Peize Liu
St. Peter's College
University of Oxford

Problem Sheet 1

B3.1: Galois Theory

AB Great work!
A few mistakes, but you obviously understand the material.

21 October, 2020

In these problems K denotes an arbitrary field and $K[x]$ denotes the ring of polynomials in one variable x over K. If p is a prime number, then $\mathbb{F}_p$ denotes the field of integers modulo p.

Question 1

Let E/K is a finite extension of fields and let $\alpha \in E/K$. Prove that there is a unique monic irreducible polynomial $p \in K[x]$ such that the homomorphism

$$K[x] \to K(\alpha)$$

which maps $x \mapsto \alpha$, induces an isomorphism

$$K(\alpha) \cong K[x]/\langle p \rangle$$

Proof. First, suppose that $[E : K] = n$. Then $\{1, \alpha, \ldots, \alpha^n\}$ is linearly dependent over K. Hence there exists $a_0, \ldots, a_n \in K$ such that

$$f(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0 = 0$$

and hence α is algebraic over K.

Let $m \in K[x]$ be the minimal polynomial of α over K. That is, m is a monic polynomial of least degree such that $m(\alpha) = 0$. By definition m is irreducible.

For $f \in K[x]$ such that $f(\alpha) = 0$, by division algorithm there exist $q, r \in K[x]$ such that $f = qm + r$ where $\deg r < \deg m$. Hence

$$0 = f(\alpha) = q(\alpha)m(\alpha) + r(\alpha) = r(\alpha)$$

By minimality of $\deg m$ we must have $r = 0$. Hence $m \mid f$.

Now suppose that m_1, m_2 are minimal polynomials of α over K. Then we have $m_1 \mid m_2$ and $m_2 \mid m_1$. That is $m_1(x) = a m_2(x)$ for some $a \in K$. But both m_1 and m_2 are monic. Therefore $a = 1$ and $m_1 = m_2$. We deduce that the minimal polynomial of α is unique.

Recall that the polynomial ring satisfies the following universal property:

For any unital commutative ring E, $\alpha \in E$, and unital ring homomorphism $f : K \to E$, there exists a unique ring homomorphism $\mathrm{ev}_\alpha : K[x] \to E$ such that $\mathrm{ev}_\alpha \circ \iota = f$ and $\mathrm{ev}_\alpha(x) = \alpha$.

$$\begin{tikzcd} K \arrow[r, "f"] \arrow[d, hook, "\iota"'] & (E, \alpha) \\ (K[x], x) \arrow[ur, dashed, "\exists!\, \mathrm{ev}_\alpha"'] & \end{tikzcd}$$

*where ev_α is called the **evalution homomorphism**.*

With $f : K \hookrightarrow E$ being the inclusion map, we apply the First Isomorphism Theorem to the evalution homomorphism:

$$K[\alpha] = \operatorname{im} \mathrm{ev}_\alpha \cong K[x]/\ker \mathrm{ev}_\alpha$$

We have shown previously that $\ker \mathrm{ev}_u = \langle m(x) \rangle$. Hence

$$K[\alpha] = K[x]/\langle m \rangle$$

Since K is a field, $K[x]$ is a principal ideal domain. As m is irreducible, $\langle m \rangle$ is a maximal ideal in $K[x]$. Hence $K[\alpha] \sim K[x]/\langle m \rangle$ is a field. Since $K(\alpha)$ is the field of fractions of $K[\alpha]$, we have $K[\alpha] = K(\alpha)$. We conclude that

$$K(\alpha) = K[x]/\langle m \rangle$$

Perfect! A

□

Question 2

Prove the Tower Law.

Proof. The **Tower Law** states that for field extensions $F \subseteq K \subseteq L$, $[L:F] = [L:K][K:F]$, where $[L:F] := \dim_F L$ and similar for the other two.

Let $\mathscr{B}$ be a basis of L over K and $\mathscr{C}$ a basis of K over F. We claim that $\mathscr{B}\mathscr{C} := \{xy \in L : x \in \mathscr{B}, y \in \mathscr{C}\}$ is a basis of L over F.

For $u \in L$, there exists a unique expression:

$$u = \sum_{i=1}^{m} r_i x_i$$

where $x_1, \ldots, x_n \in \mathscr{B}$ are distinct and $r_1, \ldots, r_n \in K$.

For each r_i, there exists a unique expression:

$$r_i = \sum_{j=1}^{m_i} \lambda_{i,j} y_{i,j}$$

where $y_{i,1}, \ldots, y_{i,m_i} \in \mathscr{C}$ are distinct and $\lambda_{i,1}, \ldots, \lambda_{i,m_i} \in F$.

Combining the expressions we express u uniquely in the spanning of $\mathscr{B}\mathscr{C}$:

$$u = \sum_{i=1}^{m} \sum_{j=1}^{m_i} \lambda_{i,j} x_i y_{i,j}$$ ✓

Perhaps give more detail why this expression is unique.

Hence $\mathscr{B}\mathscr{C}$ is a basis of L over F. In particular,

$$[L:F] = \operatorname{card} \mathscr{B}\mathscr{C} = \operatorname{card} \mathscr{B} \cdot \operatorname{card} \mathscr{C} = [L:K][K:F]$$ ✓

A⁻

□

Question 3

Find the minimal polynomial for

$$\frac{\sqrt{3}}{1 + 2^{1/3}}$$

over $\mathbb{Q}$; that is, the monic polynomial $m(x)$ of smallest possible degree with rational coefficients satisfying

$$m\left(\frac{\sqrt{3}}{1 + 2^{1/3}}\right) = 0$$

Solution. Let $u = \dfrac{\sqrt{3}}{1+2^{1/3}}$. We have

$$\begin{aligned} u = \frac{\sqrt{3}}{1+2^{1/3}} &\implies (1+2^{1/3})u = \sqrt{3} \\ &\implies 2^{1/3}u = \sqrt{3} - u \\ &\implies 2u^3 = (\sqrt{3} - u)^3 = -u^3 + 3\sqrt{3}u^2 - 9u + 3\sqrt{3} \\ &\implies u^3 + 3u = \sqrt{3}(u^2 + 1) \\ &\implies u^2(u^2+3)^2 = 3(u^2+1)^2 \\ &\implies u^6 + 3u^4 + 3u^2 - 3 = 0 \end{aligned}$$ ✓

Hence $f(x) := x^6 + 3x^4 + 3x^2 - 3 \in \mathbb{Q}[x]$ is an annihilating polynomial of u.

By Eisenstein's criterion with $p = 3$, we find that f is irreducible. Since the minimal polynomial of u divides f, we deduce that f is the minimal polynomial of u. □

✓ Great! A

Question 4

The formal derivative $D : K[x] \to K[x]$ is defined by

$$D\left(a_0 + a_1x + \cdots + a_nx^n\right) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$$

Prove that if $a, b \in K$ and $f, g \in K[x]$ then

(a) $D(af + bg) = aDf + bDg$

(b) $D(fg) = fDg + gDf$

(c) $Dh(x) = Dg(x)Df(g(x))$ when $h(x) = f(g(x))$

If $a \in K$ show that

(d) $(x-a)$ divides $f(x)$ in $K[x]$ if and only if $f(a) = 0$

(e) $(x-a)^2$ divides $f(x)$ in $K[x]$ if and only if $f(a) = 0 = Df(a)$

Deduce that if the polynomials f and Df are relatively prime in $K[x]$, then f has no multiple root.

Proof. Suppose that $f = \sum_{i=0}^{n} c_ix^i$ and $g = \sum_{i=0}^{m} d_ix^i$, where $c_n, d_m \neq 0$. Without loss of generality we assume that $n \geqslant m$ and put $d_{m+1} = \cdots = d_n = 0$.

where is $nc_0d_nx^{n-1}$ for example. Maybe should be $\sum_{k=0}^{2n-1}\sum_{i=0}^{k}(k-i+1)c_id_{k-i+1}x^k$

(a) $D(af+bg) = D\left(a\sum_{i=0}^{n} c_ix^i + b\sum_{i=0}^{n} d_ix^i\right) = D\left(\sum_{i=0}^{n}(ac_i + bd_i)x^i\right) = \sum_{i=0}^{n} i(ac_i+bd_i)x^{i-1}$
$= a\sum_{i=0}^{n} ic_ix^{i-1} + b\sum_{i=0}^{n} id_ix^{i-1} = aDf + bDg$ ✓

(b) $fDg + gDf = \left(\sum_{i=0}^{n} c_ix^i\right)\left(\sum_{i=0}^{n} id_ix^{i-1}\right) + \left(\sum_{i=0}^{n} d_ix^i\right)\left(\sum_{i=0}^{n} ic_ix^{i-1}\right) \overset{?}{=} \sum_{k=0}^{n}\sum_{i=0}^{k}(k-i)c_kd_{k-i}x^{k-1} + \sum_{k=0}^{n}\sum_{i=0}^{k} ic_kd_{k-i}x^{k-1}$
$= \sum_{k=0}^{n}\sum_{i=0}^{k} kc_kd_{k-i}x^{k-1} = D\left(\sum_{k=0}^{n}\sum_{i=0}^{k} c_id_{k-i}x^k\right) = D\left(\left(\sum_{i=0}^{n} c_ix^i\right)\left(\sum_{i=0}^{m} d_ix^i\right)\right) = D(fg)$

(c) We use induction on n to show that $D(g^n) = ng^{n-1}D(g)$. Base case: When $n = 1$ it holds trivially. Induction case: Suppose that it holds for all $k < n$. Then

$$D(g^n) = D(g \cdot g^{n-1}) = g^{n-1}D(g) + gD(g^{n-1}) = g^{n-1}D(g) + g\cdot(n-1)g^{n-2}D(g) = ng^{n-1}D(g)$$

By linearity of D,

$$D(h) = D\left(\sum_{i=0}^{n} a_ig(x)^i\right) = \sum_{i=0} a_iD\left(g(x)^i\right) = \sum_{i=0} ia_ig(x)^{i-1}D(g) = Dg \cdot Df \circ g$$ ✓

(d) By division algorithm there exist $q \in K[x]$ and $r \in K$ such that $f(x) = (x-a)q(x) + r$. Then $f(a) = (a-a)q(a) + r = r$. Hence

$$f(x) = (x-a)q(x) + f(a)$$

In particular, $(x-a)$ divides $f(x)$ in $K[x]$ if and only if $f(a) = 0$. ✓

(e) If $(x-a)^2$ divides f, then $f(a) = 0$ and $f(x) = (x-a)^2g(x)$ for some $g \in K[x]$. Then $Df(x) = 2(x-a)g(x) + (x-a)^2Dg(x)$. Hence $Df(a) = 0$.

Conversely, if $f(a) = Df(a) = 0$, by (d) $x - a$ divides f. Hence $f(x) = (x-a)g(x)$ for some $g \in K[x]$. Then $Df(x) = g(x) + (x-a)Dg(x)$. $0 = Df(a) = g(a)$ implies that $x - a$ divides g. Hence $(x-a)^2$ divides f. ✓

If f and Df are coprime, then exists $a, b \in K$ such that $af(x) + bDf(x) = 1$. Hence f and Df have no common roots. By (e) we deduce that f has no multiple root. ✓ □

Good. B+

Question 5

Show that if $a \in \mathbb{Z}$ is divisible by a prime p but not by p^2, then $x^n - a$ is irreducible over $\mathbb{Q}$ for all $n \geq 1$. Show also that it has no repeated roots in any extension of $\mathbb{Q}$.

Think it's enough to just cite this criterion

Proof. The first part is a special case of Eisenstein's criterion. Suppose that $f(x) = x^n - a$ is not irreducible in $\mathbb{Z}[x]$. Then there exists non-constant $g, h \in \mathbb{Z}[x]$ such that $f = gh$. Let $\pi : \overset{\mathbb{Z}?}{\cancel{\mathbb{Q}}} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$ induces the homomorphism $\pi : \mathbb{Q}[x] \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})[x]$. The image of f, g, h are $\overline{f}, \overline{g}, \overline{h}$. So $\overline{f} = \overline{g}\overline{h}$. Let b_0, c_0 be the constant coefficients of g and h. Then $a = -b_0 c_0$. Since $p \mid a$, we have $\overline{0} = \overline{b_0}\,\overline{c_0}$ in $\mathbb{Z}/p\mathbb{Z}$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, it has no zero-divisors. So $p \mid b_0$ ~~and~~ or $p \mid c_0$. Hence $p^2 \mid a$, which is a contradiction. × Hence $f(x) = x^n - a$ is irreducible in $\mathbb{Z}[x]$. By (a corollary of) Gauss' Lemma, f is irreducible in $\mathbb{Q}[x]$.

Think a bit more is needed.

The formal derivative of f, $Df(x) = nx^{n-1}$, has a unique root $x = 0$ in any extension of $\mathbb{Q}$. But $x = 0$ is not a root of f, as $f(0) = -a \neq 0$ (otherwise $p^2 \mid a$). f and Df have no common roots, so f has no repeated roots in any extension of $\mathbb{Q}$. ✓ □

B

Question 6

Show that if m is any positive integer, then the polynomial $x^{p^m} - x$ has no multiple root in any extension of fields $L : \mathbb{F}_p$.

Let

$$K = \left\{\alpha \in L : \alpha^{p^m} = \alpha\right\}$$

be the set of roots of $x^{p^m} - x$ in the extension L. Show that K is a subfield of L.

Let n be a positive integer. Show that if m divides n then $p^m - 1$ divides $p^n - 1$ in $\mathbb{Z}$ and $x^{p^m} - x$ divides $x^{p^n} - x$ in $\mathbb{F}_p[x]$.

Proof. Note that any extension field of $\mathbb{F}_p$ has characteristic p. Let $f(x) = x^{p^m} - x$. The formal derivative of f is

$$Df(x) = p^m x^{p^m - 1} - 1 = -1$$

as $p^m = 0$. Df has no roots in any extension of $\mathbb{F}_p$. Hence f has no multiple roots in any extension of $\mathbb{F}_p$. ✓

For $\alpha_1, \alpha_2 \in K$, it is clear from definition that $\alpha_1\alpha_2 \in K$ and $\alpha_1^{-1} \in K$. By Binomial Theorem,

maybe need small argument for this

$$(\alpha_1 + \alpha_2)^{p^m} = \alpha_1^{p^m} + \alpha_2^{p^m} + \sum_{k=1}^{p^m - 1} \frac{p^m!}{k!(p^m - k)!}\alpha_1^k \alpha_2^{p^m - k} = \alpha_1^{p^m} + \alpha_2^{p^m}$$

because p divides $\dfrac{p^m!}{k!(p^m - k)!}$ for $k < p^m$. Hence $\alpha_1 + \alpha_2 \in K$. ✓

If $p = 2$, then $-\alpha = \alpha \in K$. If $p > 2$, then p^m is odd. Hence $(-\alpha)^{p^m} = (-1)^{p^m}\alpha^{p^m} = -\alpha$. Hence $-\alpha \in K$. We conclude that K is a subfield of L.

Don't forget to check $0, 1 \in K$

Suppose that $n = km$ for $k \in \mathbb{Z}_+$. Then

$$p^{km} - 1 = (p-1)(p^{km-1} + \cdots + p + 1) = (p-1)(p^{m-1} + \cdots + p + 1)(p^{(k-1)m} + \cdots + p^m + 1) = (p^m - 1)(p^{(k-1)m} + \cdots + p^m + 1)$$

Hence $p^m - 1$ divides $p^n - 1$ in $\mathbb{Z}[x]$. ✓

Note that $x^{p^m} - x = x\left(x^{p^m - 1} - 1\right)$ and $x^{p^n} - x = x\left(x^{p^n - 1} - 1\right)$. Since $p^{m}_{\cancel{m}} - 1$ divides $p^n - 1$ in $\mathbb{Z}$, we have $\left(x^{p^m - 1} - 1\right)$ divides $\left(x^{p^n - 1} - 1\right)$ in $x \in \mathbb{Z}[x]$. Hence $x^{p^m} - x$ divides $x^{p^n} - x$ in $\mathbb{F}_p[x]$. ✓ □

"by same argument as above, with $p \leftrightarrow x$"

B

Question 7

(a) Let $f(x) = x^3 - s_1 x^2 + s_2 x - s_3 = (x - \alpha)(x - \beta)(x - \gamma) \in \mathbb{Q}[x]$ where $\alpha, \beta, \gamma \in \mathbb{C}$. Denoting $\sigma_i = \alpha^i + \beta^i + \gamma^i$ for $i \geq 0$, show that $\sigma_0 = 3, \sigma_1 = s_1$ and $\sigma_2 = s_1^2 - 2s_2$ Show further that

$$\sigma_r = s_1\sigma_{r-1} - s_2\sigma_{r-2} + s_3\sigma_{r-3}$$

for all $r \geq 3$.

(b) Let $\delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$ and $\Delta = \delta^2$. Show that

$$\Delta = -4s_1^3 s_3 + s_1^2 s_2^2 + 18 s_1 s_2 s_3 - 4s_2^3 - 27s_3^2$$

[*Hint: You may find it useful to consider the Van der Monde determinant*

$$\det\begin{pmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{pmatrix}$$

and the determinant of this matrix multiplied by its transpose to deduce first that

$$\Delta = \det\begin{pmatrix} \sigma_0 & \sigma_1 & \sigma_2 \\ \sigma_1 & \sigma_2 & \sigma_3 \\ \sigma_2 & \sigma_3 & \sigma_4 \end{pmatrix}.]$$

Proof. (a) By comparing the coefficients we observe that

$$s_1 = \alpha+\beta+\gamma \qquad s_2 = \alpha\beta+\beta\gamma+\gamma\alpha \qquad s_3 = \alpha\beta\gamma$$

Hence $\sigma_0 = \alpha^0+\beta^0+\gamma^0 = 3$. $\sigma_1 = \alpha+\beta+\gamma = s_1$. $\sigma_2 = \alpha^2+\beta^2+\gamma^2 = (\alpha+\beta+\gamma)^2 - 2(\alpha\beta+\beta\gamma+\gamma\alpha) = s_1^2 - 2s_2$.

In general, we expand the expression below

$$\begin{aligned} s_1\sigma_{r-1} - s_2\sigma_{r-2} + s_3\sigma_{r-3} &= (\alpha+\beta+\gamma)(\alpha^{r-1}+\beta^{r-1}+\gamma^{r-1}) - (\alpha\beta+\beta\gamma+\gamma\alpha)(\alpha^{r-2}+\beta^{r-2}+\gamma^{r-2}) + \alpha\beta\gamma(\alpha^{r-3}+\beta^{r-3}+\gamma^{r-3}) \\ &= \alpha^r+\beta^r+\gamma^r \\ &= \sigma_r \end{aligned}$$

Perhaps show more working

✓

(b) First we calculate σ_3 and σ_4:

$$\sigma_3 = s_1\sigma_2 - s_2\sigma_1 + s_3\sigma_0 = s_1^3 - 2s_1s_2 - s_1s_2 + 3s_3 = s_1^3 - 3s_1s_2 + 3s_3$$

$$\sigma_4 = s_1\sigma_3 - s_2\sigma_2 + s_3\sigma_1 = s_1^4 - 3s_1^2s_2 + 3s_1s_3 - s_1^2s_2 - 2s_2^2 + s_1s_3 = s_1^4 - 4s_1^2s_2 + 4s_1s_3 - 2s_2^2$$

It is well known that the van de Monde determinant satisfies

$$(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma) = \det\begin{pmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{pmatrix}$$

Hence

$$\Delta = (\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2 = \det\left(\begin{pmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{pmatrix}^T\right) = \det\begin{pmatrix} 3 & \alpha+\beta+\gamma & \alpha^2+\beta^2+\gamma^2 \\ \alpha+\beta+\gamma & \alpha^2+\beta^2+\gamma^2 & \alpha^3+\beta^3+\gamma^3 \\ \alpha^2+\beta^2+\gamma^2 & \alpha^3+\beta^3+\gamma^3 & \alpha^4+\beta^4+\gamma^4 \end{pmatrix}$$

$$= \det\begin{pmatrix} \sigma_0 & \sigma_1 & \sigma_2 \\ \sigma_1 & \sigma_2 & \sigma_3 \\ \sigma_2 & \sigma_3 & \sigma_4 \end{pmatrix} = \det\begin{pmatrix} \sigma_0 & \sigma_1 & \sigma_2 - s_1\sigma_1 + s_2\sigma_0 \\ \sigma_1 & \sigma_2 & \sigma_3 - s_1\sigma_2 + s_2\sigma_1 \\ \sigma_2 & \sigma_3 & \sigma_4 - s_1\sigma_3 + s_2\sigma_2 \end{pmatrix} = \det\begin{pmatrix} \sigma_0 & \sigma_1 & s_2 \\ \sigma_1 & \sigma_2 & s_3\sigma_0 \\ \sigma_2 & \sigma_3 & s_3\sigma_1 \end{pmatrix} = \det\begin{pmatrix} \sigma_0 & \sigma_1 & s_2 \\ \sigma_1 & \sigma_2 & 3s_3 \\ \sigma_2 & \sigma_3 & s_1s_3 \end{pmatrix}$$

$$= \det\begin{pmatrix} \sigma_0 & \sigma_1 & s_2 \\ \sigma_1 & \sigma_2 & 3s_3 \\ \sigma_2 - s_1\sigma_1 + s_2\sigma_0 & \sigma_3 - s_1\sigma_2 + s_2\sigma_1 & s_1s_3 - 3s_1s_3 + s_2^2 \end{pmatrix} = \det\begin{pmatrix} \sigma_0 & \sigma_1 & s_2 \\ \sigma_1 & \sigma_2 & 3s_3 \\ s_2 & 3s_3 & s_2^2 - 2s_1s_3 \end{pmatrix}$$

$$= \det\begin{pmatrix} 3 & s_1 & s_2 \\ s_1 & s_1^2 - 2s_2 & 3s_3 \\ s_2 & 3s_3 & s_2^2 - 2s_1s_3 \end{pmatrix} = 3\left((s_1^2-2s_2)(s_2^2-2s_1s_3) - 9s_3^2\right) - s_1\left(s_1(s_2^2-2s_1s_3) - 3s_2s_3\right) + s_2\left(3s_1s_3 - s_2(s_1^2-2s_2)\right)$$

$$= 18s_1s_2s_3 + s_1^2s_2^2 - 4s_2^3 - 4s_1^3s_3 - 27s_3^2$$

□

✓ well done.
I'm sure that wasn't fun.

A⁻

Question 8

Let E/F be an extension field of prime degree ℓ and let $\alpha \in E \backslash F$. Let M_α be F-linear map induced by the multiplication by α :

$$\begin{aligned} M_\alpha : E &\to E \\ u &\mapsto \alpha \cdot u \end{aligned}$$

Show that the characteristic polynomial of M_α is equal to the minimal polynomial of α. [*Hint: Cayley-Hamilton.*]

Proof. Consider the tower of field extensions: $F \subseteq F[\alpha] \subseteq E$. By tower law, $[F[\alpha] : F]$ divides $\ell = [E : F]$. Since ℓ is prime and $\alpha \notin F$, $[F[\alpha] : F] = \ell$ and hence $E = F[\alpha]$. ✓

We claim that $\{1, \alpha, ..., \alpha^{\ell-1}\}$ is a basis of $E = F[\alpha]$. let m be the minimal polynomial of α over F. For $f \in F[x]$, by division algorithm, there exists $q, r \in F[x]$ such that $f = qm + r$ and $\deg r < \deg m = \ell$. Then

$$f(\alpha) = r(\alpha) = a_0 + a_1\alpha + \cdots a_{\ell-1}\alpha^{\ell-1} \in \operatorname{span}\{1, \alpha, ..., \alpha^{\ell-1}\}$$

That is, $\{1, \alpha, ..., \alpha^{\ell-1}\}$ spans $F[\alpha]$. On the other hand, suppose that $a_0, ..., a_{\ell-1} \in F$ such that $a_0 + a_1\alpha + \cdots + a_{\ell-1}\alpha^{\ell-1} = 0$. Then $a_0 = \cdots = a_{\ell-1} = 0$ by minimality of of degree of m. Hence $\{1, \alpha, ..., \alpha^{\ell-1}\}$ is linearly independent.

Let $m(x) = x^\ell + a_{\ell-1}x^{\ell-1} + \cdots + a_1x + a_0$ be the minimal polynomial of α. Then

$$\alpha^\ell = -(a_{\ell-1}x^{\ell-1} + \cdots + a_1x + a_0)$$

With respect to the basis $\{1, \alpha, ..., \alpha^{\ell-1}\}$, the matrix of M_α is the (transpose of) companion matrix of m:

$$\begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ -a_0 & \cdots & -a_{\ell-2} & -a_{\ell-1} \end{pmatrix}$$

From linear algebra wo know that the characteristic polynomial of this matrix is exactly m, which finishes the proof. $\square$

Great! ✓

A