Nineth course: september 26, 2007. [12]

2.2.5 Elementary symmetric functions

References for this section are [2, 5].

Let L be the field $\mathbb{Q}(x_1,\ldots,x_n)$ of rational fractions in n variables over $\mathbb{Q}$. The *elementary symmetric functions* $s_1,\ldots,s_n\in\mathbb{Q}[x_1,\ldots,x_n]$ are defined by

$$(X-x_1)(X-x_2)\cdots(X-x_n)=X^n-s_1X^{n-1}+s_2X^{n-2}-\cdots+(-1)^ns_n.$$

For instance

$$s_1=x_1+\cdots+x_n,\quad s_n=x_1\cdots x_n$$

and

$$s_2=x_1x_2+x_1x_3+\cdots+x_1x_n+x_2x_3+\cdots+x_2x_n+\cdots+x_{n-1}x_n.$$

More generally, for $1\le k\le n$, *the* k*-th elementary symmetric function in* n *variables* is

$$s_k=\sum_{i_1<i_2<\cdots<i_k}x_{i_1}x_{i_2}\cdots x_{i_k}.$$

The *general polynomial of degree* n is $f(X)=(X-x_1)(X-x_2)\cdots(X-x_n)$. Further, let K denote the subfield $\mathbb{Q}(s_1,\ldots,s_n)$ of L. The polynomial f has its coefficients in K and its splitting field over K is L. Since f has degree n, the Galois group of L over K is (isomorphic to) a subgroup of $\mathfrak{S}_n$. As a consequence $[L:K]\le n!$.

Any permutation of $\{1,\ldots,n\}$ induces an automorphism of L which fixes each of s_k $(1\le k\le n)$. Hence K is contained in the subfield $L^{\mathfrak{S}_n}$ of L fixed by $\mathfrak{S}_n$. According to Galois theory, the extension $L/L^{\mathfrak{S}_n}$ has degree $n!$ Hence $K=L^{\mathfrak{S}_n}$ and L is an extension of K of degree $n!$ and Galois group $\mathfrak{S}_n$.

A rational function $F(x_1,\ldots,x_n)\in L$ is called *symmetric* if it is invariant under $\mathfrak{S}_n$. Hence we have proved:

Proposition 2.25. *A rational function $F(x_1,\ldots,x_n)\in\mathbb{Q}(x_1,\ldots,x_n)$ is symmetric if and only if there exists a rational function G in n variables such that*

$$F(x_1,\ldots,x_n)=G(s_1,\ldots,s_n).$$

The rational function G is unique. If F is a polynomial, then G is also a polynomial. An algorithm for computing it is given in exercise 37, § 14.6 of [2].

Exercise 2.26. *Prove that the elements $s_1,\ldots,s_n$ are algebraically independent over $\mathbb{Q}$.*

[12] Updated: October 12, 2007

2.2.6 Modules over principal rings

References for this section are [2, 3, 5].

Let A be a ring (commutative with unit, as usual), M a A–module, N_1 and N_2 submodules of M. By definition M is the direct sum of N_1 and N_2 if the map $(x_1, x_2) \mapsto x_1 + x_2$ is an isomorphism of A-modules of $N_1 \times N_2$ onto M. In this case we write $M = N_1 \oplus N_2$. This means $M = N_1 + N_2$ and $N_1 \cap N_2 = \{0\}$.

A *free A–module* is a A-module having a basis. Example like $\mathbb{Z}/2\mathbb{Z}$ (and more generally any finite abelian group viewed as a $\mathbb{Z}$–module) or $\mathbb{Q}$ show that modules over $\mathbb{Z}$ may not have a basis.

When A is a domain and M a A-module, the *rank* of M is the maximal number of elements in M which are linearly independent over A. If we denote by K the field of fractions of A and if M is a free A–module, then one can embed M into a K-vector space V and the rank of a submodule N of M is the dimension of the K–vector space spanned by N in V. For instance the rank of M itself is the number of elements in any basis of M over A.

Proposition 2.27 (Free modules over a PID)**.** *Let A be a PID, M a free A-module of rank m and N a sub–A-module of M. Then N is free of rank $n \le m$. Moreover there exists a basis $\{e_1, \dots, e_m\}$ of M as a A-module and there exists elements $a_1, \dots, a_n$ in A such that $\{a_1e_1, \dots, a_ne_n\}$ is a basis of N over A and a_i divides a_{i+1} in A for $1 \le i < n$.*

The ideals $a_1A \supset a_2A \supset \cdots \supset a_nA$ of A are called the *invariant factors* of the sub–A-module N of M: they do not depend on the basis $(a_1, \dots, e_n)$ of M satisfying the conditions of Proposition 2.27.

2.2.7 Geometry of numbers: subgroups of $\mathbb{R}^n$.

References for this section are [1, 4, 6].

Lemma 2.28. *A subgroup G of $\mathbb{R}^n$ is discrete in $\mathbb{R}^n$ if and only if there exists an open subset U of $\mathbb{R}^n$ containing 0 such that $G \cap U$ is discrete.*

Exercise 2.29. *1. Check that a non discrete subgroup of $\mathbb{R}$ is dense in $\mathbb{R}$*
2. Give the list of closed subgroups of $\mathbb{R}$.
3. Let G be a finitely generated subgroup of $\mathbb{R}$. Give a necessary and sufficient condition on the rank of G for G to be dense in $\mathbb{R}$.
4. Let $\vartheta \in \mathbb{R}$. Give a necessary and sufficient condition on ϑ for the subgroup $\mathbb{Z} + \mathbb{Z}\vartheta$ to be dense in $\mathbb{R}$.

Proposition 2.30. *Let G be a discrete subgroup of $\mathbb{R}^n$. There exists an integer t in the interval $0 \le t \le n$ and there exist elements $e_1, \dots, e_t$ in G, which are linearly independent over $\mathbb{R}$, such that $G = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_t$.*

In particular $e_1, \dots, e_t$ are linearly independent over $\mathbb{Z}$, hence G is free of rank t. The integer t is the dimension of the $\mathbb{R}$–subspace of $\mathbb{R}^n$ spanned by G.

Exercise 2.31. *From Proposition 2.30, deduce that in a discrete subgroup of $\mathbb{R}^n$, linearly independent elements over $\mathbb{Z}$ are linearly independent over $\mathbb{R}$.*

Definition. *A discrete subgroup of $\mathbb{R}^n$ of maximal rank n is called a lattice) of $\mathbb{R}^n$.*

Proof of Proposition 2.30. Denote by V the vector subspace of $\mathbb{R}^n$ over $\mathbb{R}$ spanned by G, by t its dimension and let $\{f_1, \dots, f_t\}$ be a maximal subset of G which is free over $\mathbb{R}$: it is a basis of V over $\mathbb{R}^n$ and $G' = \mathbb{Z}f_1 + \cdots + \mathbb{Z}f_t$ is a subgroup of G. We show that G' has finite index in G, which means that there are only finitely many classes of G modulo G'.

Let K be the compact subset of $\mathbb{R}^n$ defined by

$$\{u_1f_1 + \cdots + u_tf_t \; ; \; 0 \le u_i \le 1 \; (1 \le i \le t)\}.$$

Since G is discrete, $G \cap K$ is finite.

Let $x \in G$. Then $x \in V$, hence we can write $x = x_1f_1 + \cdots + x_tf_t$ with $x_i \in \mathbb{R}$. Let $m_i = [x_i]$ be the integral part of x_i:

$$m_i \in \mathbb{Z}, \quad 0 \le x_i - m_i < 1 \qquad (1 \le i \le n).$$

Set $x' = m_1f_1 + \cdots + m_tf_t$. Then $x' \in G'$ and $x - x' \in G \cap K$. Therefore there are only finitely many classes of G modulo G', which means that G' has finite index in G.

Denote by s the order of the finite group G/G' and set $f_i' = f_i/s$ $(1 \le i \le t)$. We have

$$G' = \mathbb{Z}f_1 + \cdots + \mathbb{Z}f_t \subset G \subset \mathbb{Z}f_1' + \cdots + \mathbb{Z}f_t',$$

and the conclusion follows from Proposition 2.27.

□

Theorem 2.32 (Structure of subgroups of $\mathbb{R}^n$)**.** *Let G be an additive subgroup of $\mathbb{R}^n$. There exists a maximal vector subspace V of $\mathbb{R}^n$ over $\mathbb{R}$ which is contained in the topological closure of G. Let d be the dimension of V and $d+t$ the dimension of the vector space spanned by G over $\mathbb{R}$. Set $G' = G \cap V$. Then G' is dense in V and there exists a discrete subgroup G'' of G, of rank t, such that G is the direct sum of G' and G''.*

Exercise 2.33. *Let $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$. Consider the subgroup*

$$G = \mathbb{Z}^n + \mathbb{Z}\mathbf{x} = \{(a_1 + a_0x_1, \dots, a_n + a_0x_n) \; ; \; (a_0, \dots, a_n) \in \mathbb{Z}^{n+1}\}$$

of $\mathbb{R}^n$.

1. *Show that G is discrete in $\mathbb{R}^n$ if and only if $\mathbf{x} \in \mathbb{Q}^n$.*

2. *Deduce that the following properties are equivalent.*

(i) 0 is an accumulation point of G.

(ii) For any $\epsilon > 0$, there exist integers $p_1, \dots, p_n$, q, with $q > 0$, such that

$$0 < \max_{1 \le i \le n} |qx_i - p_i| < \epsilon.$$

(iii) A least one of the n numbers $x_1, \dots, x_n$ is irrational.

3. *Check that G is dense in $\mathbb{R}^n$ if and only if the numbers $1, x_1, \ldots, x_n$ are linearly independent over $\mathbb{Q}$.*
Deduce that for any $(\xi_1, \xi_2) \in \mathbb{R}^2$ and for any $\epsilon > 0$, there exist rational integers p_1, p_2 and q with

$$|\xi_1 - p_1 - q\sqrt{2}| \leq \epsilon \quad \textit{and} \quad |\xi_2 - p_1 - q\sqrt{3}| \leq \epsilon.$$

Let G be a lattice in $\mathbb{R}^n$. For each basis $\mathbf{e} = \{e_1, \ldots, e_n\}$ of G the parallelogram

$$P_{\mathbf{e}} = \{x_1 e_1 + \cdots + x_n e_n \ ; \ 0 \leq x_i < 1 \ (1 \leq i \leq n)\}$$

is a *fundamental domain* for G, which means a complete system of representative of classes modulo G. We get a partition of $\mathbb{R}^n$ as

$$\mathbb{R}^n = \bigcup_{g \in G} (P_{\mathbf{e}} + g) \tag{2.34}$$

A change of bases of G is obtained with a matrix with integer coefficients having determinant ± 1, hence the Lebesgue measure $\mu(P_{\mathbf{e}})$ of $P_{\mathbf{e}}$ does not depend on $\mathbf{e}$: this number is called the *volume* of the lattice G and denoted by $v(G)$.

Here is an example of results obtained by H. Minkowski in the XIX–th century as an application of his *geometry of numbers.*

Theorem 2.35 (Minkowski)**.** *Let G be a lattice in $\mathbb{R}^n$ and B a measurable subset of $\mathbb{R}^n$. Set $\mu(B) > v(G)$. Then there exist $x \neq y$ in B such that $x - y \in G$.*

Proof. From (2.34) we deduce that B is the disjoint union of the $B \cap (P_{\mathbf{e}} + g)$ with g running over G. Hence

$$\mu(B) = \sum_{g \in G} \mu\left(B \cap (P_{\mathbf{e}} + g)\right).$$

Since Lebesgue measure is invariant under translation

$$\mu\left(B \cap (P_{\mathbf{e}} + g)\right) = \mu\left((-g + B) \cap P_{\mathbf{e}}\right).$$

The sets $(-g + B) \cap P_{\mathbf{e}}$ are all contained in $P_{\mathbf{e}}$ and the sum of their measures is $\mu(B) > \mu(P_{\mathbf{e}})$. Therefore they are not all pairwise disjoint – this is one of the versions of the *Dirichlet box principle*). There exists $g \neq g'$ in G such that

$$(-g + B) \cap (-g' + B) \neq \emptyset.$$

Let x and y in B satisfy $-g + x = -g' + y$. Then $x - y = g - g' \in G \setminus \{0\}$. $\square$

Corollary 2.36. *Let G be a lattice in $\mathbb{R}^n$ and let B be a measurable subset of $\mathbb{R}^n$, convex and symmetric with respect to the origin, such that $\mu(B) > 2^n v(G)$. Then $B \cap G \neq \{0\}$.*

Proof. We use Theorem 2.35 with the set

$$B' = \frac{1}{2}B = \{x \in \mathbb{R}^n \ ; \ 2x \in B\}.$$

We have $\mu(B') = 2^{-n}\mu(B) > v(G)$, hence by Theorem 2.35 there exists $x \neq y$ in B' such that $x - y \in G$. Now $2x$ and $2y$ are in B, and since B is symmetric $-2y \in B$. Finally B is convex, hence $(2x - 2y)/2 = x - y \in G \cap B \setminus \{0\}$.

□

Remark. *With the notations of Corollary 2.36, if B is also compact in $\mathbb{R}^n$, then the weaker inequality $\mu(B) \geq 2^n v(G)$ suffices to reach the conclusion. This is obtained by applying Corollary 2.36 with $(1+\epsilon)B$ for $\epsilon \to 0$.*

Exercise 2.37. *Let m and n be positive integers.*
a) Let t_{ij} for $1 \leq i,j \leq n$ be n^2 real numbers with determinant ± 1. Let $A_1, \ldots, A_n$ be positive real numbers with $A_1 \cdots A_n = 1$. Show that there exists an non–zero element $(x_1, \ldots, x_n)$ in $\mathbb{Z}^n$ such that

$$|x_1 t_{i1} + \cdots + x_n t_{in}| < A_i \quad \textit{for} \quad 1 \leq i \leq n-1$$

and

$$|x_1 t_{1n} + \cdots + x_n t_{nn}| \leq A_n.$$

`Hint`. *First solve the system with the weaker inequality $<$ in place of $<$*

$$|x_1 t_{i1} + \cdots + x_n t_{in}| \leq A_i \quad \textit{for} \quad 1 \leq i \leq n$$

by using Corollary 2.36. Next use the same method but with A_n replaced with $A_n + \epsilon$ for a sequence of ϵ which tends to 0.
b) Deduce the following result. Let ϑ_{ij} $(1 \leq i \leq n,\ 1 \leq j \leq m)$ be mn real numbers. Let $Q > 1$ be a real number. Show that there exists rational integers $q_1, \ldots, q_m$, $p_1, \ldots, p_n$ with

$$1 \leq \max\{|q_1|, \ \ldots, \ |q_m|\} < Q^{n/m}$$

and

$$\max_{1 \leq i \leq n} |\vartheta_{i1} q_1 + \cdots + \vartheta_{im} q_m - p_i| \leq \frac{1}{Q}.$$

`Hint`. *Use a) with n replaced by $n+m$ and for a triangular matrix $(t_{ij})_{1 \leq i,j \leq m+n}$ with 1 on the diagonal.*
c) Deduce that if $\vartheta_1, \ldots, \vartheta_m$ are real numbers and H a real number > 1, then there exists a tuple $(a_0, a_1, \ldots, a_m)$ of rational integers such that

$$0 < \max_{1 \leq i \leq m} |a_i| < H \quad \textit{and} \quad |a_0 + a_1\vartheta_1 + \cdots + a_m\vartheta_m| \leq H^{-m}.$$

d) Let ϑ be a real number with $|\vartheta| \leq 1/2$, d a positive integer and H a positive integer. Show that there exists a non–zero polynomial $P \in \mathbb{Z}[X]$ of degree $\leq d$ and coefficients in the interval $[-H, H]$ such that

$$|P(\vartheta)| \leq H^{-d}.$$

We conclude this section with the definition of a *rational subspace*. Let $k \subset K$ be a field extension and n a positive integer. For a K-vector subspace V of K^n, the two following properties are equivalent:
(i) There exists a basis of V which consists of elements in k^n.
(ii) There exist linear forms $L_1, \ldots, L_m$ with coefficients in k such that V is the intersection of the hyperplans $L_i = 0$, $(1 \le i \le m)$.
When there properties are satisfied the subspace V is called *rational over* k.

Exercise 2.38. *Let $\vartheta_1, \ldots, \vartheta_m$ be real numbers. Assume that $1, \vartheta_1, \ldots, \vartheta_m$ are linearly independent over $\mathbb{Q}$. Let V be a vector subspace of $\mathbb{R}^{m+1}$ which is rational over $\mathbb{Q}$ and has dimension $\le m$.*
a) Check that the intersection of V with the real line $\mathbb{R}(1, \vartheta_1, \ldots, \vartheta_m)$ is $\{0\}$.
b) Deduce that

$$\|(x_0, x_1, \ldots, x_m)\| = \max_{1 \le i \le m} |x_0\vartheta_j - x_j|$$

defines a norm on V.

2.2.8 Elimination Theory, Resultant.

References for this section are [2, 5, 7].

Let k be a field and P, Q two polynomials in $\mathbb{Q}[X]$ of degrees n and m respectively. Since $k[X]$ is a UFD, we can decompose P and Q as products of irreducible polynomials. The ideal $\mathcal{I}$ generated by P and Q is principal, generated by the greatest common divisor of P and Q (this gcd is unique up to a constant, it is unique if we require that it is monic. Bézout's Theorem states that this gcd can be written as $UP + VQ$ with U and V in $k[X]$, and Euclide's algorithms gives a solution (U, V) with $\deg U < \deg Q$ and $\deg V < \deg P$. This ideal is $k[X]$ if and only if the monic gcd is 1, which means also that P and Q have no common zero in an algebraic closure of k.

Assume $\gcd(P, Q) = 1$. The problem with Euclide's algorithm is that it is efficient for numerical purposes, when the polynomials P and Q are given, but it is not so efficient for giving estimates for the coefficients of U and V. Fortunately there is another efficient algorithm to compute U and V such that $PU + QV$ is a non–zero constant in k. Write

$$P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0, \quad Q = b_mX^m + b_{m-1}X^{m-1} + \cdots + b_0$$

and

$$U = u_{m-1}X^{m-1} + u_{m-2}X^{m-2} + \cdots + u_0, \quad V = v_{n-1}X^{n-1} + v_{n-2}X^{n-2} + \cdots + v_0.$$

Consider the coefficients $u_0, u_1, \ldots, u_{m-1}$, $v_0, v_1, \ldots, v_{n-1}$ of U and V as $m+n$ unknowns which should satisfy the system of $m+n$ equations given by the fact that the coefficients of $X, X^2, \ldots, X^{m+n-1}$ in $PU + QV$ is zero, while the constant coefficient is not zero. The determinant of the matrix of this system is not zero, since there is a solution by Bézout's Theorem. Here is the matrix

$$\begin{pmatrix}
a_n & a_{n-1} & \cdots & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\
0 & a_n & \cdots & \cdots & a_2 & a_1 & a_0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & a_n & a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_0 \\
b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & 0 & \cdots & 0 \\
0 & b_m & \cdots & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & & \vdots \\
\vdots & \vdots & & \ddots & & & & \ddots & \vdots \\
0 & 0 & \cdots & 0 & b_m & b_{m-1} & b_{m-2} & \cdots & b_0
\end{pmatrix}$$

There are m rows with the coefficients of P and n rows [13] with the coefficients of Q, the diagonal is $(a_n, \ldots, a_n, b_0, \ldots, b_0)$. This matrix can be considered for any pair (P, Q) of polynomials with coefficients in any domain A. The determinant R of this matrix is then an element in A which is called the *resultant* of P and Q. The determinant is invariant by linear combinations of the columns: multiplying the k–th column by X^{m+n-k}, adding to the last column and expanding the determinant shows that there are polynomials U and V such that $R = PU+QV$. The resultant is not zero if and only if U and V are relatively prime in $k[X]$, where k is the quotient field of A.

Exercise 2.39. *a) Using the Cauchy–Schwarz inequality*

$$\left|\sum_i x_i y_i\right|^2 \le \left|\sum_i x_i\right|^2 \cdot \left|\sum_i y_i\right|^2,$$

show that the absolute value of a determinant with complex coefficients is bounded by the product of the Euclidean norms of its columns.
b) For a polynomial $P = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$ *in* $\mathbb{C}[X]$*, define*

$$\|P\| = (|a_n|^2 + \cdots + |a_0|^2)^{1/2}.$$

Let P *and* Q *be two non–constant polynomials in* $\mathbb{Z}[X]$ *of degrees* n *and* m *respectively. Show that the two following properties are equivalent:*
(i) P *and* Q *are relatively prime in* $\mathbb{Q}[X]$*.*
(ii) For any $\vartheta \in \mathbb{C}$*,*

$$(m+n)\|P\|^m\|Q\|^n \max\{|P(\vartheta)|, |Q(\vartheta)|\} > 1.$$

References

[1] N. Bourbaki – *Eléments de Mathématique*, Topologie Générale, Herman 1974, Chap. VII, § 1, N°1, Prop. 2;

[13] The matrix has been written in the case $m = n - 1$

[2] D.S. DUMMIT & R.M. FOOTE – *Abstract Algebra*, Prentice Hall 1991, 1999.

[3] BÙI XUÂN HẢI – *Nhóm Tuyến Tính* (chuyên đề cao học), NXB ĐHQG Tp HCM 2007.

[4] G.H. HARDY & A.M. WRIGHT – *An Introduction to the Theory of Numbers*, Oxford Sci. Publ., 1938, Chap. XXIII.

[5] S. LANG – *Algebra*, Third edition. Addison-Wesley Publishing Co., Reading, Mass., 1993. Trad. franç. *Algèbre*, Dunod, 2004.

[6] W. M. SCHMIDT – *Diophantine approximation*, Lecture Notes in Mathematics, vol. 785, Springer-Verlag, Berlin, 1980. See Chap. 1 § 5.

[7] M. WALDSCHMIDT – *Nombres transcendants*, Lecture Notes in Mathematics, Vol. **402**, Springer-Verlag (1974). See Chap. 5.