Permutation Groups

Definition 1. Let Ω be a nonempty set. Define $S_\Omega = \{\Omega \to^\sigma \Omega : \sigma$ is a bijection$\}$. If $\Omega = \{1, 2, 3, ..., n\}$, then we write S_n instead of S_Ω. a bijection $\sigma \in S_n$ is called a permutation.

Examples 2. If $\Omega = \{1, 2, 3\}$, then S_3 consists of the following permutations.

$$\begin{array}{cccccc} \underline{\sigma_1} & \underline{\sigma_2} & \underline{\sigma_3} & \underline{\sigma_4} & \underline{\sigma_5} & \underline{\sigma_6} \\ 1 \mapsto 1 & 1 \mapsto 2 & 1 \mapsto 3 & 1 \mapsto 2 & 1 \mapsto 3 & 1 \mapsto 1 \\ 2 \mapsto 2 & 2 \mapsto 3 & 2 \mapsto 1 & 2 \mapsto 1 & 2 \mapsto 2 & 2 \mapsto 3 \\ 3 \mapsto 3 & 3 \mapsto 1 & 3 \mapsto 2 & 3 \mapsto 3 & 3 \mapsto 1 & 3 \mapsto 2 \end{array}$$

Here is an example of how the composition works

$$\begin{array}{c} \underline{\sigma_3 \circ \sigma_5} \\ 1 \mapsto 3 \mapsto 2 \\ 2 \mapsto 2 \mapsto 1 \\ 3 \mapsto 1 \mapsto 3 \end{array}$$

It follows that $\sigma_3 \circ \sigma_5 = \sigma_4$ and a similar computation shows that $\sigma_5 \circ \sigma_3 = \sigma_6$. Here is a tableof all possible compositions

$\circ$	1_Ω	σ_2	σ_3	σ_4	σ_5	σ_6
1_Ω	1_Ω	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_3	1_Ω	σ_5	σ_6	σ_4
σ_3	σ_3	1_Ω	σ_2	σ_6	σ_4	σ_5
σ_4	σ_4	σ_6	σ_5	1_Ω	σ_3	σ_2
σ_5	σ_5	σ_4	σ_6	σ_2	1_Ω	σ_3
σ_6	σ_6	σ_5	σ_4	σ_3	σ_2	1_Ω

A multiplication table of this type gives a great deal of information about S_3. Since the table is not symmetric about the diagonal, we may conclude that $\circ$ is not commutative. Also we can easily check, for example, that $\sigma_3^{-1} = \sigma_2$ and that $\sigma_4^{-1} = \sigma_4$.

Definition 3. A typical element in S_n is denoted

$$\sigma = \begin{bmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{bmatrix}.$$

For example, if $n = 4$ then

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{bmatrix}$$

indicates that $\sigma(1) = 2, \sigma(2) = 4, \sigma(3) = 3, \sigma(4) = 1$. A *cycle* of length k is a permutation $\sigma \in S_n$ such that $\sigma(a_1) = a_2, \sigma(a_2) = a_3$,...,$\sigma(a_k) = a_1$ and

$\sigma(x) = x$ for all other $x \in \{1, 2, ..., n\}$. In this case, we write $\sigma = (a_1\ a_2\ ...\ a_k)$. It is easy to check that $\sigma^r(a_i) = a_{i+r(\mathrm{mod}\,k)}$ for each integer r. For example if $n = 7$ then

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 5 & 1 & 4 & 2 & 7 \end{bmatrix} = (1\ 6\ 2\ 3\ 5\ 4).$$

Two cycles $\sigma = (a_1\ a_2 ... a_k)$ and $\tau = (b_1\ b_2 ... b_l)$ are called *disjoint* if the sets $\{a_1, a_2, ..., a_k\}$ and $\{b_1, b_2, ..., b_l\}$ are disjoint.

Theorem 4. Every $\sigma \in S_n$ is a product of disjoint (and hence commuting) cycles.

Example 5. Let $n = 12$ and let

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 4 & 8 & 5 & 9 & 10 & 12 & 1 & 11 & 7 & 2 & 6 \end{bmatrix}.$$

Then $\sigma = (1\ 3\ 8)(2\ 4\ 5\ 9\ 11)(6\ 10\ 7\ 12)$.

Definition 6. We call any 2-cycle in S_n a *transposition*. We say that a permutation in S_n is *even* if it can be written as a product of an even number of transpositions. We call it *odd* otherwise.

Theorem 7. Every permutation in S_n can be written (not necessarily uniquely) as a product of transpositions.

Proof. By Theorem 1.8.3 any permutaion $\sigma \in S_n$ can be written as a product of disjoint cycles. Thus it suffices to show that every cycle can be written as a product of transpositions. One easily checks that $(1\ 2\ ...\ k) = (1\ k)(1\ k-1)...(1\ 2)$ and the proposition is verified.

Definition 8. Consider the group S_n and let $x_1, x_2, ..., x_n$ be indeterminates. We define the polynomial $P = P(x_1, x_2, ..., x_n) = \Pi_{i<j}(x_i - x_j)$. If $\sigma \in S_n$ then we set $\sigma(P) = \Pi_{i<j}(x_{\sigma(i)} - x_{\sigma(j)})$.

Example 9. Let $n = 4$ and let $\sigma = (2\ 4)$. Then

$$P = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$$

and

$$\begin{aligned} \sigma(P) &= (x_1 - x_4)(x_1 - x_3)(x_1 - x_2)(x_4 - x_3)(x_4 - x_2)(x_3 - x_2) \\ &= -(x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4) \\ &= -P. \end{aligned}$$

Lemma 10. Let $\sigma \in S_n$ be any transposition. Then $\sigma(P) = -P$.

Proof. Suppose that $\sigma = (r\ s)$ with $r < s$. We check cases regarding the factors of P.
(1) The factor $(x_i - x_j)$ has indices distinct from r, s. Thus, $\sigma(x_i - x_j) = (x_i - x_j)$ and no change in sign occurs.
(2) The factor $(x_i - x_j) = (x_r - x_s)$ so that $\sigma(x_r - x_s) = (x_s - x_r) = -(x_r - x_s)$.
(3) The factor $(x_i - x_j)$ has an index equal to either r or s but not both. We check pairs. If the other index is k then we have either $k < r < s$, $r < k < s$, or $r < s < k$.
If $k < r < s$ then $\sigma((x_k - x_r)(x_k - x_s)) = (x_k - x_s)(x_k - x_r) = (x_k - x_r)(x_k - x_s)$ and no change in sign occurs.
If $r < k < s$ then $\sigma((x_r - x_k)(x_k - x_s)) = (x_s - x_k)(x_k - x_r) = (-(x_r - x_k))(-(x_k - x_s)) = (x_r - x_k)(x_k - x_s)$ and no change in sign occurs.
If $r < s < k$ then $\sigma((x_r - x_k)(x_s - x_k)) = (x_s - x_k)(x_r - x_k) = (x_r - x_k)(x_s - x_k)$ and no change in sign occurs.
Thus, there is only one net change in sign at the factor $(x_r - x_s)$ so that $\sigma(P) = -P$.

Theorem 11. A permutation is either even or odd but not both.

Proof. Let $\sigma \in S_n$ and write $\sigma = \tau_1\tau_2...\tau_j$ where each τ_i is a transpositions and suppose that there is another decomposition $\sigma = \omega_1\omega_2...\omega_k$ into transpositions. Then $\sigma(P) = \tau_1\tau_2...\tau_j(P) = (-1)^j P$ and $\sigma(P) = \omega_1\omega_2...\omega_k(P) = (-1)^k P$ so that $(-1)^j P = (-1)^k P$. It follows that $j \equiv k (\bmod 2)$; that is, j, k are both even or both odd.

Definition 12. We define a map $\operatorname{sgn} : S_n \to \{\pm 1\}$ given by

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \sigma \text{ even} \\ -1 & \sigma \text{ odd} \end{cases}.$$

This map is well-defined by Theorem 11.

Theorem 13. For $\sigma, \tau \in S_n$ we have $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$

Theorem 14. The following hold for a fixed integer $n \geq 2$.
(a) S_n is closed with respect to composition of maps $\circ$.
(b) The operation of composition $\circ$ is associative.
(c) S_n has the identity map 1 with respect to composition.
(d) Each $\sigma \in S_n$ has a unique inverse $\sigma^{-1} \in S_n$.

Determinants

Definition 1. Let $A = [a_{ij}] \in \mathcal{M}_n(F)$ and define a map $\det : \mathcal{M}_n(F) \to F$ by

$$\det(A) = \det(a_{ij}) = \Sigma_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}.$$

We often write $|A| = \det(a_{ij})$.

Example 2. Let

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}.$$

Then $S_2 = \{\sigma_1, \sigma_2\}$ where

$$\sigma_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = (1) \text{ and } \sigma_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (1\ 2).$$

It follows that

$$\begin{aligned} \det(A) &= \Sigma_{\sigma \in S_2} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \\ &= \operatorname{sgn}(\sigma_1) a_{1\sigma_1(1)} a_{2\sigma_1(2)} + \operatorname{sgn}(\sigma_2) a_{1\sigma_2(1)} a_{2\sigma_2(2)} \\ &= a_{11}a_{22} - a_{12}a_{21}. \end{aligned}$$

Lemma 3. Let $\sigma \in S_n$. If $i \leq \sigma(i)$ for each $i \in \{1, 2, ..., n\}$, then $\sigma = 1$.

Proof. Since $\sigma(n) \in \{1, 2, ..., n\}$, it is certainly true that $\sigma(n) \leq n$. On the other hand, $i \leq \sigma(i)$ for each $i \in \{1, 2, ..., n\}$ implies that $n \leq \sigma(n)$. Therefore, $\sigma(n) = n$ and it now follows that $\sigma(n-1) \in \{1, 2, ..., n-1\}$. Indeed, if $\sigma(n-1) = n$, then the previous sentence gives $\sigma(n-1) = \sigma(n)$. Since σ is 1-1, we arrive at the absurdity $n - 1 = n$. Since $\sigma(n-1) \in \{1, 2, ..., n-1\}$, we have that $\sigma(n-1) \leq n - 1$ and the assumption $i \leq \sigma(i)$ for each $i \in \{1, 2, ..., n\}$ implies $n - 1 \leq \sigma(n-1)$. Hence, $\sigma(n-1) = n - 1$ and continuing in this way, we find that $\sigma(i) = i$ for each $i \in \{1, 2, ..., n\}$. Therefore, σ is the identity permutation (1) as needed.

Theorem 4. If $A = [a_{ij}]$ is an upper triangular $n \times n$ matrix, then $\det(A) = a_{11}a_{22} \cdots a_{nn}$.

Proof. Since A is upper triangular, we know that $i > j$ implies $a_{ij} = 0$. If the summand $\operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$ in the definition of the determinant is non-zero, then $a_{i\sigma(i)} \neq 0$ for each $i \in \{1, 2, ..., n\}$. By upper triangularity, we have that $i \leq \sigma(i)$ for each $i \in \{1, 2, ..., n\}$. But then Lemma 3 says that $\sigma(i) = i$ for each $i \in \{1, 2, ..., n\}$. In other words, the only non-zero summand in $\det(A)$ corresponds to the identity permutation $\sigma = 1$. Therefore,

$$\operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} = a_{11}a_{22} \cdots a_{nn}.$$

Lemma 5. Fix any $i, j \in \{1, 2, ..., n\}$ such that $i < j$. If $S = \{\sigma \in S_n : \sigma(i) < \sigma(j)\}$ and $T = \{\sigma \in S_n : \sigma(i) > \sigma(j)\}$ then the following hold.
(1) $S_n = S \cup T$ is a disjoint union.
(2) $|S| = |T|$
(3) $T = S\tau$ where $\tau = (i\ j)$ is the transposition switching i and j.

Proof.
(1) Choose any $\sigma \in S_n$. Since $\sigma(i), \sigma(j) \in \{1, 2, ..., n\}$, it is certainly true that either $\sigma(i) < \sigma(j)$ or $\sigma(i) = \sigma(j)$ or $\sigma(i) > \sigma(j)$. If $\sigma(i) = \sigma(j)$, then injectivity (1-1) of σ implies $i = j$ which is false. Hence either $\sigma(i) < \sigma(j)$ or $\sigma(i) > \sigma(j)$. Therefore, either $\sigma \in S$ or $\sigma \in T$.
(2) Let $\tau = (i\ j) \in S_n$ and definea map $\Phi : S \to T$ by $\Phi(\sigma) = \sigma \circ \tau$. We must show that Φ is a well-defined bijection. (WD1) Since $(\sigma \circ \tau)(j) = \sigma(\tau(j)) = \sigma(i) < \sigma(j) = \sigma(\tau(i)) = (\sigma \circ \tau)(j)$, we have that $\Phi(\sigma) = \sigma \circ \tau \in T$. (1-1) If $\Phi(\sigma_1) = \Phi(\sigma_2)$, then $\sigma_1 \circ \tau = \sigma_2 \circ \tau$. Multiplying by τ^{-1},we have that $(\sigma_1 \circ \tau) \circ \tau^{-1} = (\sigma_2 \circ \tau) \circ \tau^{-1}$. By associativity, $\sigma_1 \circ (\tau \circ \tau^{-1}) = \sigma_2 \circ (\tau \circ \tau^{-1})$ and so $\sigma_1 \circ 1 = \sigma_2 \circ 1$. Therefore, $\sigma_1 = \sigma_2$ as needed. (Onto) Choose any $\sigma \in T$. Then $\sigma \circ \tau^{-1} \in S$ (as in WD1) and $\Phi(\sigma \circ \tau^{-1}) = (\sigma \circ \tau^{-1}) \circ \tau = \sigma$ (as in 1-1).
(3) Follows immediately from (2). Indeed $T = \Phi(S) = S\tau$.

Theorem 6. If $\mathbf{r}_i(A) = \mathbf{r}_j(A)$, then $\det(A) = 0$.

Proof. As in the previous lemma, let $\tau = (i\ j)$ and $S = \{\sigma \in S_n : \sigma(i) < \sigma(j)\}$. We have

$$
\begin{aligned}
& \det(A) \\
= \ & \Sigma_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} \quad (1) \\
= \ & \Sigma_{\sigma \in S \cup T} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} \quad (2) \\
= \ & \Sigma_{\sigma \in S} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} + \Sigma_{\sigma \in T} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} \quad (3) \\
= \ & \Sigma_{\sigma \in S} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} + \Sigma_{\sigma \in S\tau} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} \quad (4) \\
= \ & \Sigma_{\sigma \in S} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} + \Sigma_{\sigma \in S} \operatorname{sgn}(\sigma\tau) a_{1\sigma\tau(1)} \cdots a_{n\sigma\tau(n)} \quad (5) \\
= \ & \Sigma_{\sigma \in S} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} - \operatorname{sgn}(\sigma) a_{1\sigma\tau(1)} \cdots a_{n\sigma\tau(n)} \quad (6) \\
= \ & \Sigma_{\sigma \in S} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{i\sigma(i)} \cdots a_{j\sigma(j)} \cdots a_{n\sigma(n)} - \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{i\sigma(j)} \cdots a_{j\sigma(i)} \cdots a_{n\sigma(n)} \quad (7) \\
= \ & 0 \quad (\text{since } a_{i\sigma(i)} = a_{j\sigma(i)} \text{ and } a_{j\sigma(j)} = a_{i\sigma(j)} \quad (8)
\end{aligned}
$$

Theorem 7. $\det(A) = \det(A^{\mathrm{T}})$.

Proof.

$$
\begin{aligned}
& \det(A^{\mathrm{T}}) \\
= \; & \Sigma_{\sigma\in S_n} \operatorname{sgn}(\sigma)\, \mathrm{ent}_{1\sigma(1)}(A^{\mathrm{T}}) \cdots \mathrm{ent}_{n\sigma(n)}(A^{\mathrm{T}}) \\
= \; & \Sigma_{\sigma\in S_n} \operatorname{sgn}(\sigma)\, \mathrm{ent}_{\sigma(1)1}(A) \cdots \mathrm{ent}_{\sigma(n)n}(A) \\
= \; & \Sigma_{\sigma\in S_n} \operatorname{sgn}(\sigma)\, \mathrm{ent}_{k_1 1}(A) \cdots \mathrm{ent}_{k_n n}(A) \quad \text{(setting } k_i = \sigma(i)\text{)} \\
= \; & \Sigma_{\sigma\in S_n} \operatorname{sgn}(\sigma)\, \mathrm{ent}_{k_1 \sigma^{-1}(k_1)}(A) \cdots \mathrm{ent}_{k_n \sigma^{-1}(k_n)}(A) \quad \text{(since } i = \sigma^{-1}(k_i)\text{)} \\
= \; & \Sigma_{\sigma\in S_n} \operatorname{sgn}(\sigma)\, \mathrm{ent}_{1\sigma^{-1}(1)}(A) \cdots \mathrm{ent}_{n\sigma^{-1}(n)}(A) \quad \text{(since } \{1,...,n\} = \{k_1,...,k_n\}\text{)} \\
= \; & \Sigma_{\sigma\in S_n} \operatorname{sgn}(\sigma^{-1})\, \mathrm{ent}_{1\sigma^{-1}(1)}(A) \cdots \mathrm{ent}_{n\sigma^{-1}(n)}(A) \quad \text{(since sgn is multiplicative)} \\
= \; & \Sigma_{\sigma\in S_n} \operatorname{sgn}(\sigma)\, \mathrm{ent}_{1\sigma(1)}(A) \cdots \mathrm{ent}_{n\sigma(n)}(A) \quad \text{(as } \sigma \text{ runs through } S_n \text{ so does } \sigma^{-1}\text{)}
\end{aligned}
$$

Corollary 8. If A is lower triangular, then the result of Theorem 4 still holds.

Exercises

1. Prove the following identities for $i \neq j$ and $c \in F$.
(a) $\det(I_n) = 1$
(b) $\det([0]) = 0$
(c) $\det(cI_n) = c^n$

2. Prove that det is linear ineach row. That is, prove the equalities

$$
\det \begin{bmatrix} \mathbf{r}_1 \\ \vdots \\ c\mathbf{r}_i \\ \vdots \\ \mathbf{r}_n \end{bmatrix} = c \det \begin{bmatrix} \mathbf{r}_1 \\ \vdots \\ \mathbf{r}_i \\ \vdots \\ \mathbf{r}_n \end{bmatrix} \quad \text{and} \quad \det \begin{bmatrix} \mathbf{r}_1 \\ \vdots \\ \mathbf{r}_i + \mathbf{s}_i \\ \vdots \\ \mathbf{r}_n \end{bmatrix} = \det \begin{bmatrix} \mathbf{r}_1 \\ \vdots \\ \mathbf{r}_i \\ \vdots \\ \mathbf{r}_n \end{bmatrix} + \det \begin{bmatrix} \mathbf{r}_1 \\ \vdots \\ \mathbf{s}_i \\ \vdots \\ \mathbf{r}_n \end{bmatrix}.
$$

Conclude that $\det(cA) = c^n \det(A)$. Conclude also that if $\mathbf{r}_i(A) = (0, 0, ..., 0)$, then $\det(A) = 0$.

3. Prove that for any $i, j \in \{1, 2, ..., n\}$ with $i \neq j$

$$
\det \begin{bmatrix} \mathbf{r}_1(A) \\ \vdots \\ \mathbf{r}_i(A) \\ \vdots \\ \mathbf{r}_j(A) \\ \vdots \\ \mathbf{r}_n(A) \end{bmatrix} = -\det \begin{bmatrix} \mathbf{r}_1(A) \\ \vdots \\ \mathbf{r}_j(A) \\ \vdots \\ \mathbf{r}_i(A) \\ \vdots \\ \mathbf{r}_n(A) \end{bmatrix}.
$$

4. Prove the following facts for the elementary matrices. Assume that $i, j \in \{1, 2, ..., n\}$ with $i \neq j$ and $c \neq 0$.
(a) $\det(E_{i \to ci}) = c$.
(b) $\det(E_{i \leftrightarrow j}) = -1$.
(c) $\det(E_{i \to i+cj}) = 1$.

5. Prove that for any $\sigma \in S_n$

$$\det \begin{bmatrix} \mathbf{r}_{\sigma(1)}(A) \\ \mathbf{r}_{\sigma(2)}(A) \\ \vdots \\ \mathbf{r}_{\sigma(n)}(A) \end{bmatrix} = \operatorname{sgn}(\sigma) \det \begin{bmatrix} \mathbf{r}_1(A) \\ \mathbf{r}_2(A) \\ \vdots \\ \mathbf{r}_n(A) \end{bmatrix}.$$

Hint: Use Exercise 2 and Theorem 6.

6. Prove that for any $i, j \in \{1, 2, ..., n\}$ with $i \neq j$

$$\det \begin{bmatrix} \mathbf{r}_1(A) \\ \vdots \\ c\mathbf{r}_j(A) + \mathbf{r}_i(A) \\ \vdots \\ \mathbf{r}_j(A) \\ \vdots \\ \mathbf{r}_n(A) \end{bmatrix} = \det \begin{bmatrix} \mathbf{r}_1(A) \\ \vdots \\ \mathbf{r}_i(A) \\ \vdots \\ \mathbf{r}_j(A) \\ \vdots \\ \mathbf{r}_n(A) \end{bmatrix}$$

7. Prove that if E is an elementary matrix, then $\det(EA) = \det(E)\det(A)$.

Multiplicative Properties

Theorem 9. A square matrix A is invertible if and only if $\det(A) \neq 0$.

Proof. ($\Rightarrow$) If A is invertible, then it is a product of elementary matrices and we can write $A = E_1 E_2 \cdots E_m$. By Exercise 7, We have

$$\begin{aligned} & \det(A) \\ = \ & \det(E_1 E_2 \cdots E_m) \\ = \ & \det(E_1)\det(E_2 \cdots E_m) \\ & \vdots \\ = \ & \det(E_1)\det(E_2) \cdots \det(E_m). \end{aligned}$$

By Exercise 4, each $\det(E_k) \neq 0$. Therefore, $\det(A) \neq 0$.

($\Rightarrow$) If A is not invertible, then it is singular and so $\text{rank}(A) < n$. It follows that there exist elementary matrices $E_1, E_2, ..., E_m$ such that $E_1 E_2 \cdots E_m A$ has at least one row of all zeros. By Exercises 2 and 7, we have that

$$0 = \det(E_1 E_2 \cdots E_m A) = \det(E_1)\det(E_2)\cdots\det(E_m)\det(A).$$

By Exercise 4, each $\det(E_k) \neq 0$. Therefore, $\det(A) = 0$.

Theorem 10. If $A, B \in \mathcal{M}_n(F)$, then $\det(AB) = \det(A)\det(B)$.

Proof. We consider the two cases where A is invertible and A is not invertible. If A is invertible, then there exist elementary matrices $E_1, E_2, ..., E_m$ such that $A = E_1 E_2 \cdots E_m$. It follows that $AB = E_1 E_2 \cdots E_m B$ and so

$$\begin{aligned}
& \det(AB) \\
= \; & \det(E_1 E_2 \cdots E_m B) \\
= \; & \det(E_1)\det(E_2 \cdots E_m B) \\
& \vdots \\
= \; & \det(E_1)\det(E_2)\cdots\det(E_m)\det(B) \\
& \vdots \\
= \; & \det(E_1 E_2 \cdots E_m)\det(B) \\
= \; & \det(A)\det(B).
\end{aligned}$$

If A is not invertible, then AB is not invertible either. Therefore $\det(AB) = 0 = 0\det(B) = \det(A)\det(B)$.

Corollary 11. If A is invertible, then $\det(A^{-1}) = \frac{1}{\det(A)}$.

Proof. Since $AA^{-1} = I_n$, Theorem 11 says $\det(A)\det(A^{-1}) = 1$. Since A is invertible, $\det(A) \neq 0$, we can divide to get $\det(A^{-1}) = \frac{1}{\det(A)}$.

Definition 12. Let $A \in \mathcal{M}_n$ and define the characteristic polynomial of A to be

$$\chi_A(x) = \det(A - xI_n).$$

It is necessarily the case that $\chi_A(x) \in F[x]$. The characteristic equation of $T \in \mathcal{A}(F^n)$ is defined to be $\chi_{A_T}(x)$.

Theorem 13. Let $A, B \in \mathcal{M}_n(F)$. The following hold.
(a) If $A \sim B$, then $\chi_A(x) = \chi_B(x)$.
(b) If $\lambda \in F$, then λ is an eigenvalue of A if and only if λ is a root of $\chi_A(x)$.
(c) (Cayley-Hamilton) $\chi_A(A) = 0$.

Proof.

(a) Since $A \sim B$, there exists an invertible matrix P such that $B = PAP^{-1}$. Verify using the usual matrix arithmetic that $P(A - xI_n)P^{-1} = PAP^{-1} - xI_n$. Therefore,

$$\begin{aligned} & \chi_B(x) \\ = \;& \det(B - xI_n) \\ = \;& \det(PAP^{-1} - xI_n) \\ = \;& \det(P(A - xI_n)P^{-1}) \\ = \;& \det(P)\det(A - xI_n)\det(P^{-1}) \\ = \;& \det(P)\det(A - xI_n)\det(P)^{-1} \\ = \;& \det(P)^{-1}\det(P)\det(A - xI_n) \\ = \;& \det(A - xI_n) \\ = \;& \chi_A(x). \end{aligned}$$

(b) If $\lambda \in F$ is an eigenvalue of A, then $\mathrm{Null}(A - \lambda I_n) \neq \{\mathbf{0}\}$. It follows that $A - \lambda I_n$ is not an invertible matrix. By Theorem 9, $\det(A - \lambda I_n) = 0$ and so $\chi_A(\lambda) = 0$. Just reverse the argument for the converse.
(c) If $A \in \mathcal{M}_n(\mathbb{C})$, then there exists an invertible matrix such that $B = PAP^{-1}$ is upper triangular. We now have

$$\begin{aligned} & \chi_A(x) \\ = \;& \chi_B(x) \quad \text{(part(b))} \\ = \;& \det(B - xI_n) \quad \text{(defn)} \\ = \;& (b_{11} - x)(b_{22} - x)\cdots(b_{nn} - x) \quad \text{(Theorem 4)} \end{aligned}$$

This was our original definition for the characteristic polynomial and we have already proved the result in this case. If $A \in \mathcal{M}_n(\mathbb{R})$, then $A \in \mathcal{M}_n(\mathbb{C})$ and we can repeat the program above.