degree, hence must divide h. Hence g^2 divides $gh = f$.

2. Let $\mathbb{F}$ denote a finite field. Prove that $\mathbb{F}$ has p^r elements, for some prime $p > 1$ and positive integer r.

   Solution : Since $\mathbb{F}$ is a finite field, it has characteristic p for some prime $p > 1$, and is a vector space over $\mathbb{Z}/(p)$ of finite dimension. Let r be this dimension. Then it has p^r elements.

3. Let K denote the splitting field of a polynomial $f(x) \in F[x]$ of degree d. Prove that $[K : F]$ divides $d!$.

   Solution : This exercise amounts to adapting the proof of Proposition 15.6.3 with a little care. As there, we proceed by induction over d.

   Assume first that f has a root α in F, i.e. $f(x) = (x - \alpha)q(x)$. $(*)$ Let K be the splitting field of q over F. By induction hypothesis, $[K : F]$ then divides $\deg(q) = (d-1)!$, hence $d!$.

   Otherwise, let g be an irreducible factor of $f = gh$ with $\deg(g) = k$, $\deg(h) = d-k$. Let F_1 denote the extension field $F[x]/(g)$. By construction, g has a root in F_1 and $[F_1 : F] = k$. Therefore, this root is also a root of f over F_1, and we may write

   $$f(x) = (x - \alpha)g_1(x)h(x).$$

   Now we repeat $(*)$ as follows : Let G_1 to be the splitting field of g_1 over F_1. By induction hypothesis, $[G_1 : F_1]$ divides $\deg(g_1) = (k-1)!$. Let K be the splitting field of h over G_1. Then again by induction hypothesis, $[K : G_1]$ divides $(d-k)!$.

   We can now conclude since K is also a splitting field of f over F and $[K : F] = [K : G_1][G_1 : F_1][F_1 : F]$ divides $(d-k)!k!$, hence

   $$\binom{d}{k}(d-k)!k! = d!.$$

4. Factor $x^9 - x$ and $x^{27} - x$ in $\mathbb{F}_3$.

   Solution : The monic irreducible polynomials of degree at most 3 over $\mathbb{F}_3$ are

$$x,\ x+1,\ x-1,\ x^2+1,\ x^2+x-1,\ x^2-x-1,$$
$$x^3-x+1,\ x^3-x-1,\ x^3+x^2-1,\ x^3-x^2+1,$$
$$x^3+x^2+x+1,\ x^3+x^2+x-1,\ x^3+x^2-x+1,$$
$$x^3-x^2+x+1,\ x^3-x^2+x-1,\ x^3-x^2-x-1.$$

   Because the irreducible factors of a polynomial $x^{3^r} - x$ over $\mathbb{F}_3$ are the irreducible polynomials over $\mathbb{F}_3$ whose degrees divide r,

$$x^9 - x \ = \ x(x+1)(x-1)(x^2+1)(x^2+x-1)(x^2-x-1)$$

   and

$$\begin{aligned} x^{27} - x \ &= \ x(x+1)(x-1)(x^3+x^2+x+1)(x^3+x^2+x-1)\cdots \\ &\cdots(x^3+x^2-x+1)(x^3-x^2+x+1)(x^3-x^2+x-1)(x^3-x^2-x-1). \end{aligned}$$

5. Let $\mathbb{F}$ be a field of characteristic $p \neq 0, 3$. Show that, if α is a zero of $f(x) = x^p - x + 3$ in an extension field of $\mathbb{F}$, then $f(x)$ has p distinct zeroes in $\mathbb{F}(\alpha)$.

   Solution : The field $\mathbb{F}$ contains $\mathbb{Z}/(p)$ as subfield, since it has characteristic p. For each $n \in \mathbb{Z}/(p)$, consider

$$f(\alpha+n) \ = \ (\alpha+n)^p - (\alpha+n) + 3 \ = \ \alpha^p - \alpha + 3 \ = \ 0,$$

   where we used in the second equation $n^p \equiv n \bmod p$. This shows that f has p distinct zeroes in $\mathbb{F}(\alpha)$.

6. Let F denote a field, p a prime and take $a \in F$ such that a is not a p^{th} power. Show that $x^p - a$ is irreducible over F.

   Solution : Let K be the splitting field of $x^p - a$. Assume by contradiction that $x^p - a$ decomposes into two non-trivial factors g and h over F. Over K, we may assume that

$$x^p - a = \underbrace{(x-a_1)\cdots(x-a_n)}_{=g(x)}\underbrace{(x-a_{n+1})\cdots(x-a_p)}_{=h(x)}.$$

   To get a contradiction, we must show that a is then a p^{th} power in F. By assumption, both $g(0)$ and $h(0)$ are elements of F, hence $A = a_1 \cdots a_n$ and $B = a_{n+1} \cdots a_p$ are both elements of F. Note that $A^p = a_1^p \cdots a_n^p = a^n$ and $B^p = a^{p-n}$. Using a Bézout identity $kn + lp = 1$, we can write

$$a = a^{kn} a^{lp} = A^{kp} a^{l(p-n)} a^{ln} = A^{(k+l)p} B^{lp} = \left(A^{k+l} B^l\right)^p.$$