MAT 612 HW #8 Name SOLUTIONS

04/23/10. due Wednesday 04/28/10. 5 pm

25 points

1. Suppose E be a finite field of order q, with prime subfield $F \cong \mathbb{Z}_p$, $q = p^n$.

(a) Prove that E is the splitting field over F of the polynomial $f(x) = x^q - x$.

(b) Using (a), prove that, for any prime p and positive integer n, there exists a field E of order $q = p^n$, which is unique up to isomorphism.[1]

(c) In the notation of part (a), prove that f is separable over F, and conclude that E is Galois over F.

(d) Show that the mapping $x \mapsto x^p$ is an F-automorphism of E. Deduce that $\mathrm{Gal}(E, F)$ is isomorphic to $\mathbb{Z}_n$.

2. Prove that the Galois group of the polynomial $f(x) = x^4 - 2$ is isomorphic to the dihedral group D_4.

3. Assume char$(F) \nmid n$. Suppose F is a field containing an element ω satisfying $\omega^n = 1$, and such that all roots of $x^n - 1$ are powers of ω. (ω is called a *primitive n^{th} root of unity.*) Let $E = F[\alpha]$, where $\alpha^n = a \in F$.

(a) Show that E is Galois over F, and that $|\mathrm{Gal}(E, F)|$ divides n.

FALSE → (see solutions) (b) Show that there is an F-automorphism $\phi: E \to E$ satisfying $\phi(\alpha) = \alpha\omega$.

(c) Show that the automorphism φ of part (b) generates $\mathrm{Gal}(E, F)$, hence $\mathrm{Gal}(E.F)$ is cyclic of order dividing n.

4. Let $f(x, y) = x^2 + x^3 - y^2 \in \mathbb{C}[x, y]$.

(a) Show f is irreducible. (Consider f as a polynomial in ~~x~~ y over the PID ~~$\mathbb{C}[y]$~~ $\mathbb{C}[x]$; apply Eisentein's Criterion.)

(b) Let $I = (f)$ and $R = \mathbb{C}[x, y]/I$. Since f is irreducible, R is an integral domain. Let E be the quotient field of R. Show that E is (up to isomorphism) an extension field of $\mathbb{C}$.

(c) Show that x represents a transcendental element of E over $\mathbb{C}$, and E is algebraic over $\mathbb{C}(x)$.

(d) Show that F is Galois over $\mathbb{C}(x)$ and identify the Galois group.[2]

① (a) Since $F - \{0\}$ is a group of order $q-1$, $x^{q-1} = 1$ for all $x \neq 0$ by Lagrange's Thm. Then $x^q = x$ for all $x \in F$, including $x = 0$. $f(x) = x^q - x$ has q distinct roots in E, so all its roots are in E. Since E is a field, it is therefore a splitting field for f.

(b) Let E be a splitting field for $f(x) = x^q - x$ over $\mathbb{Z}_p$.

(over)

[1] This field is called "the Galois field of order q," denoted $\mathrm{GF}(q)$.

[2] The inclusion $\mathbb{C}(x) \to E$ corresponds to the projection from the curve $f(x, y) = 0$ onto the x axis.

Claim every element of E is a root of f. Indeed, if $f(\alpha) = f(\beta) = 0$, then $f(\alpha+\beta) = (\alpha+\beta)^q - (\alpha+\beta)$
$= \alpha^q + \beta^q - \alpha - \beta = (\alpha^q - \alpha) + (\beta^q - \beta) = 0 + 0 = 0$
since $\mathrm{char}(E) = p$ and $q = p^n$. Also $f(\alpha\beta) = (\alpha\beta)^q - \alpha\beta$
$= \alpha^q\beta^q - \alpha\beta = \alpha\beta - \alpha\beta = 0$. It follows that the set of roots of f form a field (since they are algebraic), hence equals E by minimality of splitting fields.
Since $f'(x) = qx^{q-1} - 1 = -1 \neq 0$, f has q distinct roots in E, hence $|E| = q$. By (a) any field of q elements is a splitting field of f, hence they are all isomorphic by uniqueness of splitting fields.

(c) We showed f is separable in part (b), hence E is Galois over $\mathbb{Z}_p$.

(d) By the freshman's dream, $(\alpha+\beta)^p = \alpha^p + \beta^p$. Also $(\alpha\beta)^p = \alpha^p\beta^p$. Finally $\alpha^p = \alpha$ if $\alpha \in F = \mathbb{Z}_p$. Thus $\varphi \in Gal(E,F)$.
Note that $\varphi^k(\alpha) = \alpha^{p^k} = \alpha$ for all $\alpha \in F - \{0\}$ iff $\alpha^{p^k-1} = 1$ for all $\alpha \in F - \{0\}$ iff $p^n - 1$ divides $p^k - 1$, since $F - \{0\}$ is cyclic of order $p^n - 1$. This implies $k \geq n$.
Since $\alpha^{p^n} = \alpha$ for all $\alpha \in F$, φ has order equal to n.
Since $|Gal(E,F)| = |E:F| = n$, $Gal(E,F)$ is cyclic of order n, generated by φ.

(2) Let $\alpha = \sqrt[4]{2}$. Then the roots of $f(x) = x^4 - 2$ are $\pm\alpha, \pm i\alpha$, hence $E = \mathbb{Q}[\alpha, i\alpha]$ is a splitting field for $f(x)$ inside $\mathbb{C}$. Since $2i = (\alpha^3)(\alpha i)$, $E = \mathbb{Q}[\alpha, i]$. Then $|E:\mathbb{Q}| = |E:\mathbb{Q}[\alpha]|\,|\mathbb{Q}[\alpha]:\mathbb{Q}|$
$= 2 \cdot 4 = 8$, since $m_i^{\mathbb{Q}[\alpha]}(x) = x^2 + 1$ and $m_\alpha^{\mathbb{Q}} = x^4 - 2$.
Let $G = Gal(E, \mathbb{Q})$. Then $|G| = |E:\mathbb{Q}| = 8$, and G acts faithfully on the roots of $f(x)$, so $G \lesssim S_4$. Since f is irreducible, G is isomorphic to a <u>transitive</u> subgroup of S_4. Let $\varphi \in G$ with $\varphi(\alpha) = i\alpha$. Claim $\varphi(i\alpha) \neq \alpha$. Otherwise, $\{\alpha, i\alpha\}$ would be an orbit, so $(x-\alpha)(x-i\alpha) = x^2 - (1+i)\alpha x + \alpha^2$ would be fixed by G, hence would have rational coefficients.

(2) (cont'd.) Then φ must have order 4, since S_4 has no elements of order 8. Let $\psi \in G$ be complex conjugation. (Since f has real coefficients, its roots come in conjugate pairs; hence E is invariant under conjugation. Since $\overline{z+w} = \bar{z} + \bar{w}$ and $\overline{zw} = \bar{z}\bar{w}$, ψ is an automorphism of E.) Then $\psi \neq \varphi^2$, since $\psi(\alpha)=\alpha$ and $\varphi^2(\alpha) = \varphi(i\alpha) \neq \alpha$. Then $\psi \notin \langle\varphi\rangle$, so $G = \langle \varphi, \psi \rangle$. Now, φ must permute the roots of $x^2+1 \in \mathbb{Q}[x]$, hence $\varphi(i) = \pm i$. Then, replacing φ by $\varphi\psi$ if necessary, we may assume $\varphi(i) = -i$. (Recall that $\psi(\alpha) = \alpha$ so $\varphi\psi(\alpha) = \varphi(\alpha) = i\alpha$.) Then we may choose a labelling so that $\varphi = (1234)$ and $\psi = (12)$. Then $G = \langle \varphi, \psi \rangle \cong \langle (1234), (12) \rangle \cong D_4$. $\square$

(3) (a) α is a root of $f(x) = x^n - a$. Since $(\alpha\omega^k)^n = \alpha^n(\omega^k)^n = a \cdot 1 = a$, $\alpha\omega^k$ is a root of $x^n - a$ for $0 \le k < n$. Let $g(x) = x^n - 1$. Since $\text{char}(F) \nmid n$, $g'(\alpha) = n\alpha^{n-1} \neq 0$ if $\alpha \neq 0$; it follows that g has no repeated roots. Thus $\{\omega^k \mid 0 \le k < n\}$ is a set of n elements. Then $\{\alpha\omega^k \mid 0 \le k < n\}$ is the set of all n roots of $f(x)$. Thus $F[\alpha]$ is a splitting field for $f(x)$ over F (since $\omega \in F$). Each irreducible factor of f is the minimal polynomial of $\alpha\omega^k$ for some k. Since $F[\alpha\omega^k] = F[\alpha]$, these polynomials each have degree $|F[\alpha]:F|$. Since the sum of these degrees is equal to n, $|F[\alpha]:F|$ divides n.

(b) The correct statement is: there exists $\varphi \in \text{Gal}(E,F)$ such that $\varphi(\alpha) = \alpha\omega^k$ for some $0 < k < n$. For this we need to assume $\alpha \notin F$. Then m_α^F has degree at least two, hence has a root besides α. This other root must

$\longrightarrow$ (over)

be $\alpha\omega^k$ for some k, $0<k<n$.

(c) For this, choose k minimal with $\varphi(\alpha)=\alpha\omega^k$ for some $\varphi\in Gal(E,F)$. If $\psi\in Gal(E,F)$ then $\psi(\alpha)=\alpha\omega^l$ for some l. Claim k divides l – otherwise $l=qk+r$ for $0<r<k$. Then

$$\varphi^q(\alpha)=\varphi^{q-1}(\alpha\omega^k)=\varphi^{q-1}(\alpha)\varphi^{q-1}(\omega^k)=\varphi^{q-1}(\alpha)\omega^k$$
$$=\varphi^{q-2}(\alpha\omega^k)\omega^k=\varphi^{q-2}(\alpha)\omega^{2k}=\cdots=\alpha\omega^{qk}.$$

Then

$$\psi\circ\varphi^{-q}(\alpha)=\psi(\alpha\omega^{-qk})=\alpha\omega^{l-qk}=\alpha\omega^r,$$

and $\psi\circ\varphi^{-q}\in Gal(E,F)$, contradicting minimality of k. Then $l=qk$, so $\psi(\alpha)=\alpha\omega^l=\alpha\omega^{qk}=\varphi^q(\alpha)$, implying $\psi=\varphi^q$. Thus $Gal(E,F)$ is cyclic, generated by φ.

(4) (a) $f(x,y)=x^2+x^3-y^2=-y^2+x^2(1+x)\in\mathbb{C}[x][y]$. Let $p=1+x$. Then p is a prime in $\mathbb{C}[x]$, $p\nmid -1$, $p\mid x^2(1+x)$, and $p^2\nmid x^2(1+x)$. Thus f is irreducible over $\mathbb{C}[x]$ by Eisenstein's criterion. ($\mathbb{C}[x]$ is a PID, hence a UFD.) It follows that f is irreducible in $\mathbb{C}[x,y]$, since units in $\mathbb{C}[x][y]$ are units in $\mathbb{C}[x]$, hence nonzero constants (hence units in $\mathbb{C}[x,y]$).

(b) The function $\mathbb{C}\longrightarrow\mathbb{C}[x,y]/I$; $c\longmapsto c+I$ is injective because $I\cap\mathbb{C}=0$. Since R embeds in E, this shows that E contains a copy of $\mathbb{C}$.

(c) If $x+I$ were algebraic over $\mathbb{C}$, then there would be a nonzero polynomial $p\in\mathbb{C}[t]$ such that $p(x)\in I$. But no nonzero multiple of $f(x,y)$ is independent of y. Thus $x+I$ is transcendental. On the other hand, $f(x,t)=x^2+x^3-t^2\in\mathbb{C}(x)[t]$ and $f(x,y)=0$ in E, so $y+I$ is algebraic over be $\alpha\omega^k$ for some k, $0<k<n$.

(c) For this, choose k minimal with $\varphi(\alpha)=\alpha\omega^k$ for some $\varphi\in Gal(E,F)$. If $\psi\in Gal(E,F)$ then $\psi(\alpha)=\alpha\omega^l$ for some l. Claim k divides l – otherwise $l=qk+r$ for $0<r<k$. Then

$$\varphi^q(\alpha)=\varphi^{q-1}(\alpha\omega^k)=\varphi^{q-1}(\alpha)\varphi^{q-1}(\omega^k)=\varphi^{q-1}(\alpha)\omega^k$$
$$=\varphi^{q-2}(\alpha\omega^k)\omega^k=\varphi^{q-2}(\alpha)\omega^{2k}=\cdots\Rightarrow\alpha\omega^{qk}.$$ Then
$$\psi\circ\varphi^{-q}(\alpha)=\psi(\alpha\omega^{-qk})=\alpha\omega^{l-qk}=\alpha\omega^r,$$
and $\psi\circ\varphi^{-q}\in Gal(E,F)$, contradicting minimality of k. Then $l=qk$, so $\psi(\alpha)=\alpha\omega^l=\alpha\omega^{qk}=\varphi^q(\alpha)$, implying $\psi=\varphi^q$. Thus $Gal(E,F)$ is cyclic, generated by φ.

(4) (a) $f(x,y)=x^2+x^3-y^2=-y^2+x^2(1+x)\in\mathbb{C}[x][y]$.
Let $p=1+x$. Then p is a prime in $\mathbb{C}[x]$, $p\nmid -1$, $p\mid x^2(1+x)$, and $p^2\nmid x^2(1+x)$. Thus f is irreducible over $\mathbb{C}[x]$ by Eisenstein's criterion. ($\mathbb{C}[x]$ is a PID, hence a UFD.) It follows that f is irreducible in $\mathbb{C}[x,y]$, since units in $\mathbb{C}[x][y]$ are units in $\mathbb{C}[x]$, hence nonzero constants (hence units in $\mathbb{C}[x,y]$).

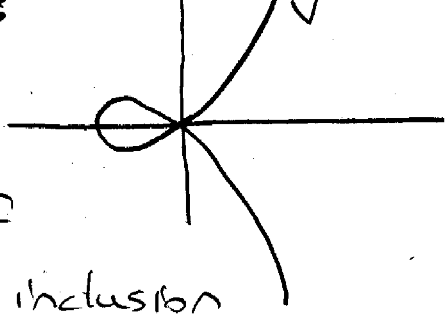
(b) The function $\mathbb{C}\longrightarrow\mathbb{C}[x,y]/I$; $c\longmapsto c+I$ is injective because $I\cap\mathbb{C}=0$. Since R embeds in E, this shows that E contains a copy of $\mathbb{C}$.

(c) If $x+I$ were algebraic over $\mathbb{C}$, then there would be a nonzero polynomial $p\in\mathbb{C}[t]$ such that $p(x)\in I$. But no nonzero multiple of $f(x,y)$ is independent of y. Thus $x+I$ is transcendental. On the other hand, $f(x,t)=x^2+x^3-t^2\in\mathbb{C}(x)[t]$ and $f(x,y)=0$ in E, so $y+I$ is algebraic over

$\mathbb{C}(x+I) \cong \mathbb{C}(x)$. Then $|E:F| = 2$ so E is alg. / F.

(d) $|E:\mathbb{C}(x)| = 2$ because $f(x,t) \in \mathbb{C}[x][t]$ has degree 2 and is irreducible. Since y and $-y$ are the two roots of $f(x,t)$, and $E = \mathbb{C}(x)[y]$, E is Galois / F. $Gal(E,F)$ has order $2 = |E:F|$, hence is isomorphic to $\mathbb{Z}_2$.

Note: R is the coordinate ring of the variety $V = \{x^2 + x^3 - y^2 = 0\}$:



$\mathbb{C}[x]$ is the coordinate ring of the x-axis. The inclusion of fields $\mathbb{C}(x) \hookrightarrow E$ corresponds to the projection $V \longrightarrow$ (x-axis); the fact that E is Galois over $\mathbb{C}(x)$ with group $\mathbb{Z}_2$ reflects the fact that the projection is generically 2-to-1.