HW due Mar 5

Tao Ju

March 5, 2014

Problem 20
Let α be transcendental over $\mathbb{Z}_2$. Let $F = \mathbb{Z}_2(\alpha)$ and let $p(x) = x^2 - \alpha$.
(a) Prove that p is irreducible over F.
(b) Prove that if β is a root of p in some extension field, then $p(x) = (x - \beta)^2$.
(c) Suppose that F is a finite field of characteristic 2. Prove that for every $a \in F$ there is a $b \in F$ such that $b^2 = a$.
(d) Suppose that F is a finite field of odd characteristic. Prove that there exists $a \in F$ for every $b \in F$ such that $b^2 \neq a$.
(e) Find a field F and an irreducible polynomial $p(x)$ of degree three such that in any extension field in which p splits there exist a β such that $p(x) = (x - \beta)^3$.

Proof:
(a)
Suppose p is not irreducible, so $p(x) = (x - a)(x - b)$ for some $a, b \in F$. Notice that $x^2 - \alpha = x^2 - (a + b)x + ab$ implies $a = -b$ and $\alpha = -ab = a^2$. Since $a \in F$, there exist two polynomials $f(\alpha), g(\alpha) \in \mathbb{Z}_2[\alpha]$ and $g(\alpha) \neq 0$ s.t. $a = f(\alpha)/g(\alpha)$.
Assume $f(\alpha) = t_n\alpha^n + t_{n-1}\alpha^{n-1} + \cdots + t_0$ where $t_0, \cdots, t_n \in \mathbb{Z}_2$. Since $2t = 0$ and $t^2 = t$ for all $t \in \mathbb{Z}_2$, we have

$$(f(\alpha))^2 = \left(\sum_{i=0}^{n} t_i\alpha^i\right)^2 = \sum_{i=0}^{n} t_i^2\alpha^{2i} + \sum_{0\le i<j\le n} 2t_it_j\alpha^{i+j} = \sum_{i=0}^{n} t_i\alpha^{2i} = f(\alpha^2).$$

As the same reason we have $(g(\alpha))^2 = g(\alpha^2)$. Thus

$$\alpha = a^2 = \frac{(f(\alpha))^2}{(g(\alpha))^2} = \frac{f(\alpha^2)}{g(\alpha^2)} \quad \Rightarrow \quad \alpha g(\alpha^2) - f(\alpha^2) = 0$$

which is not trivial since $\alpha g(\alpha^2) - f(\alpha^2)$ must include some odd power of α. Then α is the root of $xg(x^2) - f(x^2) = 0$, which contradicts against that α is transcendental over $\mathbb{Z}_2$.
Therefore p is irreducible.

(b)
Assume $\beta \in E$ for some extension field E. Then $0 = p(\beta) = \beta^2 - \alpha$. Thus over field E, $p(x) = x^2 - \beta^2 = x^2 - 2x\beta + \beta^2 = (x - \beta)^2$.

(c)
Since F is a finite field of characteristic 2, by Corollary 30, $|F| = 2^n$ for some $n \in \mathbb{N}^*$. Then $F^* = F \setminus \{0\} \cong \mathbb{Z}_{2^n-1}$. Assume α generates F^*. Consider $\beta = \alpha^{2^{n-1}}$, then $\beta^2 = \alpha^{2^n} = \alpha$. Thus every element a in F^* can be denoted as b^2 for some $b \in F^*$. It is clear $0 = 0^2$. Thus we've achieved our goal.

(d)
Assume F is a finite field of odd characteristic p, by Corollary 30, $|F| = p^n$ for some $n \in \mathbb{N}^*$. Then

$F^* = F \setminus \{0\} \cong \mathbb{Z}_{p^n-1}$. Assume a generates F^*. Suppose there exists some $a^k \in F^*$ s.t. $(a^k)^2 = a$, as to say $2k = 1 \mod p^n - 1$. $2k$ and $p^n - 1$ are both even numbers but 1 is odd, contradiction. Thus $a \neq b^2$ for every $b \in F^*$. Of course $0^2 \neq a$, so we've reached our goal.

(e)

(The example and proof are almost the same as (a) and (b).)

Let α be transcendental over $\mathbb{Z}_3$, ~~for instance $\alpha = \pi$.~~ Let $F = \mathbb{Z}_3(\alpha)$ and let $p(x) = x^3 - \alpha$. Divide the proof into two parts:

(1) Prove that p is irreducible over F.

Suppose p is not irreducible, so $p(x) = f(x)g(x)$ for some $f(x), g(x) \in F[x]$. It is clear that $\deg f = 1$ or $\deg g = 1$, we assume $\deg f = 1$ and $f(x) = x - a$ for some $a \in F$ without loss of generality. And we have $0 = f(a)g(a) = p(a) = a^3 - \alpha$. Since $a \in F$, there exist two polynomials $f(\alpha), g(\alpha) \in \mathbb{Z}_2[\alpha]$ and $g(\alpha) \neq 0$ s.t. $a = f(\alpha)/g(\alpha)$.

Assume $f(\alpha) = t_n\alpha^n + t_{n-1}\alpha^{n-1} + \cdots + t_0$ where $t_0, \cdots, t_n \in \mathbb{Z}_3$. Since $3t = 0$ and $t^3 = t$ for all $t \in \mathbb{Z}_3$, we have

$$(f(\alpha))^3 = \sum_{i=0}^{n} t_i^3\alpha^{3i} + \sum_{0\leq i<j\leq n} 3t_it_j(\alpha^{2i+j} + \alpha^{i+2j}) + \sum_{0\leq i<j<k\leq n} 6t_it_jt_k\alpha^{i+j+k} = \sum_{i=0}^{n} t_i\alpha^{3i} = f(\alpha^2).$$

As the same reason we have $(g(\alpha))^3 = g(\alpha^3)$. Thus

$$\alpha = a^3 = \frac{(f(\alpha))^3}{(g(\alpha))^3} = \frac{f(\alpha^3)}{g(\alpha^3)} \quad \Rightarrow \quad \alpha g(\alpha^3) - f(\alpha^3) = 0$$

which is not trivial since $\alpha g(\alpha^3) - f(\alpha^3)$ must include some α^{3k+1} for $k \in \mathbb{N}$. Then α is the root of $xg(x^3) - f(x^3) = 0$, which contradicts against that α is transcendental over $\mathbb{Z}_3$.

Therefore p is irreducible.

(2) Prove that if β is a root of p in some extension field, then $p(x) = (x - \beta)^3$.

Assume $\beta \in E$ for some extension field E. Then $0 = p(\beta) = \beta^3 - \alpha$. Thus over field E, $p(x) = x^3 - \beta^3 = x^3 - 3x^2\beta + 3x\beta^2 - \beta^3 = (x - \beta)^3$.

Math 542

Killian Kvalvik

March 5, 2014

Ок

20. *Let α be transcendental over $\mathbb{Z}_2$. Let $F = \mathbb{Z}_2(\alpha)$ and let $p(x) = x^2 - \alpha$.*

   (a) *Prove that p is irreducible over F.*
   Suppose not. Then p is divisible by a polynomial of lower order which is a linear polynomial. Therefore p has a root in F; call it β. Since $\beta \in F = \mathbb{Z}_2(\alpha)$, there exist relatively prime polynomials $q, r \in \mathbb{Z}_2[x]$ such that $\beta = \frac{q(\alpha)}{r(\alpha)}$. But $\beta^2 - \alpha = p(\beta) = 0$, so $(q(\alpha))^2 - \alpha \cdot (r(\alpha))^2 = 0$. But this implies that α is algebraic over $\mathbb{Z}_2$, a contradiction. Therefore p is irreducible. Need to argue $(q(x))^2 - x(r(x))^2$ not zero poly.

   (b) *Prove that if β is a root of p in some extension field, then $p(x) = (x-\beta)^2$.*
   Since $p(\beta) = \beta^2 - \alpha = 0$, $\beta^2 = \alpha$. Thus $(x-\beta)^2 = (x-\beta)(x-\beta) = x^2 - \beta x - \beta x + \beta^2 = x^2 + \alpha = x^2 - \alpha = p(x)$.

   (c) *Suppose that F is a finite field of characteristic 2. Prove that for every $a \in F$ there exists a $b \in F$ such that $b^2 = a$.*
   Let $c, d \in F$. Assume $c^2 = d^2$. Then $c^2 - d^2 = (c+d)(c-d) = (c-d)^2 = 0$, so $c - d = 0$ and $c = d$. Therefore, the function $\alpha : F \to F$ such that $\alpha(c) = c^2$ is injective, so it must also be surjective. Therefore, for every $a \in F$, there exists a $b \in F$ such that $b^2 = a$.

   (d) *Suppose that F is a finite field of odd characteristic. Prove that there exists $a \in F$ such that for all $b \in F$, $b^2 \neq a$.*
   Since F does not have characteristic 2, there exists a $c \in F$ such that $c + c \neq 0$, so $c \neq -c$. But $c^2 = (-c)^2$, so the function $x \mapsto x^2$ is not injective. Therefore it cannot be surjective, so there exists an $a \in F$ such that for all $b \in F$, $b^2 \neq a$.

   (e) *Find a field F and an irreducible polynomial $p(x)$ of degree 3 such that in any extension field in which p splits, there exists a β such that $p(x) = (x-\beta)^3$.*
   ?

degree of $(q(x))^2$ even
degree of $x(r(x))^2$ odd
so $(q(x))^2 - x(r(x))^2$ non trivial.