ALGEBRA 7: matrices and determinants

We suppose that all vector spaces are vector spaces over a field $k$.

**Exercise 7.1.** Let $v_1, \ldots, v_n \in V$, $w_1, \ldots, w_m \in W$ be bases in vector spaces $V$ and $W$. Consider a homomorphism $e_i^j$ from $V$ to $W$ that maps $v_i$ to $w_j$ and maps $v_k$ to zero for $k \neq i$. Prove that $e_i^j$ form a basis in the space of homomorphisms Hom($V, W$).

**Definition 7.1.** In the previous problem setting consider a homomorphism $\gamma \in \text{Hom}(V, W)$. Consider $\gamma = \gamma_i^j e_i^j$, $\gamma_i^j \in k$. The matrix
\[
\begin{pmatrix}
\gamma_1^1 & \cdots & \gamma_1^m \\
\vdots & \ddots & \vdots \\
\gamma_m^1 & \cdots & \gamma_m^m
\end{pmatrix}
\]
is called the **matrix of the homomorphism** $\gamma$.

**Exercise 7.2.** Consider homomorphisms $a \in \text{Hom}(U, V)$, $b \in \text{Hom}(V, W)$ defined by the matrices $(a_i^j)$, $(b_k^l)$. Prove that the composition of $a$ and $b$ is defined by the matrix $c_i^k = \sum_j a_i^j b_j^k$.

**Remark.** Note that the matrix product formula makes sense for matrices of elements of an arbitrary ring.

**Exercise 7.3.** Consider the space $A$ of square matrices of the size $n \times n$, with the multiplication $A \times A \rightarrow A$ defined by the formula $(a_i^j) \circ (b_k^l) \rightarrow \sum_j a_i^j b_j^k$. Prove that this is an algebra with unit. Prove that this algebra is isomorphic to the algebra of linear operators from $k^n$ to $k^n$.

**Definition 7.2.** This algebra is called the **matrix algebra** and is denoted Mat($n$). The unit element of this algebra (the diagonal matrix with $a_{ii} = 1$) is called the **identity matrix** and is denoted $\text{Id}$.

**Exercise 7.4.** Consider a linear operator $f \in \text{Hom}(V, V)$ and let $v_1, \ldots, v_n$ be a basis of $V$ and $(f_i^j)$ be the matrix of $f$. Consider another basis $v'_1, \ldots, v'_n$ of $V$. Prove that there exists a unique operator $g$ that maps $v_i$ to $v'_i$, and $g$ is invertible. Let $(g_i^j)$, $((g^{-1})_i^j)$ be the matrices of $g$ and $g^{-1}$. Prove that $f$ is defined by the matrix $h_i^j := (g_i^j) \circ (f_i^j) \circ ((g^{-1})_i^j)$ in the basis $v'_1, \ldots, v'_n$.

**Definition 7.3.** In that case the matrices $(h_i^j)$, $(f_i^j)$ are said to be **equivalent**.

**Exercise 7.5.** Find all the matrices equivalent to $c \text{Id}$ where $c \in k$.

**Exercise 7.6 (!).** Consider a matrix $E(i, j)$
\[
\begin{pmatrix}
0 & \cdots & 0 & \cdots & 0 \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
0 & \cdots & 1 & \cdots & 0 \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
0 & \cdots & 0 & \cdots & 0
\end{pmatrix},
\]
which has 1 on the position $i, j$ and has 0 everywhere else. What are the values of $i, j, i', j'$ that make the matrices $E(i, j)$ and $E(i', j')$ equivalent?

**Exercise 7.7 (!).** Consider a matrix $A$ which is equivalent to $E(i, j)$. Prove that all rows of $A$ are proportional. Prove that all columns of $A$ are proportional.
Exercise 7.8 (*). Prove that if all rows and columns of $A$ are proportional, then $A$ is equivalent to $E(i,j)$.

Definition 7.4. Consider a vector space $V$ and an endomorphism $A \in \text{End}(V)$ over it (i.e. a homomorphism from $V$ to itself) and its dual space $V^*$. An operator $A^*: V^* \longrightarrow V^*$ that maps a linear functional $\gamma \in V^*$ to the linear functional $A^*(\gamma)(v) = \gamma(A(v))$ is called a conjugate operator for $A$.

Exercise 7.9. Consider a finite-dimensional vector space $V$ and its dual space $V^*$. Construct the natural isomorphism between $\Lambda^k(V)^*$ and $\Lambda^k(V^*)$.

Remark. “Natural” means that it does not require any extra choice (choice of base, for example). In this situation, a natural isomorphism $\Lambda^k(V)^* \cong \Lambda^k(V^*)$ is permutable with the standard action of $GL(V)$ on $\Lambda^k(V)^*$, $\Lambda^k(V^*)$. The spaces $V$ and $V^*$ are isomorphic, but one can prove that there is no $GL(V)$-invariant isomorphism $V \cong V^*$. In other words it is impossible to construct a natural homomorphism $V \cong V^*$.

Exercise 7.10 (!). Consider a vector space $V$, an endomorphism $A \in \text{End}(V)$ and the conjugate operator $A^*$. Prove that $\det A^* = \det A$.

Hint. Use the previous problem.

Definition 7.5. Consider a square matrix $(A^i_j)$ and a matrix $(B^i_j)$, that is constructed from $(A^i_j)$ by reflecting it over the diagonal: $B^j_i = A^i_j$. Then $(B^j_i)$ is called the transposed matrix of $(A^i_j)$, and is denoted $(A^i_j)^\perp$.

Exercise 7.11 (!). Consider a basis $v_1, \ldots, v_n$ in $V$ and a dual basis $v^1, \ldots, v^n$ in $V^*$ ($v^i$ maps $v_i$ to 1 and maps other $v_j$s to zero). Consider an operator $A \in \text{End}(V)$ and its matrix $(A^i_j)$. Prove that $A^*$ is given as the matrix $(A^i_j)^\perp$.

Definition 7.6. Consider a nondegenerate bilinear symmetric form $g$ defined on a vector space $V$. An operator $A \in \text{End}(V)$ is called orthogonal with respect to $g$ (or simply orthogonal) iff $g(Av, Av) = g(v, v)$ for any $v \in V$.

Exercise 7.12 (!). Prove that any orthogonal operator is invertible.

Exercise 7.13 (!). Consider a linear operator $A \in \text{End}(V)$ on a vector space endowed with a nondegenerate bilinear symmetric form $g$. Identify $V$ and $V^*$ using $g$. Then the dual operator $A^*$ can be considered as an endomorphism of $V$. Prove that a linear operator $A$ is orthogonal iff $A^{-1} = A^*$.

Exercise 7.14 (!). Prove that the determinant of an orthogonal operator equals $\pm 1$.

Definition 7.7. A nondegenerate bilinear antisymmetric form (see ALGEBRA 3) is called a symplectic form.

Exercise 7.15 (*). Consider a vector space $V$ with a symplectic form $\omega$ defined on it. An operator $A \in \text{End}(V)$ is called symplectic, if it preserves $\omega$, i.e. if $\omega(Av, Av) = \omega(v, v)$. Prove that any symplectic operator has the determinant 1.
Exercise 7.16 (!). Consider a two-dimensional vector space \( V \) over \( \mathbb{R} \) and let \( A \) be the matrix
\[
\begin{pmatrix}
a & b \\
c & d
\end{pmatrix}.
\]
Consider the matrix
\[
A' = \begin{pmatrix}
d & b \\
-c & a
\end{pmatrix}.
\]
Prove that \( AA' = \Delta \text{Id} \), where \( \Delta \in k \) is the number \( ad - bc \). Prove that \( A \) is invertible iff \( \Delta \neq 0 \).

Exercise 7.17 (!). In the previous problem setting prove that \( \Delta \) equals to \( A \) determinant .

Exercise 7.18. Consider a two-dimensional vector space \( V \) over \( \mathbb{R} \) endowed with a positive bilinear symmetric form. Let \( A \) be an orthogonal operator and its matrix in an orthonormal basis has a form
\[
\begin{pmatrix}
a & b \\
c & d
\end{pmatrix}.
\]
It follows from the Problem 7.14 that \( \det A = \pm 1 \).

a. Suppose \( \det A = 1 \). Prove that \( b = -c, \ a = d \) and \( a^2 + b^2 = 1 \).

b. Suppose \( \det A = -1 \). Prove that \( b = c, \ a = -d \) and \( a^2 + b^2 = 1 \).

Exercise 7.19 (*). Use the statement of the previous problem to describe (in terms of \( 2 \times 2 \) matrices) the group of movements of a plane which preserve the origin. Prove that this is a dihedral group (cf. ALGEBRA 1).

Definition 7.8. Consider a matrix \( (A^i_j) \). It is said that the matrix \( (B^i_j) \) is obtained from \( (A^i_j) \) using the row-wise Gauss transformation, if \( (B^i_j) = (A^i_j) \circ E \), where \( E \) is the matrix either of the following form:
\[
\begin{pmatrix}
1 & \cdots & \cdots \\
\vdots & \ddots & \vdots \\
\vdots & \ddots & \ddots \\
\cdots & \cdots & \cdots \\
1 & \cdots & \cdots \\
\end{pmatrix},
\]
\[
\begin{pmatrix}
1 & \cdots & \cdots \\
\vdots & \ddots & \vdots \\
\vdots & \ddots & \ddots \\
\cdots & \cdots & \cdots \\
1 & \cdots & \cdots \\
\end{pmatrix},
\]
\[
\begin{pmatrix}
1 & \cdots & \cdots \\
\vdots & \ddots & \vdots \\
\vdots & \ddots & \ddots \\
\cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots \\
1 & \cdots & \cdots \\
\end{pmatrix},
\]
\[
\begin{pmatrix}
1 & \cdots & \cdots \\
\vdots & \ddots & \vdots \\
\vdots & \ddots & \ddots \\
\cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots \\
1 & \cdots & \cdots \\
\end{pmatrix},
\]
\[
\begin{pmatrix}
1 & \cdots & \cdots \\
\vdots & \ddots & \vdots \\
\vdots & \ddots & \ddots \\
\cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots \\
1 & \cdots & \cdots \\
\end{pmatrix},
\]
(dots denote zeroes). If \( (B^i_j) = E \circ (A^i_j) \), where \( E \) is as above, then one says that \( (B^i_j) \) is obtained from \( (A^i_j) \) using the column-wise Gauss transformation.
Exercise 7.20. Prove that the row-wise Gauss transformation can be described in terms of the following matrix operations: $(B_{ij})$ is obtained from $(A_{ij})$ by permuting of rows or by adding the $j$-th row multiplied by $\lambda$ to the $i$-th. What operations can be used to describe the column-wise Gauss transformation?

Exercise 7.21. Prove that a matrix of the form (7.1) has determinant -1 and that a matrix of the form (7.2) has determinant 1.

Exercise 7.22 (!). Prove that a Gauss transformation of the form (7.2) does not change the determinant but a transformation of the form (7.1) multiplies it by -1.

Definition 7.9. A matrix $(A_{ij})$ is called upper triangular, if $A_{ij} = 0$ when $i < j$:

$$
\begin{pmatrix}
* & * & \ldots & * & * \\
0 & * & \ldots & * & * \\
0 & 0 & \ldots & * & * \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \ldots & 0 & * \\
0 & 0 & \ldots & 0 & 0
\end{pmatrix}.
$$

A matrix is called diagonal, if $A_{ij} = 0$ when $i \neq j$.

Exercise 7.23 (!). Consider an upper triangular matrix $(A_{ij})$ of the size $n \times n$. Prove that $\det(A_{ij})$ equals to the product of all the diagonal coefficients:

$$
\det(A_{ij}) = \prod_i A_{ii}.
$$

Exercise 7.24. 

a. Prove that any matrix can be brought into upper triangular form using row-wise Gauss transformations;

b. Prove that any matrix can be brought into diagonal form using row-wise and column-wise Gauss transformations.

Remark. Since Gauss transformations preserve the determinant (up to $\pm 1$), one can compute the determinant of a square matrix by bringing it to diagonal form and multiplying the coefficients on the diagonal.

Exercise 7.25 (*). Consider a Euclidean ring $A$ (cf. ALGEBRA 2) such that any element $a \in A$ admits decomposition into prime factors. Solve the Problem 7.24 for matrices with elements from $A$.

Hint. First consider matrices $(a_{ij})$ of the size $1 \times 2$, then prove the statement by induction for matrices of the size $1 \times n$ (which is the same as $n \times 1$). Prove that after the matrix is brought into upper triangular form, the only non-zero element will be $\text{GCD}(a_1^1, \ldots, a_n^1)$. Consider now an arbitrary matrix of the size $m \times n$ and permute the columns and the rows in such a way that $a_1^1$ be non-zero. To prove (b) apply the Gauss transformation to rows, columns then once more to rows, once more to columns etc. and obtain a matrix where $a_1^1 \neq 0$ and such that all other elements of the first column and the first row are zeroes.
Grassmann algebra and minors of matrices

Exercise 7.26 (!). Consider a basis $v_1, \ldots, v_n$ of a vector space $V$, then $v_{i_1} \wedge v_{i_2} \wedge \cdots \wedge v_{i_k}$, $i_1 < i_2 < \cdots < i_k$ is the corresponding basis in $\Lambda^k(V)$. Consider a matrix $A \in \text{End}(V)$, and $A(i_1, i_2, \ldots, i_k; i'_1, i'_2, \ldots, i'_k)$, the coefficients of the matrix of the endomorphism induced by $A$ on $\Lambda^k(V)$ in the basis described above. Prove that $A(i_1, i_2, \ldots, i_k; i'_1, i'_2, \ldots, i'_k)$ is the determinant of the matrix which is obtained from $A$ after all rows except $i_1$-th, $i_2$-th, $\ldots$, $i_k$-th and all columns except $i'_1$-th, $i'_2$-th, $\ldots$, $i'_k$-th has been removed from it.

Remark. This determinant is called the minor of the matrix $A$.

Hint. Take the composition of $A$ with an operator that maps $v_{i_l}$ to $v_{i'_l}$, and reduce the problem to the case $i_l = i'_l$. Prove that the coefficients $A(i_1, i_2, \ldots, i_k; i'_1, i'_2, \ldots, i'_k)$ do not depend on rows except the $i_1$-th, $i_2$-th, $\ldots$, $i_k$-th rows, and on columns except the $i'_1$-th, $i'_2$-th, $\ldots$, $i'_k$-th columns. Then put $A_{ij} = 0$ if $i$ and $j$ do not belong to $\{i_1, i_2, \ldots, i_k\}$. Thus you have reduced the problem to the case when $V = V_1 \oplus V_2$ and $A$ is of the form $B \oplus 0_{V_2}$ where $B \in \text{End}(V_1)$ and $0_{V_2}$ acts on $V_2$ by mapping all vectors to 0. In this situation one can apply the formula $\Lambda^* (V) = \Lambda^* (V_1) \otimes \Lambda^* (V_2)$ to get the desired result.

Definition 7.10. Consider a linear operator $A \in \text{End}(V)$. Consider the endomorphism induced by $A$ on $\Lambda^*(V)$. Consider the biggest number $N$ such that this endomorphism is non-zero on $\Lambda^N(V)$. This number $N$ is called the rank of the linear operator $A$ (denoted $\text{rk} A$). If $A$ is represented by a matrix $(A_{ij})$ then $\text{rk} A$ is called the rank of this matrix.

Exercise 7.27 (!). Consider an operator $A$ that induces the zero action on $\Lambda^k(V)$. Prove that $A$ induces the zero action on $\Lambda^l(V)$ for any $l > k$.

Exercise 7.28. Prove that the rank of a matrix is the size of its biggest non-zero minor.

Exercise 7.29. Prove that the rank of an operator $A$ is the biggest number $N$ such that there are vectors $v_1, \ldots, v_N$ such that $A(v_1), \ldots, A(v_N)$ are linearly independent.

Exercise 7.30 (!). Prove that the rank of an operator $A$ is the dimension of its image.

Exercise 7.31. Consider a matrix of rank 1. Prove that all its rows are proportional. Prove that all its columns are proportional.

Exercise 7.32. Prove that $\text{rk} A = \text{rk} A^*$.

Hint. Use the Problem 7.9.

Definition 7.11. A bilinear form $\mu : V_1 \otimes V_2 \rightarrow k$ is called nondegenerate pairing if for every non-zero $v_1 \in V_1$ there is a vector $v'_1 \in V_2$ such that $\mu (v_1, v'_1) \neq 0$ and for any non-zero $v_2 \in V_2$ there is a vector $v'_2 \in V_1$ such that $\mu (v_2, v'_2) \neq 0$.

Exercise 7.33. Consider finite-dimensional vector spaces $V_1, V_2$. Prove that a nondegenerate pairing $\mu : V_1 \otimes V_2 \rightarrow k$ defines an isomorphism between $V_1$ and $V_2^*$ and any isomorphism between those spaces is defined in this way.
Exercise 7.34 (!). Consider an $n$-dimensional vector space $V$. Construct the natural isomorphism
\[ \Lambda^k(V)^* \cong \Lambda^{n-k}(V) \otimes \det V^* \]
(det $V$ denotes the one-dimensional vector space $\Lambda^n(V)$).

Hint. Use the previous problem.

Exercise 7.35. Consider an $n$-dimensional vector space $V$ with the basis $v_1, v_2, \ldots, v_n$ and an operator $A \in \text{End} \ V$. Consider the basis $w_1, w_2, \ldots, w_n$ in $\Lambda^{n-1}(V)$ where $w_k = v_1 \wedge v_2 \wedge \cdots \wedge v_{k-1} \wedge v_{k+1} \wedge \cdots$ (there are all $v_i$ in the product except one). Consider the matrix $(A^i_j)$ of $A$ and consider $A^i_j$, the minor that is obtained from $A$ after $i$-th row and $j$-th column have been removed. Prove that $A$ acts on $\Lambda^{n-1}(V)$ by the matrix $(\tilde{A}^i_j)$ in this basis.

Exercise 7.36. In the previous problem setting consider a nondegenerate bilinear pairing
\[ V \otimes \Lambda^{n-1}(V) \rightarrow \det V, \]
defined by the form $v \otimes w \rightarrow v \wedge w$. Choose the isomorphism $k \cong \det V$ such that $v_1 \wedge v_2 \wedge \cdots \wedge v_n$ is mapped to 1. This gives a nondegenerate pairing defined on $V$ and $\Lambda^{n-1}(V)$. Prove that the basis in $\Lambda^{n-1}(V)$ dual to $v_1, v_2, \ldots, v_n$ is $w_1, -w_2, w_3, -w_4, \ldots$. Prove that $A$ acts on $\Lambda^{n-1}(V)$ by the matrix $((-1)^{i+j}\tilde{A}^i_j)$ in this basis.

Exercise 7.37. Consider a nondegenerate bilinear pairing $\mu : V \otimes V^\prime \rightarrow k$ and endomorphisms $A \in \text{End} \ V$ and $B \in \text{End} \ V^\prime$ such that $\mu(Av, Bv') = \mu(v, v')$ for all $v, v' \in V, V^\prime$. Choose dual bases in $V, V^\prime$ and suppose $(\alpha_j^i)$ and $(\beta_j^i)$ are the matrices of $A$ and $B$. Prove that $(\alpha_j^i) \circ (\beta_j^i)^{-1} = \text{id}$.

Exercise 7.38 (!). Consider an $A \in \text{End} V$ where $V$ is an $n$-dimensional vector space with a basis $v_1, v_2, \ldots, v_n$ and $(A^i_j)$ is the matrix of the operator $A$. Prove that $A$ is invertible iff $\det A \neq 0$. Prove that
\[ A^{-1} = \frac{1}{\det A}((-1)^{i+j}\tilde{A}^i_j)^{-1}. \]

Hint. Prove that for the natural pairing form
\[ V \otimes \Lambda^{n-1}(V) \xrightarrow{\mu} \det V, \]
it holds that $\mu(A(v), A(w)) = \det A \mu(v, w)$, where $A(w)$ denote the natural action of $A$ on $\Lambda^{n-1}(V)$. Then use the previous problem for $(A^i_j) = (\alpha_j^i), \frac{1}{\det A}((-1)^{i+j}\tilde{A}^i_j) = (\beta_j^i)^{-1}$.

Remark. We have obtained the well-known formula for calculation of the inverse matrix by expansion by minors. The geometric meaning of this formula can be explained as follows: minors of a matrix are (by definition) the matrix coefficients of the action of this matrix on $\Lambda^{n-1}(V)$ and the natural pairing between $V$ and $\Lambda^{n-1}(V)$ is multiplied by $\det A$ by the action of $A$. This allows for the calculation of $A^{-1}$ using $\det A$ and $A$.

Calculation of determinant

Exercise 7.39 (!). Consider the matrix $(A^i_j)$ of a linear operator $A$. Prove that $\det A$ is equal to
\[ \sum_{\sigma \in S_n} \text{sgn}(\sigma) A_{\sigma_1}^1 A_{\sigma_2}^2 \cdots A_{\sigma_n}^n \]
where $(\sigma_1, \sigma_2, \ldots, \sigma_n) \in S_n$ is a permutation, the sum is over the elements of the group of all permutations and $\text{sgn}$ is the sign of the permutation $\sigma$.
Hint. Use the explicit formula (one that uses the sum over the elements of $S_n$) from ALGEBRA 6 for the tensor $v_1 \wedge v_2 \wedge \cdots \wedge v_n$.

Remark. The determinant is usually defined using this formula.

Exercise 7.40. Consider the matrix $(A^i_j)$ of a linear operator $A$. Prove that $\det A$ can be calculated as follows:

$$A^1_1 A^1_1 - A^1_2 A^1_2 + A^1_3 A^1_3 \ldots$$

where $A^i_j$ are minors that are obtained after removing the $i$-th row and $j$-th column.

Remark. This procedure is called determinant expansion along a row.

Exercise 7.41 (*). (Vandermonde determinant) Consider the matrix

$$\begin{pmatrix}
1 & 1 & 1 & \ldots & 1 \\
t_1 & t_2 & t_3 & \ldots & t_n \\
t_1^2 & t_2^2 & t_3^2 & \ldots & t_n^2 \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
t_1^{n-1} & t_2^{n-1} & t_3^{n-1} & \ldots & t_n^{n-1}
\end{pmatrix},$$

where $n > 1$. Prove that its determinant is $\prod_{i<j}(t_i - t_j)$.

Exercise 7.42 (*). Consider the matrix

$$\begin{pmatrix}
t & x_1 & x_2 & x_3 & \ldots & x_n \\
t^2 & x_1^2 & x_2^2 & x_3^2 & \ldots & x_n^2 \\
t^4 & x_1^4 & x_2^4 & x_3^4 & \ldots & x_n^4 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
t^{2n} & x_1^{2n} & x_2^{2n} & x_3^{2n} & \ldots & x_n^{2n}
\end{pmatrix},$$

and denote its determinant as $P_n(t, x_1, \ldots, x_n)$. Suppose that this matrix is over the field $\mathbb{Z}/2\mathbb{Z}$. Prove that $P_n(t, x_1, \ldots, x_n)$ becomes zero if one takes $t = \sum \alpha_i x_i$ to be an arbitrary linear combination of $x_i$. Deduce from Bézout’s theorem that

$$P_n(t, x_1, \ldots, x_n) = Q(x_1, \ldots, x_n) \prod (t - \sum \alpha_i x_i),$$

where $\alpha_i \in \mathbb{Z}/2\mathbb{Z}$, and $Q \in \mathbb{Z}/2\mathbb{Z}[x_1, \ldots, x_n]$ is a polynomial.

Hint. Use long division of $P_n$ by $t - \sum \alpha_i x_i$. If you get a non-zero value, then if you substitute $t$ for $t = \sum \alpha_i x_i$ in $P(t)$ then you will also get a non-zero value.

Exercise 7.43 (*). Prove in the previous problem setting that $Q = P_{n-1}(x_n)$.

Exercise 7.44 (*). Deduce from the previous problem that $Q(x_1, \ldots, x_n) \neq 0$.

Exercise 7.45 (*). (Dickson’s theorem) Consider the polynomial

$$F_n(t) = \prod (t - \sum \alpha_i x_i) \in \mathbb{Z}/2\mathbb{Z}[x_1, \ldots, x_n].$$

Prove that

$$F_n(t) = t^{2^n} + \sum_{i=0}^{n-1} c_{n,i} t^{2^i},$$

where $c_{n,i} \in \mathbb{Z}/2\mathbb{Z}[x_1, \ldots, x_n]$ are polynomials in $x_1, \ldots, x_n$. 
Hint. Use the previous problem and problem 7.42.

Remark. Polynomials $c_{n,i} \in \mathbb{Z}/2\mathbb{Z}[x_1, \ldots, x_n]$ are called Dickson’s invariants.

Exercise 7.46 (*). Consider the coefficients $Q_r$ (which are $c_{n,i}$ according to Dickson’s theorem) of the polynomial $F_n(t)$ as elements of the symmetric algebra $S^*(V)$ where $V$ is the vector space over the field $\mathbb{Z}/2\mathbb{Z}$ with basis $x_1, \ldots, x_n$. Consider the action of the group $GL(V)$ of invertible linear operators on $V$ and extend it naturally (by multiplicativity) over the symmetric algebra. Prove that $Q_r$ is invariant with respect to $GL(V)$:

$$Q_r(x_1, x_2, \ldots, x_n) = Q_r(h(x_1), h(x_2), \ldots, h(x_n))$$

where $h \in GL(V)$ is an arbitrary invertible endomorphism.

Remark. Consider the subring of $GL(V)$-invariant polynomials in the polynomials ring $S^*(V)$. Dickson (1911) proved that this ring is the ring of polynomials with generators $c_{n,i}$. Consult


for details.