MA-219 Linear Algebra

14. Determinants – Permutations, Multi-linear and alternating maps

October 28, 2003 ; Submit solutions **before 11:00 AM ; November 03, 2003.**

14.1. Let T be a set of transpositions in the group $\mathfrak{S}_n$, $n \geq 1$. We associate the graph [1] Γ_T to T as follows: the vertices of Γ_T are the numbers $1, \ldots, n$ and two vertices i and j with $i \neq j$ are joined by a edge if and only if the transposition $\langle i, j\rangle = \langle j, i\rangle$ belong to T. Let $\Gamma_1, \ldots, \Gamma_r$ be the connected components of Γ_T .

a). The transpositions in T generate the group $\mathfrak{S}_n$ if and only if Γ_T is connected, i.e. if any two vertices of Γ_T can be joined by the sequence of edges in Γ_T. The subgroup of $\mathfrak{S}_n$ generated by T is the product $\mathfrak{S}(\Gamma_1) \times \cdots \times \mathfrak{S}(\Gamma_r) \subseteq \mathfrak{S}_n$.

b). If T is a generating system for the group $\mathfrak{S}_n$, then T has at least $n-1$ elements. (**Hint:** Let $\tau_1, \ldots, \tau_m$ be the elements of T (may be with repeatations) with $\tau_1 \cdots \tau_m = \mathrm{id}$. Then m is even and $m \geq 2\sum_{\rho=1}^{r}(|\Gamma_\rho|-1)$.)

c). Every generating system of $\mathfrak{S}_n$ consisting of transpositions contain a (minimal) generating system of $\mathfrak{S}_n$ with $n-1$ elements. (The graphs corresponding to such a minimal generating systems are called *trees*. Every connected graph has a generating system which is a tree. –There are exactly n^{n-2} generating systems consisting $n-1$ transpositions. (**Hint:** Prove this by descending induction k; induction starts at $k = n-1$: the number of trees in which the number 1 belongs to exactly k edges, is $(n-1)^{n-k-1}\binom{n-2}{k-1}$ and add.)

d). The transpositions $\langle 1, 2\rangle$, $\langle 2, 3\rangle , \ldots , \langle n-1, n\rangle$ (resp. $\langle 1, 2\rangle$, $\langle 1, 3\rangle , \ldots , \langle 1, n\rangle$) form a minimal generating system of $\mathfrak{S}_n$. (**Hint:** If a, b, c are three distinct elements, then $\langle a\, b\rangle\langle a\, c\rangle\langle a\, b\rangle = \langle b\, c\rangle$.)

14.2. a). Let v_j , $j \in J$ be a basis of the K-vector space V and let $w_{(j_i)}$, $(j_i) \in J^I$ be a family of elements of the K-vector space W, where I is a finite indexed set. Then there exists a unique K-multilinear map $f : V^I \to W$ such that $f\big((v_{j_i})_{i\in I}\big) = w_{(j_i)}$, $(j_i) \in J^I$. If V and W are finite dimensional, then the K-vector space of the multilinear maps from V^I into W has the dimension $(\mathrm{Dim}_K\, V)^{|I|} \cdot \mathrm{Dim}_K\, W$.

b). A multilinear map $f : V^n \to W$ of K-vector spaces is alternating if $f(x_1, \ldots, x_n) = 0$ for every n-tuple $(x_1, \ldots, x_n)$ in which two *consecutive* components are equal.

14.3. Let V and W be K-vector spaces.

a). Let I be a finite indexed set with n elements. Suppose that in K the element $n! = n! \cdot 1_K$ is non-zero, i.e. $\mathrm{Char}\, K = 0$ or $\mathrm{Char}\, K > n$. Then the maps $f \mapsto \frac{1}{n!}Af$ and $f \mapsto \frac{1}{n!}Sf$

---

[1]) **Simplicial Complexes and Graphs.** A *simplicial complex* $\mathcal{K}$ is a set $\mathbf{V}(\mathcal{K})$ called the *vertex set* (of $\mathcal{K}$) and a family of subsets of $\mathbf{V}(\mathcal{K})$, called *simplexes* (in $\mathcal{K}$) such that
(i) for each $v \in \mathbf{V}(\mathcal{K})$, the singleton set $\{v\}$ is a simplex in K.
(ii) if $\mathbf{s}$ is a simplex in $\mathcal{K}$ then so is every subset of $\mathbf{s}$.

A simplex $\mathbf{s}$ in $\mathcal{K}$ is called a *q-simplex* if $\mathrm{card}(\mathbf{s}) = q+1$ and say that $\mathbf{s}$ has *dimension* q. For a simplicial complex $\mathcal{K}$, we write $\dim(\mathcal{K}) := \sup\{q \mid \text{there exists a } q - \text{simplex in } \mathcal{K}\}$ and is called the *dimension of* $\mathcal{K}$. A simplicial complex of dimension ≤ 1 is called a *graph*.

An *edge* in $\mathcal{K}$ is an ordered pair (v_0, v_1) of vertices such that $\{v_0, v_1\}$ is a simplex in $\mathcal{K}$. If $\mathbf{e} = (v_0, v_1)$ is an edge in $\mathcal{K}$ the vertex v_0 (respectively v_1) is called the *origin* (respectively *end*) of $\mathbf{e}$ and usually denoted by $\mathrm{orig}(\mathbf{e})$ (respectively $\mathrm{end}(\mathbf{e})$).

A *path* α in $\mathcal{K}$ of length n is a sequence $\mathbf{e}_1\mathbf{e}_2\cdots\mathbf{e}_n$ of edges in K with $\mathrm{end}(\mathbf{e}_i) = \mathrm{orig}(\mathbf{e}_{i+1})$ for every $1 \leq i \leq n-1$. For a path $\alpha = \mathbf{e}_1\mathbf{e}_2\cdots\mathbf{e}_n$ we put $\mathrm{orig}(\alpha) = \mathrm{orig}(\mathbf{e}_1)$ and $\mathrm{end}(\alpha) := \mathrm{end}(\mathbf{e}_n)$ and say that α is a path from $\mathrm{orig}(\alpha)$ to $\mathrm{end}(\alpha)$.

A simplicial complex $\mathcal{K}$ is called *connected* if for every pair (v_0, v_1) of vertices in $\mathcal{K}$ there exists a path α in $\mathcal{K}$ such that $\mathrm{orig}(\alpha) = v_0$ and $\mathrm{end}(\alpha) = v_1$.

are projections of the K-vector space of the multilinear maps $V^I \to W$ onto the subspace of the alternating resp. the symmetric I-linear maps.

b). Suppose that $\operatorname{Char} K \neq 2$. The space of the bilinear maps $V \times V \to W$ is the direct sum of the subspace of the alternating (i.e. skew-symmetric) and the subspace the symmetric bilinear maps. The corresponding projections are $\frac{1}{2}A$ resp. $\frac{1}{2}S$. (**Remark:** A bilinear map $f : V \times V \to W$ can be decomposed into its skew-symmetric part $\frac{1}{2}Af$ and its symmetric part $\frac{1}{2}Sf$.)

14.4. Let K be a field and let V, W be vector spaces over K.

a). Let $f : V^n \to K$ be an alternating multilinear form on V and let $g : V \to W$ be a K-linear map. Then $(x_0, \ldots, x_n) \longmapsto \sum_{i=0}^n (-1)^i f(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)\, g(x_i)$ is an alternating K-multilinear map $V^{n+1} \to W$.

b). (Cramer's Formula) Suppose that V is a n-dimensional K-vector space. Then for every determinant function $\Delta : V^n \to K$ and for arbitrary $x_0, \ldots, x_n \in V$, prove that
$\sum_{i=0}^n (-1)^i \Delta(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots x_n)\, x_i = 0$. (**Hint:** Use the part a) above.)

On the other side one can see (simple) test-exercises; their solutions need not be submitted.

Test-Exercises

T14.1. **a).** Give an element of biggest posible order in the group $\mathfrak{S}_5$.

b). For $n \geq 4$, the group $\mathfrak{A}_n$ is not abelian.

T14.2. For the following permutations compute the number of variations and the sign.

a). The permutation $i \mapsto n - i + 1$ in $\mathfrak{S}_n$.

b). $\begin{pmatrix} 1 & 2 & \ldots & n & n+1 & \ldots & 2n \\ 1 & 3 & \ldots & 2n-1 & 2 & \ldots & 2n \end{pmatrix} \in \mathfrak{S}_{2n}$.

c). $\begin{pmatrix} 1 & 2 & \ldots & n & n+1 & \ldots & 2n \\ 2 & 4 & \ldots & 2n & 1 & \ldots & 2n-1 \end{pmatrix} \in \mathfrak{S}_{2n}$.

d). $\begin{pmatrix} 1 & \ldots & n-r+1 & n-r+2 & \ldots & n \\ r & \ldots & n & 1 & \ldots & r-1 \end{pmatrix} \in \mathfrak{S}_n,\ 1 \leq r \leq n$. (**Ans:** $(-1)^{(r-1)(n+1)}$.)

e). $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \ldots & 2n \\ 1 & 2n & 3 & 2(n-1) & 5 & 2(n-2) & \ldots & 2 \end{pmatrix} \in \mathfrak{S}_{2n}$.

f). For a subset $J \subseteq \{1, \ldots, n\}$ with $J = \{j_1, \ldots, j_m\}$, $j_1 < \cdots < j_m$, let σ_J be the permutation

$$\sigma_J = \begin{pmatrix} 1 & \ldots & m & m+1 & \ldots & n \\ j_1 & \ldots & j_m & i_1 & \ldots & i_{n-m} \end{pmatrix} \in \mathfrak{S}_n ,$$

where the numbers $i_1 < \cdots < i_{n-m}$ are the elements of the complement of J in $\{1, \ldots, n\}$. (**Hint:** The number of variations of σ_J is $F(\sigma_J) = \left(\sum_{k=1}^m j_k\right) - \binom{m+1}{2}$ and hence Sign $(\sigma_J) = (-1)^{F(\sigma_J)}$.)

g). Let σ resp. τ be permutations of the finite sets I resp. J. Compute the sign of the permutation $\sigma \times \tau : (i,\ j) \mapsto (\sigma\, i,\ \tau\, j)$ of $I \times J$ (in terms of Sign σ, Sign τ and $m := |I|,\ n := |J|$).

T14.3. Let $n \in \mathbb{N}^+$. Then

a). A subgroup of the permutation group $\mathfrak{S}_n$ which contain an odd permutation contains equal number of even and odd permutations.

b). A permutation $\sigma \in \mathfrak{S}_n$ which is of odd order is an even permutation.

c). The square σ^2 of a permutation $\sigma \in \mathfrak{S}_n$ is an even permutation.

d). Let $\sigma = \langle i_0, \ldots, i_{k-1} \rangle$ be a cycle of length $k \geq 2$. What is the inverse of σ ? For which $m \in \mathbb{Z}$, σ^m is a cycle of length k ?

e). Let $\sigma \in \mathfrak{S}_n$ and $m \in \mathbb{Z}$. Every orbit of σ of length k decomposes into ggT (k, m) orbits of the length $k/$ ggT (k, m) of σ^m.

f). Let I be a finite set. The inverse σ^{-1} of a permutation $\sigma \in \mathfrak{S}(I)$ has the same orbits and same sign as those of σ.

g). Let $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the canonical prime factorisation of $m \in \mathbb{N}^*$. Then the permutation group $\mathfrak{S}_n$ contain an element of order m if and only if $n \geq p_1^{\alpha_1} + \cdots + p_r^{\alpha_r}$. For which $n \in \mathbb{N}$ there exists an element of order 3000 (resp. 3001) in the group $\mathfrak{S}_n$?

T14.4. **a).** If $\sigma \in \mathfrak{S}_n$, $n \in \mathbb{N}^+$ has s orbits, then σ can be represented as a product of $n-s$ transpositions and cannot be represented as a product of less than $n - s$ transpositions.

b). Let $\sigma \in \mathfrak{S}_n$, $n \in \mathbb{N}^+$ be a permutation of type $(\nu_1, \ldots, \nu_n)$. Then the number of permuations in $\mathfrak{S}_n$ which commute with σ is $\nu_1! \cdots \nu_n!\, 1^{\nu_1} \cdots n^{\nu_n}$. (**Hint:** These permutations form the centraliser $\mathrm{C}_{\mathfrak{S}_n}(\sigma)$ of σ.)

T14.5. **a).** The cycles $\langle 1, 2 \rangle$, $\langle 2, \ldots, n \rangle$ generate the group $\mathfrak{S}_n$, $n \geq 2$. (**Hint:** Use 14.1-d))

b). The cycles $\langle 1, 2 \rangle$, $\langle 1, 2, \ldots, n \rangle$ generate the group $\mathfrak{S}_n$, $n \geq 2$. (**Hint:** Use 14.1-d))

c). $\langle 1, n \rangle$, $\langle 1, \ldots, n \rangle$ generate the group $\mathfrak{S}_n$, $n \geq 2$. (**Hint:** Use 14.1-d))

T14.6. Let $n \in \mathbb{N}^+$.

a). For $n \geq 2$, Sign : $\mathfrak{S}_n \to \{-1, 1\}$ is the only non-trivial group homomorphism. (**Hint:** $\langle a\, b \rangle$ and $\langle c\, d \rangle$ be two transpositions $\mathfrak{S}_n$. If $\sigma \in \mathfrak{S}_n$ be an arbitrary permutation with $a \mapsto c$, $b \mapsto d$, then $\sigma\langle a\,b\rangle\sigma^{-1} = \langle c\,d\rangle$ and so every homomorphism $\varphi : \mathfrak{S}_n \to \{1, -1\}$ have the same value on all transpositions. If this value is 1, then φ; if it si -1, then $\varphi = \text{Sign}$.)

b). $\mathfrak{A}_n$ is the commutator $\mathfrak{S}_n$.

c). Using the simplicity of the group $\mathfrak{A}_n$, $n \geq 5$, prove that the group $\mathfrak{A}_n$ is the only non-trivial normal subgroup in the group $\mathfrak{S}_n$ for $n \geq 5$.

d). The groups $\mathfrak{A}_4$ and $\mathfrak{V}_4$ are the only non-trivial normal subgroups in $\mathfrak{S}_4$.

e). The group $\mathfrak{V}_4$ is the only non-trivial normal subgroup in $\mathfrak{A}_4$.

T14.7. Let I be a finite set and let $\sigma \in \mathfrak{S}(I)$ be a permutation of I of prime power order p^m, p prime. Then the number of fixed points of σ and the number of $n := |I|$ of elements of I are congruent modulo p. In particular,
(1) If n is not divisible by p, then σ has at least one fixed point.
(2) If n is divisible by p, then the number of fixed points of σ is also divisible by p. (**Remark :** This is a special case of the assertion ???)

T14.8. Let G be a finite group of order n and let $\lambda : G \to \mathfrak{S}(G)$ be the corresponding Cayley's homomorphism.

a). For every $g \in G$, the permutation λ_g has exactly $n/\text{ord}\, g$ orbits of lengths $\text{ord}\, g$. In particular, $\text{Sign}\,\lambda_g = (-1)^{n-(n/\text{ord}\, g)} = (-1)^{[G:\text{H}(g)]+|G|}$, where $\text{H}(g)$ is the cyclic subgroup of G generated by g.

b). If $G := \mathfrak{S}_n$ and $n \geq 4$, then $\lambda(G) = \lambda(\mathfrak{S}_n) \subseteq \mathfrak{A}(\mathfrak{S}_n)$. (**Hint :** Compute $\text{Sign}(\lambda_\tau)$, where $\tau \in \mathfrak{S}_n$ is a transposition.)

c). $\lambda(G) \not\subseteq \mathfrak{A}(G)$ if and only if n is even and G has an element of order 2^α, where 2^α is the biggest power of 2 which divide n. (i.e. if and only if the 2–Sylow subgroup of G is cyclic and is non-trivial). Moreover, in this case G has a normal subgroup of index 2.

d). If $|G| = 2m$, m is odd, then G has a normal subgroup of index 2. (**Hint :** G has an element g of order 2. Compute the $\text{Sign}(\lambda_g)$.)

e). The order of a finite simple non-abelian group is divisible by 4. (**Hint :** Use d) and the theorem of F e i t – T h o m p s o n *Every finite non-abelian simple group has even order*. The proof of this theorem is not easy. See [**Feit, W. and Thompson, J. :** Solvability of groups of odd order, *Pacific Journal of Mathematics*, pp-775-1029, (1963).])

T14.9. Every finite subgroup is isomorphic to a subgroup of an alternating group $\mathfrak{A}_m$. (**Hint :** Use ??-b) or the following remark : For $n \in \mathbb{N}$, let f be the bijection $i \mapsto n + i$ of $\{1, \ldots, n\}$ onto $\{n + 1, \ldots, 2n\}$. The map $\sigma \mapsto \sigma'$, which maps every permutation $\sigma \in \mathfrak{S}_n$ to the permutation $\sigma' \in \mathfrak{S}_{2n}$ where $\sigma' = \sigma$ on $\{1, \ldots, n\}$ and $\sigma' = f\sigma f^{-1}$ on $\{n + 1, \ldots, 2n\}$, is a homomorphism from $\mathfrak{S}_n$ into $\mathfrak{A}_{2n}$.)

T14.10. a). Compute the class number of the group $\mathfrak{S}_n$ for $n \leq 6$. (**Hint :** Use 44.9.)

b). For $n \geq 3$, the center $\text{Z}(\mathfrak{S}_n) = \{\text{id}\}$. (**Hint :** For $\sigma \in \mathfrak{S}_n$, $n \geq 3$, $\sigma \neq \text{id}$, find a transposition $\langle ab\rangle$ with $\sigma\langle ab\rangle\sigma^{-1} = \langle\sigma(a)\sigma(b)\rangle \neq \langle ab\rangle$.)

T14.11. Let G be a subgroup of $\mathfrak{S}_n$, $n \geq 2$. Suppose that the natural operation of G on $\{1, \ldots, n\}$ is transitive.

a). If G contain a transposition and a cycle of order $n - 1$, then $G = \mathfrak{S}_n$. (**Hint :** Use T14.5-a).)

b). If G contain a transposition and a cycle of prime order p with $\frac{n}{2} < p < n$, then $G = \mathfrak{S}_n$.

T14.12. Let p be a prime number.

a). If the subgroup G of $\mathfrak{S}_p$ contain a transposition and if p divides the order of G, then $G = \mathfrak{S}_p$. (**Hint :** G contain an element of order p. This must be a cycle. Now use T14.5-c). — **Remark :** Show that the condition "$p \mid |G|$" is equivalent with "the natural opeartion of G on $\{1, \ldots, p\}$ is transitive".)

b). Let G be the subgroup of $\mathfrak{S}_{p+1}$. Suppose that G has the following properties:
(1) The natural opeartion of G on $\{1, \ldots, p + 1\}$ is transitive.
(2) p divides the order of G.
(3) G contains a transposition.
Then $G = \mathfrak{S}_{p+1}$. (**Hint :** Use T14.11-a).)

T14.13. The quaternion group Q can be embedded in the group $\mathfrak{S}_n$, $n \in \mathbb{N}$, if and only if $n \geq 8$. (**Hint:** Study the elements of the order 4.)

T14.14. Let V and W be K-vector spaces, I be a finite indexed set and $f : V^I \to W$ be a multilineare map. Let $g : U \to V$ and $h : W \to X$ be K-vector space homomorphisms. Then $h \circ f \circ g^I : U^I \to X$ is a multilineare map, where g^I is defined by $g^I\big((u_i)\big) := \big(g(u_i)\big)$, $(u_i) \in U^I$. If f is symmetric resp. skew-symmetric resp. alternating, then so is $h \circ f \circ g^I$.

T14.15. (Functoriality) Let V', V, V'', W', W, W'' be K-vector spaces and I be a finite indexed set. Let $f' : V' \to V$, $f : V \to V''$, $g' : W' \to W$ and $g : W \to W''$ be K-linear maps. Then

a). The map $\mathrm{Mult}_K(I, f'; W) : \mathrm{Mult}_K(I, V, W) \to \mathrm{Mult}_K(I, V', W)$ defined by $\Phi \mapsto \Phi \circ f'^I$ is K-linear. Moreover, $\mathrm{Mult}_K(I, \mathrm{id}_V; W) = \mathrm{id}_{\mathrm{Mult}_K(I,V;W)}$ and $\mathrm{Mult}_K(I, f'' \circ f'; W) = \mathrm{Mult}_K(I, f'; W) \circ \mathrm{Mult}_K(I, f''; W)$.

b). The map $\mathrm{Mult}_K(I, V; g') : \mathrm{Mult}_K(I, V, W') \to \mathrm{Mult}_K(I, V, W)$ defined by $\Phi \mapsto g' \circ \Phi$ is K-linear. Moreover, $\mathrm{Mult}_K(I, V; \mathrm{id}_W) = \mathrm{id}_{\mathrm{Mult}_K(I,V;W)}$ and $\mathrm{Mult}_K(I, V; g \circ g') = \mathrm{Mult}_K(I, V; g) \circ \mathrm{Mult}_K(I, V; g')$.

c). The map $\mathrm{Alt}_K(I, f'; W) : \mathrm{Alt}_K(I, V, W) \to \mathrm{Alt}_K(I, V', W)$ defined by $\Phi \mapsto \Phi \circ f'^I$ is K-linear. Moreover, $\mathrm{Alt}_K(I, \mathrm{id}_V; W) = \mathrm{id}_{\mathrm{Alt}_K(I,V;W)}$ and $\mathrm{Alt}_K(I, f'' \circ f'; W) = \mathrm{Alt}_K(I, f'; W) \circ \mathrm{Alt}_K(I, f''; W)$.

d). The map $\mathrm{Alt}_K(I, V; g') : \mathrm{Alt}_K(I, V, W') \to \mathrm{Alt}_K(I, V, W)$ defined by $\Phi \mapsto g' \circ \Phi$ is K-linear. Moreover, $\mathrm{Alt}_K(I, V; \mathrm{id}_W) = \mathrm{id}_{\mathrm{Alt}_K(I,V;W)}$ and $\mathrm{Alt}_K(I, V; g \circ g') = \mathrm{Alt}_K(I, V; g) \circ \mathrm{Alt}_K(I, V; g')$.

(**Remark:** This mean that the part a) and c) (resp. b) and d)) for a fixed K-vector space W (resp. V) the assignment $V \mapsto \mathrm{Mult}_K(I, V; W)$ and $V \mapsto \mathrm{Alt}_K(I, V; W)$ (resp. $W \mapsto \mathrm{Mult}_K(I, V; W)$ and $W \mapsto \mathrm{Alt}_K(I, V; W)$) are *contravariant* and *covariant* functors from the *category* $\mathcal{V}_K$ of K-vector spaces to itself, respectively.)—In particular, the assignment $V \mapsto \mathrm{Alt}_K(I, V)$ is a *contravariant functor* from the *category* $\mathcal{V}_K$ of K-vector spaces to itself.)

T14.16. Let A be a commutative ring, V be an A–module, I, $J := I \cup \{k\}$ be finite index sets with $k \notin I$ and let $\Phi \in \mathrm{Alt}_A(I, V; A)$. Then the map

$$\Phi' : V^J \to V \quad \text{defined by} \quad (v_i)_{i\in J} \mapsto \Phi((v_i)_{i\in I})v_k$$

is multi-linear, i.e. $\Phi' \in \mathrm{Mult}_A(J, V; V)$ and the map $\Phi'' := \Phi' - \sum_{i\in I} \langle ik\rangle \Phi'$ is alternating, i.e. $\Phi'' \in \mathrm{Alt}_A(J, V; V)$. (**Remark:** The map Φ'' is obtained from Φ' by the process similar to that of anti-symmetrisation by using the transpositions $\langle ik\rangle \in \mathfrak{S}(J)$; the factor -1 appears in the sum as a common Sign of the transpositions $\langle ik\rangle$. — Note the formula for Φ'' in the specail case $I = \{1, \ldots, n\}$, $J = \{1, \ldots, n, n+1\}$.)

T14.17. (Determinants over a commutative ring) Let A be a commutative ring.

a). Let V be a finite free A–module with a basis x_i, $i \in I$. Then the map $\varphi : \mathrm{Alt}_A(I, V) \cong A$ defined by . $\Phi \mapsto \Phi((x_i)_{i\in I})$ is an A–isomorphism.

b). Let V and W be arbitrary modules over A and let $f : V \to W$ be an A–linear map. Then for every finite indexed set I, f induces a natural A–linear map

$$\mathrm{Alt}_A(I, f) = \mathrm{Alt}(I, f) : \mathrm{Alt}_A(I, W) \to \mathrm{Alt}_A(I, V)$$

defined by $\Phi \mapsto \Phi \circ f^I$, where the map $f^I : V^I \to W^I$, is defined by $(v_i) \mapsto (f(v_i))$. Moreover, if $g : W \to X$ is another A–linear map of A–modules, then

$$\mathrm{Alt}(I, gf) = \mathrm{Alt}(I, f) \circ \mathrm{Alt}(I, g),$$

c). Let V be a free A–module of finite rank n and I be an indexed set with n elements. Then $\mathrm{Alt}(I, f)$ is an endomorphism of $\mathrm{Alt}(I, V) \cong A$ and hence $\mathrm{Alt}(I, f)$ is the multiplication by a uniquely determined element $a \in A$, and so is a homothecy ϑ_a. *The element $a \in A$ with $\mathrm{Alt}(I, f) = \vartheta_a$ is independent of the choice of the indexed set I.* (**Proof:** Let J be another set with n elements and $\mathrm{Alt}(J, f) = \vartheta_b$. there exists a bijection $\varkappa : I \to J$. Then $(v_j)_{j\in J} \mapsto (v_{\varkappa i})_{i\in I}$ is an A–isomorphism $\eta : V^J \to V^I$ and hence $\Phi \mapsto \Phi\eta$ is a bijection from $\mathrm{Alt}(I, V)$ onto $\mathrm{Alt}(J, V)$. For an arbitrary $\Phi \in \mathrm{Alt}(I, V)$ we have :

$$\begin{aligned} a\cdot(\Phi\eta) &= (a\Phi)\eta = (\mathrm{Alt}(I, f)\,\Phi)\eta = (\Phi f^I)\eta = \Phi(f^I\eta) = \Phi(\eta f^J) \\ &= (\Phi\eta) f^J = \mathrm{Alt}(J, f)\,(\Phi\eta) = b\cdot(\Phi\eta)\,. \end{aligned}$$

and hence $a = b$.)

d). Let V be a finite free A–module with a basis consisting of n elements and let $f \in \mathrm{End}_A V$. Then the uniquely determined element $a \in A$ with $\mathrm{Alt}(n, f) = \vartheta_a$ is called the d e t e r m i n a n t of f (over A) and is denoted by $\mathrm{Det}\, f$. The d e t e r m i n a n t m a p $f \mapsto \mathrm{Det}\, f$ ide denoted by $\mathrm{Det} : \mathrm{End}_A V \to A$. (**Remark :** In the definition of determinant instead of the standard indexed set $\{1, \dots, n\}$, we may choose any other indexed set I with n elements (see part c). For a finite free A–module V of rank n the elements of $\mathrm{Alt}(n, V)$ are also called d e t e r m i n a n t f u n c t i o n s (on V or on V^n.)

e). Let V be a finite free A–module with basis $x_i,\ i \in I$ and let $f \in \mathrm{End}_A V$.

(1) For every I-linear form $\Phi \in \mathrm{Alt}_A(I, V)$ and for every I–tuple $(v_i) \in V^I$:

$$\Phi((f(v_i))_{i\in I}) = (\mathrm{Alt}(I, f)\Phi)((v_i)_{i\in I}) = \mathrm{Det}\, f \cdot \Phi((v_i)_{i\in I})\,.$$

(2) For an alternating I-linear form Δ on V^I with $\Delta((x_i)_{i\in I}) = 1$: $\mathrm{Det}\, f = \Delta((f(x_i))_{i\in I})$.
(**Proof :** By part a) Δ is a basis of $\mathrm{Alt}_A(I, V)$ and by definition $\mathrm{Alt}(I, f)(\Delta) = (\mathrm{Det}\, f)\cdot\Delta$. Taking the image of $(x_i)_{i\in I} \in V^I$ on both sides, we get $\Delta((f(x_i))_{i\in I}) = \mathrm{Det}\, f \cdot \Delta((x_i)_{i\in I}) = \mathrm{Det}\, f$.)

f). Let V be a finite free A–module with a basis consisting n elements. Then the determinant map

$$\mathrm{Det} : \mathrm{End}_A V \to A$$

have the following properties:

(1) $\mathrm{Det}(\mathrm{id}_V) = 1$.
(2) $\mathrm{Det}(fg) = (\mathrm{Det}\, f)(\mathrm{Det}\, g)$ for all $f, g \in \mathrm{End}_A V$.
(3) $\mathrm{Det}(af) = a^n \mathrm{Det}\, f$ for all $a \in A$ and all $f \in \mathrm{End}_A V$.

T14.18. Let A be a commutative ring and let V be a finite free A–module and $f \in \mathrm{End}_A V$. Show that : There exists a $g \in \mathrm{End}_A V$ such that $(\mathrm{Det}\, f)\cdot \mathrm{id}_V = fg = gf$. (**Hint :** Let $x_1, \dots, x_n$ be a basis of V, $\Delta \in \mathrm{Aut}_A(n, V)$ be such that $\Delta(x_1, \dots, x_n) = 1$ and $\Phi = \mathrm{Alt}(n, f)(\Delta) = \mathrm{Det}\, f \cdot \Delta$. Let $g_i,\ i = 1, \dots, n$ be the linear form on V defined by $v \mapsto \Delta(f(x_1), \dots, f(x_{i-1}), v, f(x_{i+1}), \dots, f(x_n))$ and let $g : V \to V$ be the map defined by $v \mapsto \sum_{i=1}^n g_i(v)x_i$. The equation $gf = (\mathrm{Det}\, f)\cdot \mathrm{id}_V$ can be verified directly from definitions. For the proof of $fg = (\mathrm{Det}\, f)\cdot\mathrm{id}_V$ apply the exercise T14.16 to Φ and construct $(n + 1)$–linear map $\Phi' : (v_1, \dots, v_n, v_{n+1}) \mapsto \Phi(v_1, \dots, v_n)v_{n+1} = \Delta(f(v_1), \dots, f(v_n))v_{n+1}$ and hence the alternating $(n + 1)$–linear map $\Phi'' : V^{n+1} \to V$ is the zero map. Deduce that : $(\mathrm{Det}\, f)V \subseteq \mathrm{im}\, f$. Further, this shows that $\mathrm{Det}\, f$ is a unit in A if and only if f is bijective. If $\mathrm{Det}\, f$ is a non-zero divisor in A, then f injective.

T14.19. *Let A be a commutative ring and let V be a non-zero finite free A–module. The determinant map* $\mathrm{Det} : \mathrm{End}_A V \to A$ *is a surjective monoid homomorphism of the multiplicative monoid of* $\mathrm{End}_A V$ *onto the multiplicative monoid of A. Further, it maps the unit group* $(\mathrm{End}_A V)^\times = \mathrm{Aut}_A V$ *onto the unit group* $A^\times$ *and* $\mathrm{Det}^{-1}(A^\times) = \mathrm{Aut}_A V$. *This mean that* : *an operator* $f \in \mathrm{End}_A V$ *is an automorphism if and only if* $\mathrm{Det}\, f$ *is a unit in A.* (**Proof :** It follows from T14.17(1) and (2) that Det is a homomorphism. Further, by the commutativity of A we have

$$\mathrm{Det}(fg) = (\mathrm{Det}\, f)(\mathrm{Det}\, g) = (\mathrm{Det}\, g)(\mathrm{Det}\, f) = \mathrm{Det}(gf)\,.$$

By restricting we get a group homomorphism $\mathrm{Det} : \mathrm{Aut}_A V \to A^\times$. In particular, we have

$$\mathrm{Det}(f^{-1}) = (\mathrm{Det}\, f)^{-1}$$

for $f \in \mathrm{Aut}_A V$. The surjectivity of Det follows easily : Let $a \in A$ be given and let $x_1, \dots, x_n$ be a basis von V. Then $n \geq 1$. For the endomorphism f_1 with $x \mapsto ax_1$ and $x_i \mapsto x_i$ for $i \geq 2$, the determinant $\mathrm{Det}\, f_1 = \Delta(ax_1, x_2, \dots, x_n) = a\Delta(x_1, \dots, x_n) = a$, where Δ is a basis element of $\mathrm{Alt}_A(n, V)$ with $\Delta(x_1, \dots, x_n) = 1$. If $a \in A^\times$, then $f_1 \in \mathrm{Aut}_A V$, this also proves the surjectivity of the restriction $\mathrm{Det} : \mathrm{Aut}_A V \to A^\times$. Now, it remains to prove that : If $\mathrm{Det}\, f$ is a unit in A, then f is an automorphism.

The proof of this asserrtion is not that easy One has to use either the expansion of the determinants or one can also give a direct proof using T14.18. *We also note here the simple proof in the special case when A is a field, i.e. in the case when V is a vector space:* We use the ir benutzen eine Basis $x_1, \ldots, x_n$ von V and the alternating n–linear form Δ on V^n with $\Delta(x_1, \ldots, x_n) = 1$. Then $\operatorname{Det} f = \Delta(f(x_1), \ldots, f(x_n))$. By hypothesis $\operatorname{Det} f \neq 0$. Then the vectors $f(x_1), \ldots, f(x_n)$ are linearly independent and so f is an isomorphism.)

T14.20. Let A, V and x_i, $i \in I$ be as in T14.17-a). For every A–module W, the map $\Phi \mapsto \Phi((x_i)_{i\in I})$ defines an isomorphism $\operatorname{Alt}(I, V; W) \to W$.

T14.21. Let $x_1, \ldots, x_n$ be a basis of the free module V over a commutative ring A. For a subset $H \subseteq \{1, \ldots, n\}$, $H = \{i_1, \ldots, i_r\}$, $i_1 < \cdots < i_r$, let x_H denote the r–tuple $(x_{i_1}, \ldots x_{i_r}) \in V^r$. Then for every $r \in \mathbb{N}$, the map

$$\Phi \mapsto (\Phi(x_H))_{|H|=r}$$

defines an A–isomorphism $\operatorname{Alt}(r, V) \to A^{\mathfrak{P}_r(n)}$, where $\mathfrak{P}_r(n)$ is the set of subsets of $\{1, \ldots, n\}$ of cardinality r. In particular, $\operatorname{Alt}(r, V)$ is a free module of rank $\binom{n}{r}$. (**Hint:** The standardbasis–element e_H, H as above, of $A^{\mathfrak{P}_r(n)}$ define an r-alternating function $\Delta_H := \operatorname{Alt}(r, \pi_H)(\Delta'_H)$, where $\pi_H : V \to V_H := \sum_{i\in H} Ax_i$ is the projection with $x_i \mapsto x_i$, if $i \in H$, and $x_i \mapsto 0$, if $i \notin H$ and $\Delta'_H : V_H^r \to A$ is the determinant function with $\Delta'_H(x_{i_1}, \ldots, x_{i_r}) = 1$, see T14.17-a).)

T14.22. Let $m, n \in \mathbb{N}$ and $m \le n$. For arbitrary matrices $\mathfrak{A} = (a_{ij}) \in \mathrm{M}_{m,n}(A)$ and $\mathfrak{B} = (b_{ji}) \in \mathrm{M}_{n,m}(A)$ over a commutative ring A :

$$\operatorname{Det}(\mathfrak{A}\mathfrak{B}) = \sum_{1\le j_1<\cdots<j_m\le n} \begin{vmatrix} a_{1j_1} & \cdots & a_{1j_m} \\ \vdots & \ddots & \vdots \\ a_{mj_1} & \cdots & a_{mj_m} \end{vmatrix} \begin{vmatrix} b_{j_11} & \cdots & b_{j_1m} \\ \vdots & \ddots & \vdots \\ b_{j_m1} & \cdots & b_{j_mm} \end{vmatrix} .$$

(**Hint:** Let $f : A^n \to A^m$ and $g : A^m \to A^n$ be the A–linear maps with the matrices $\mathfrak{A}$ resp. $\mathfrak{B}$ with respect to the standard bases. Then compute the composition $\operatorname{Alt}(m, fg) = \operatorname{Alt}(m, g) \circ \operatorname{Alt}(m, f)$ by using the basis Δ_H, $H \in \mathfrak{P}_m(n)$ of $\operatorname{Alt}(m, A^n)$ see the exercise T14.21, where $x_1, \ldots, x_n$ is the standard basis of A^n.)

T14.23. Let A be a non-zero commutative ring and let V, W be finite free A–modules with bases $x_1, \ldots, x_n$ resp. $y_1, \ldots, y_m$. Further, let $f : V \to W$ be an A–homomorphism with the matrix $\mathfrak{A} = (a_{ij}) \in \mathrm{M}_{m,n}(A)$ with respect to the given bases. Then

a). Coker f is annihilated by all minors of $\mathfrak{A}$ of order m. – In particular, if $W = V$, then $\operatorname{Det} f) \cdot \operatorname{Ker} f = 0$ and $\operatorname{Det} f) \cdot \operatorname{Coker} f = 0$.

b). The following statements are equivalent:

(1) f is surjective. (2) The minors of $\mathfrak{A}$ of order m generate the unit-ideal in A. (**Hint:** For (1) $\Rightarrow$ (2) consider a homomorphism $g : W \to V$ with $fg = \mathrm{id}_W$ and the matrix $\mathfrak{B}$. From $\mathfrak{A}\mathfrak{B} = \mathfrak{E}_m$ and the exercise T14.22 the assertion (2) follows. For (2) $\Rightarrow$ (1) use the part a).)

T14.24. Let A be a non-zero commutative ring and let V be a finite free A–module with a basis consisting of n elements, $n \ge 2$. Then the determinant map $\operatorname{Det} : \operatorname{End}_A V \to A$ is not additive.

T14.25. Let A be a commutative ring and let V be an A–module. Suppose that $\mathfrak{A} = (a_{ij}) \in \mathrm{M}_n(A)$ and the elements $x_1, \ldots, x_n$ of V satisfy the equations

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \\ \cdots\cdots\cdots\cdots&\cdots\cdots . \\ a_{n1}x_1 + \cdots + a_{nn}x_n &= 0 \end{aligned}$$

Then $(\operatorname{Det}\mathfrak{A})x_j = 0$ for every $j = 1, \ldots, n$. (**Hint:** Use the Cramer's rule.)

T14.26. (Dedekind's lemma) *Let V be a finitely gebnerated module over a commutative ring A and let $\mathfrak{a} \subseteq A$ be an ideal in A. Suppose that $V = \mathfrak{a}V$. Then there exists an element $a \in \mathfrak{a}$ such that $(1 - a)V = 0$.* (**Proof:** Let $x_1, \ldots, x_n$ be a generating system for V. Since $x_i \in \mathfrak{a}V$, there exist elements $a_{ij} \in \mathfrak{a}$ such that $x_i = \sum_{j=1}^{n} a_{ij} x_j$, i.e. $\sum_{j=1}^{n} (\delta_{ij} - a_{ij}) x_j = 0$. From T14.22 it follows that $\mathrm{Det}(\mathfrak{E} - \mathfrak{A}) x_j = 0,\ j = 1, \ldots, n$, i.e. $\mathrm{Det}(\mathfrak{E} - \mathfrak{A}) \cdot V = 0$, weher $\mathfrak{A} := (a_{ij})$. The matrix $\mathfrak{E} - \mathfrak{A}$ is the unit matrix modulo $\mathfrak{a}$, we have $\mathrm{Det}(\mathfrak{E} - \mathfrak{A}) \equiv \mathrm{Det}\, \mathfrak{E} = 1$ modulo $\mathfrak{a}$. and so $\mathrm{Det}(\mathfrak{E} - \mathfrak{A}) = 1 - a$ with an element $a \in \mathfrak{a}$.)

T14.27. *If f is a surjective endomorphism of a finitely generated module V over a commutative ring A, then f is an automorphismus.* (**Proof:** We consider V as a module over the commutative subalgebra $A[f]$ of $\mathrm{End}_A V$ generated by f, where $fx := f(x)$ for $x \in V$. Then the surjectivity of f mean $V = fV$. The Dedekind's Lemma assures the existence of an endomorphism $gf \in A[f] \cdot f,\ g \in A[f]$ such that $(1 - gf)V = 0$. This mean : $(1 - gf)x = 0$ or $x = gfx = g(f(x))$ for all $x \in V$, i.e. $gf = \mathrm{id}_V$. Since $g \in A[f]$, we have $fg = gf$ and so f is invertible and $g = f^{-1}$. — This proof show more : *Under the above hypothesis the inverse f^{-1} belong to $A[f]$ and hence is a polynomial f over A.*)