1. The polynomial $z^m - 1$ splits over $\mathbb{Q}$ to irreducible components

$$z^m - 1 = (z-1)\, p_1(z) \cdots p_k(z).$$

Since over $\mathbb{C}$ $z^m - 1 = 0$ has $m$ different roots

$$z^m - 1 = \prod_{j=0}^{m-1} \left(z - e^{i 2\pi j/m}\right)$$

for $j \neq k$ $(p_j, p_k) = 1$ ($p_j(z)$, $p_k(z)$ are coprime).

So a primitive $m$-root of 1, $\zeta$ is a root of some $p_k(\zeta) = 0$.

$$p_k = z^{m_k} + a_1 z^{m_k - 1} + \cdots + a_k$$

where $a_j$ are rational (By Gauss's lemma - integers)

So $\zeta^{m_k} = -a_1 \zeta^{m_k - 1} - \cdots - a_k$

and $1, \zeta, \ldots, \zeta^{m_k - 1}$ are lin. in. over $\mathbb{Q}$ since $p_k(z)$ irreducible. According to Theorem 1.15 (p 20 of my notes) $\mathbb{Q}[z]/(p_k(z))$ is a field. Every element in this field is isomorphic $\mathbb{Q}[\zeta] := \{ \cancel{a_0} + b_0 + b_1\zeta + \cdots + b_{m_k - 1}\zeta^{m_k - 1} \}$

Now $\zeta \in \mathbb{Q}[\zeta]$. Since $\mathbb{Q}[\zeta]$ is a field $\zeta^q \in \mathbb{Q}[\zeta]$ for all $q \in \mathbb{N}$. Since $\zeta$ is a primitive root, $\zeta, \zeta^2, \ldots, \zeta^m = 1$ are in $\mathbb{Q}[\zeta]$

So it is also true that

$$\mathbb{Q}[\zeta] = \{ b_0 + b_1 \zeta + \cdots + b_{m-1}\zeta^{m-1} \}$$
$$b_0, \ldots, b_{m-1} \in \mathbb{Q}$$

2. (a) Simple computation.

$$\overline{(a_0 + a_1 \underline{i} + a_2 \underline{j} + a_3 \underline{k})(b_0 + b_1 \underline{i} + b_2 \underline{j} + b_3 \underline{k})}$$

$$= \overline{(b_0 + b_1 \underline{i} + b_2 \underline{j} + b_3 \underline{k})}\ \overline{(a_0 + a_1 \underline{i} + a_2 \underline{j} + a_3 \underline{k})}$$

Since $\overline{\underline{i}\,\underline{j}} = \overline{\underline{k}} = -\underline{k} = \overline{\underline{j}} \cdot \overline{\underline{i}} = (-\underline{j})(-\underline{i}) = -\underline{k}$

similarly for all other products

(b) $q\bar{q} = \bar{q}q = a_0^2 + a_1^2 + a_2^2 + a_3^2$ – straight computation.
"$|q|^2$"

~~Hence for $\bar{q} \neq 0$~~

$$q^{-1} = \frac{1}{|q|^2}\bar{q}$$

---

Page 11 – M425 notes

1. (a) ~~$A = A^T$~~ $AA^{-1} = I_n \Rightarrow (AA^{-1})^T = I_n^T = I_n$

$(A^{-1})^T A^T = I_n \Rightarrow (A^T)^{-1} = (A^{-1})^T$

b. $A = A^T \Leftrightarrow (A^{-1}) = (A^T)^{-1} = (A^{-1})^T$

c. $A^T = -A \Leftrightarrow (-A)^{-1} = -A^{-1} = (A^T)^{-1} = (A^{-1})^T$

d, Follow from G–J elimination

$$[A|I] \to [I|A^{-1}]$$

If $A$ l.t. use only ERO in Gauss elimination which are lower triangular so $A^{-1} = E_k \dots E_1$ and each $E_i$ is l.t. As a product of l.t. is l.t $A^{-1}$ is l.t.
Similarly for u.t.

2, Gaus elimination with no making pivots to (1)

$E_k \dots E_1 A = U$ ← upper triangular
each $E_i = \begin{bmatrix} 1 & 0 \\ a_{ij} & 1 \end{bmatrix}$ so

$$A = (E_1^{-1} \dots E_k^{-1})U = LU$$

3. ~~AB^T~~ $B = [\underline{b}_1 \dots \underline{b}_n]$ $\underline{b}_i \in \mathbb{R}^m$

$$AB = [A\underline{b}_1 \ \dots \ A\underline{b}_n]$$

Recall that $A\underline{x}$ is a linear combination of the columns of $A$.

So $A\underline{b}_1, \dots, A\underline{b}_n \in R(A)$ (the column space of $A$)

Hence the column space of $A$ contains the column space of $AB$. Hence

$$\operatorname{rank}(AB) \le \operatorname{rank}(A)$$

Observe that $(AB)^T = B^T A^T$ so

$$\operatorname{rank}(AB) = \operatorname{rank}((AB)^T) = \operatorname{rank}(B^T A^T) \le \underset{\overset{\shortparallel}{\operatorname{rank}(B)}}{\operatorname{rank}(B^T)}.$$

Hence $\operatorname{rank}(AB) \le \min(\operatorname{rank} A, \operatorname{rank} B)$.

Suppose $A$ invertible.

Then $B = A^{-1}(AB)$

$$\operatorname{rank}(B) \le \min(\underbrace{\operatorname{rank}(A^{-1})}_{m = \ell}, \underset{\overset{\wedge}{m}}{\operatorname{rank}(AB)})$$

$$= \operatorname{rank}(AB)$$

But $\operatorname{rank}(AB) \le \operatorname{rank}(B)$.

Hence $\operatorname{rank}(AB) = \operatorname{rank}(B)$ if $A$ invertible

Similarly $\operatorname{rank}(AB) = \operatorname{rank}(A)$ if $B$ invertible.

1. a. $\text{span}(1, t, \dots, t^n) \stackrel{\text{def}}{=} P_n$.

b. It is left to show that $1, \dots, t^n$ l.i. Suppose that

$$p(t) = \sum_{i=0}^{n} a_i t^i \equiv 0 \qquad \text{so } 0 = p^{(j)}(0) = j!\, a_j \Rightarrow a_j = 0,\ j = 0, \dots, n$$

Hence $1, t, \dots, t^n$ l.i.

2. $$\begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_n \end{bmatrix} = \underbrace{\begin{bmatrix} a_{00} & 0 & \cdots & 0 \\ a_{10} & a_{11} & & 0 \\ \vdots & & \ddots & \\ a_{n0} & \cdots & & a_{nn} \end{bmatrix}}_{A} \begin{bmatrix} 1 \\ \vdots \\ t^n \end{bmatrix}; \quad A = \begin{bmatrix} a_{00} & 0 & \cdots & 0 \\ a_{10} & a_{11} & & \\ \vdots & & \ddots & \end{bmatrix}$$

$A$ is lower triangular, $a_{ii} \neq 0$ since $\deg p_i = i$

So $\det A = a_{00} a_{11} \cdots a_{nn} \neq 0$

$A$ invertible. Hence $p_0, \dots, p_n$ is a basis too.

3. Take $p_k(t) = x^n + x^k$ for $k = 0, 1, \dots, n$

Then

$$\begin{bmatrix} p_0 \\ \vdots \\ p_n \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & 1 & 0 & \cdots & 0 & 1 \\ & & \ddots & & \\ 0 & & & & 1 \end{bmatrix}}_{A} \begin{bmatrix} 1 \\ \vdots \\ t^n \end{bmatrix}, \quad A \text{ upper triangular}, \ \det A = 1$$

Hence $p_0, \dots, p_n$ basis.

5. Put a matrix from the given columns

$$A = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \to$$

Bring it to REF

$$B = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & -1 & -1 & 0 \\ 0 & 0 & 1 & -2 & -1 & -1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$B$ = has full rank, So column space of $A$ is $\mathbb{C}^4$ $(\mathbb{R}^4)$

The first 4 columns form a basis. Probably any 4 of them form a basis. This needs $\binom{6}{4} = \binom{6}{2} = \underline{\underline{15}}$ checks!