Algebra, Arithmetic and Geometry – With a View Toward Applications / 2005

Lectures : Tuesday/Thursday 18:15–19:15 ; LH-1, Department of Mathematics
Supplementary Lectures : Friday 18:15–19:15 ; LH-1, Department of Mathematics

4. Linear Equations, Linear independence, Bases – Dimensions of vector spaces

Johann Carl Friedrich Gauss[†]
(1777-1855)

In the exercises below A denote a ring with unity 1_A (not necessarily commutative).

4.1. Let K be a division ring and let V be a non- zero vector space over K. Let $\mathfrak{G} = (g_i)_{i\in I}$ be a finite system of linear equations in n unknowns in V over K. Use Gauss elimination to show that:

a). If $\mathrm{L}(\mathfrak{G}) \neq \emptyset$ and $g \in K^n \times V$ with $g \notin K\mathfrak{G}$, then $\mathrm{L}(\mathfrak{G}) \neq \mathrm{L}(\mathfrak{G} \cup \{g\})$.

b). Let $\mathfrak{H}$ be another finite system of linear equations in n unknowns in V over K. Suppose that $\mathrm{L}(\mathfrak{G}) \neq \emptyset$ and $\mathrm{L}(\mathfrak{H}) \neq \emptyset$. Then $\mathrm{L}(\mathfrak{G}) = \mathrm{L}(\mathfrak{H})$ if and only if $K\mathfrak{G} = K\mathfrak{H}$.

4.2. Let K be a field and let k be a subfield of K. Further, let $\mathfrak{G}$ be a finite system of linear equations in n unknowns over k and let $\mathrm{L}_k(\mathfrak{G})$ denote the solution set in k^n. The system $\mathfrak{G}$ is also a system of linear equations over K and let the solution set of this system in K^n be denoted by $\mathrm{L}_K(\mathfrak{G})$. Then $\mathrm{L}_k(\mathfrak{G}) = k^n \cap \mathrm{L}_K(\mathfrak{G})$ and use Gauss elimination process to prove:

a). $\mathrm{L}_k(\mathfrak{G}) \neq \emptyset$ if and only if $\mathrm{L}_K(\mathfrak{G}) \neq \emptyset$.

b). If $\mathfrak{G}$ homogeneous, then $\mathrm{L}_K(\mathfrak{G}) = K \cdot \mathrm{L}_k(\mathfrak{G})$.

c). If $\mathfrak{G}$ homogeneous, then $\mathfrak{G}$ has a non-trivial solution over k if and only if $\mathfrak{G}$ has a non-trivial solution over K.

4.3. Let V be a free module over a ring A. Further, let $a \in A$ be not a left-zero divisor in A. Then the homothecy $\vartheta_a : V \to V, x \mapsto ax$ is injective. Deduce that: Let B be a ring and let A be a subring of B such that B is a free A–module. Show that an element $a \in A$ is a left-zero divisor in A, if and only if a is a left-zero divisor in B. Further, show that $(\mathfrak{a}B) \cap A = \mathfrak{a}$ for all left-ideals $\mathfrak{a} \subseteq A$.

4.4. a). Let $x_1, \ldots, x_n,\ x_{n+1},\ n \in \mathbb{N}$, be elements of a vector space V over a division ring K. Show that $x_i,\ 1 \leq i \leq n+1$, are linearly independent if and only if x_i with $1 \leq i \leq n$ are linearly independent and x_{n+1} does not belong to the $K-$ subspace generated by $x_1, \ldots, x_n$.

b). Let V be a K–vector space which is not finitely generated. Construct recursively a linearly independent sequence $(x_n)_{n\in\mathbb{N}}$ of elements in V.

4.5. Let $U,\ W$ be free A-submodules of the A–module V. Further, let $x_i,\ i \in I$, resp. $y_j,\ j \in J$, be a basis of U resp. W. Show that $x_i,\ y_j,\ i \in I,\ j \in J$ together form a basis of $U + W$ if and only if $U \cap W = 0$.

4.6. a). A basis of a free module V over a non-zero ring A is a minimal generating system of the A–module V.

b). Every basis of a finite free module over a non-zero ring is finite.

4.7. Let A be a non-zero commutative ring. Show that A is a principal ideal domain if and only if every ideal in A is a free A–submodule of A. (**Remark :** In general this assertion is not true for non-commutative rings. Counter example!)

4.8. Let B be a ring and let A be a subring of B such that B is a free A–module. Show that $A^\times = A \cap B^\times$. Moreover, if B is a division ring, then so is A. (**Hint :** If $a \in A \cap B^\times$, then use $B = aB$.)

4.9. Let K be a division ring and let V be a K–vector space with basis $x_1, \ldots, x_n$. Further, let $y \in V$, $y = a_1x_1 + \cdots + a_nx_n$ with $a_i \in K$. Give necessary and sufficient condition on the coeficients $a_1, \ldots, a_n$ such that $x_1 - y, \ldots, x_n - y$ is a basis of V.

4.10. Let K be a field and let A be a subring of K such that every element of K can be expressed as a quotient a/b with $a, b \in A$, $b \neq 0$. (i.e. K is the quotient field of A). If K is a finite A–module, then prove that $A = K$. In particular, $\mathbb{Q}$ is not a finite $\mathbb{Z}$–module. (**Hint :** Suppose $K = Ax_1 + \cdots + Ax_n$ and $b \in A$, $b \neq 0$, with $bx_i \in A$ for $i = 1, \ldots, n$. Now, try to express $1/b^2$ as a linear combination of x_i.)

4.11. Let K be a division ring and A be a commutative subring of K such that K is a finite A–module. Show that A is a field. (**Hint :** Note that K contains a quotient field Q of A. Let $x_1, \ldots, x_m$ be a A-generating system of K and let $y_1, \ldots, y_n$ be a Q–basis of K with $y_1 = 1$. Then $y_1^*(x_1), \ldots, y_1^*(x_m)$ is an A– generating system of Q, where y_1^* is the first coordinate function with respect to the basis $y_1, \ldots, y_n$. Now use the above exercise 4.10.)

4.12. Let L be a division ring and let K be a sub-division ring of L. Further, let V_L be an L–vector space with the L–basis $x_1, \ldots, x_n$ and V be the K–vector space $Kx_1 + \cdots + Kx_n \subseteq V_L$. (For example: $V_L := L^n$; $x_1, \ldots, x_n$ is the standard basis; $V = K^n$.)

a). Show that : $y_1, \ldots, y_m \in V$ are linearly independent over K (resp. form a K–generating system of V resp. form a K–basis of V) if and only if they are linearly independent over L (resp. form a L–generating system of V_L resp. form a L–basis of V_L).

b). Let U be a K–subspace of V. Let U_L denote the L-subspace of V_L generated by U. Show that: $\mathrm{Dim}_K\, U = \mathrm{Dim}_L\, U_L$ and $U = V \cap U_L$. If W is another K–subspace of V, then $U \subseteq W$ (resp. $U = W$) if and only if $U_L \subseteq W_L$ (resp. $U_L = W_L$).

c). Prove the analogous assertions in the case V_L is not finite dimensional (over L).

4.13. Let K be a divison ring and let M be a maximal K–linear independent subset in the set of 0-1–sequences from $K^{\mathbb{N}}$. Show that : M has the cardinality of the continuum. (**Hint :** (In view of the exercise 4.11, we may assume that K is the quotient field of its prime ring $\mathbb{Z} \cdot 1_K$. Using cardinality arguments show that the dimension of the subspace generated by the 0-1–sequences in $K^{\mathbb{N}}$ is the cardinality of the continuum.)

4.14. Let x_i, $i \in I$, be a family of n–tuples from $\mathbb{Z}^n$. For a prime number p, let K_p denote a field with p elements. Show that the following statements are equivalent:

(i) The x_i are linearly independent over $\mathbb{Z}$.

(ii) The images of x_i, $i \in I$, in $\mathbb{Q}^n$, are linearly independent over $\mathbb{Q}$.

(iii) There exists a prime number p such that the images of x_i, $i \in I$, in K_p^n, are linearly independent over K_p.

(iv) For almost all prime numbers p, the images of x_i, $i \in I$, in K_p^n, are linearly independent over K_p.

— If $|I| = n$, then the above statements are further equivalent to the following statement:

(v) There exists a non-zero integer m such that $m\mathbb{Z}^n \subseteq \sum_{i \in I} \mathbb{Z}x_i$.

4.15. Let x_i, $i \in I$, be a family of n–tuples from $\mathbb{Z}^n$. For every prime number p let K_p denote a field with p elements. Show that the following statements are equivalent:

(i) The x_i, $i \in I$, generate (the $\mathbb{Z}$-module) $\mathbb{Z}^n$.

(ii) For every prime numebr p, the images of x_i, $i \in I$, in K_p^n, generate the K_p-vector space K_p^n.

(**Hint**: ((ii) $\Rightarrow$ (i): Let $U := \sum_{i\in I} \mathbb{Z}x_i$. Note that by exercise 4.13, there exists a non-zero integer m with $m\mathbb{Z}^n \subseteq U$. Further: to every prime number p and every $x \in \mathbb{Z}^n$ there exist $x' \in U$, $y \in \mathbb{Z}^n$ such that $x = x' + py$, i.e. $\mathbb{Z}^n \subseteq U + p\mathbb{Z}^n$ for every prime number p. From this deduce that $U = \mathbb{Z}^n$.)

4.16. Let V be a vector space and let U_1, U_2 be subspaces of V. Then there exists a basis x_i, $i \in I$, of V satisfying the following property: for given subsets I_1, I_2 of I, if x_i, $i \in I_1 \cap I_2$, is a basis $U_1 \cap U_2$, x_i, $i \in I_1$, a basis of U_1 and x_i, $i \in I_2$, a basis of U_2, then x_i, $i \in I_1 \cup I_2$, is a basis of $U_1 + U_2$. (**Hint**: Proceed as in the proof in the finite dimensional case. – **Remark**: Therefore the dimension formula also holds for not finite dimensional subspaces U, W.)

4.17. Let I be a non-empty open interval in $\mathbb{R}$ and let $\mathrm{C}^{\omega}_{\mathbb{R}}(I)$ (respectively, $\mathrm{C}^{0}_{\mathbb{R}}(I)$) be the $\mathbb{R}$-vector space of all real-analytic[1]) (respectively, continuous) real-valued functions on I. Then $\mathrm{C}^{\omega}_{\mathbb{R}}(I) \subsetneq \mathrm{C}^{0}_{\mathbb{R}}(I)$ and if U is a $\mathbb{R}$-subspace of $\mathrm{C}^{0}_{\mathbb{R}}(I)$ with $\mathrm{C}^{\omega}_{\mathbb{R}}(I) \subseteq U$, then show that $\mathrm{Dim}_{\mathbb{R}}\, U$ is the cardinality of the continuum. (**Hint**: Without loss of generality let $I =]-1, 1[$. Let $(a_{ij})_{i\in\mathbb{N}}$, $j \in J$, be a linearly independent family of 0-1–sequences in $\mathbb{R}^{\mathbb{N}}$, where $|J| = \aleph := |\mathbb{R}|$, see Exercise 4.13. Then the functions $t \mapsto \sum_{i\geq 0} a_{ij}t^i$, $j \in J$, in $\mathrm{C}^{\omega}_{\mathbb{R}}(I)$ are linearly independent over $\mathbb{R}$. **Alternative hint**: the family of the functions $t \mapsto \exp(at)$, $a \in \mathbb{R}$, on I is linearly independent. Similarly, the rational functions $t \mapsto 1/(t-a)$, $a \in \mathbb{R}$, $|a| \geq 1$, are linearly independent in $\mathrm{C}^{\omega}_{\mathbb{R}}(]-1, 1[)$.) Prove the analogous results for the complex vector space $\mathrm{H}(U)$ of holomorphic functions defined on a domain $U \subseteq \mathbb{C}$.

4.18. For a given $n \in \mathbb{N}$, let $a_1, \ldots, a_n \in K$ be n distinct elements in a field K. Then the sequences $g_i := (a_i^{\nu})_{\nu\in\mathbb{N}} \in K^{\mathbb{N}}$, $i = 1, \ldots, n$, are linearly independent over K. (**Hint**: Suppose that the g_i are linearly dependent. Without loss of generality we may assume that $\mathrm{Dim}_K(\mathrm{Rel}_K(g_1, \ldots, g_n)) = 1$, see exercise T4.7. Let $(b_1, \ldots, b_n)$ be a basis element of relations. Then the element $(b_1a_1, \ldots, b_na_n)$ is also a relation of the g_i. This is a contradiction.)

4.19. Let K be a field and let I be an infinite set. Then $\mathrm{Dim}_K(K^I) = |K^I|$. (**Hint**: (In view of[2]), it is enough to prove that $|K| \leq \mathrm{Dim}_K K^I$. Let $\sigma : \mathbb{N} \to I$ be injective and for $a \in K$, let g_a denote the I–tuple with $(g_a)_{\sigma(\nu)} := a^{\nu}$ for $\nu \in \mathbb{N}$ and $(g_a)_i := 0$ for $i \in I \setminus \mathrm{im}\,\sigma$. Then by exercise 4.18, $(g_a)_{a\in K}$ are linearly independent.) Deduce that $\mathrm{Dim}_K K^I > \mathrm{Dim}_K K^{(I)}$. – **Remark**: This dimension formula for K^I is also valid for division rings K. Proof!.)

4.20. Let K be a division ring. Further, let $x_i = (a_{i1}, \ldots, a_{in}) \in K^n$, $i = 1, \ldots, n$. With the j–th components of this n–tuple we form the new n–tuples $y_j := (a_{1j}, \ldots, a_{nj})$, $j = 1, \ldots, n$. Show that : the elements $x_1, \ldots, x_n$ of the K–*Left*-vector space K^n are linearly independent if and only if the elements $y_1, \ldots, y_n$ of the K–*right*-vector space K^n are linearly independent. (**Hint**: Suppose that $x_1, \ldots, x_n$ are linearly independent and $y_1b_1 + \cdots + y_nb_n = 0$, $b_j \in K$. Then $x_1, \ldots, x_n \in \mathrm{Rel}_K(b_1, \ldots, b_n)$, and a dimension argument shows that $\mathrm{Rel}_K(b_1, \ldots, b_n) = K^n$, this means $b_1 = \cdots = b_n = 0$.)

4.21. Let K be a division ring, I be a set and let $f_1, \ldots, f_n \in K^I$, $n \in \mathbb{N}$. The following statements are equivalent:

(i) The $f_1, \ldots, f_n$ are linearly independent over K.

(ii) There exists a subset $J \subseteq I$ such that $|J| = n$ and that the restrictions $f_1|J, \ldots, f_n|J \in K^J$ are linearly independent (and hence form a basis of K^J).

(iii) The value –n–tuples $(f_1(i), \ldots, f_n(i)) \in K^n$, $i \in I$, generate K^n as a K–*right*-vector space.

(**Hint**: The implication (i) $\Rightarrow$ (ii) can be proved by induction on n: Suppose that there exists a subset $J' \subseteq I$ with $(n-1)$–elements is found for $f_1, \ldots, f_{n-1}$ such that $f_1|J', \ldots, f_{n-1}|J'$ are linearly independent over K and so

[1]) A function $f : I \to \mathbb{R}$ is called real-analytic at $a \in I$, if there exist a open neighbourhood U of a and a convergent power series $\sum_{i=0}^{\infty} a_i(x-a)^i$ such that $f(x) = \sum_{i=0}^{\infty} a_i(x-a)^i$ for all $x \in U \cap I$. A function $f : I \to \mathbb{R}$ is called real-analytic if it is real-analytic at every $a \in I$.

[2]) Let A be a ring and let V be a free A–module of infinite rank. Then $|V| = |A| \cdot \mathrm{rank}_A\, V = \mathrm{Sup}\{|A|, \mathrm{rank}_A\, V\}$.

form a basis of $K^{J'}$. Then $f_n|J' = a_1(f_1|J') + \cdots + a_{n-1}(f_{n-1}|J')$ with $a_1, \ldots, a_{n-1} \in K$. Now, by (i) there exists an element $j \in I \smallsetminus J'$ such that $f_n(j) \neq a_1 f_1(j) + \cdots + a_{n-1} f_{n-1}(j)$. Now, choose $J := J' \cup \{j\}$. — For the equivalence (ii) $\Leftrightarrow$ (iii) use the exercise 4.20.)

4.22. Let K be a division ring and let $a_1, \ldots, a_n \in K$. Let $g_i := (a_i^\nu)_{\nu \in \mathbb{N}} \in K^{\mathbb{N}}$ and $f_i := (1, a_i, \ldots, a_i^{n-1}) \in K^n$, $i = 1, \ldots, n$. Then $g_1, \ldots, g_n$ are linearly independent over K if and only if $f_1, \ldots, f_n$ are linearly independent over K. (**Hint:** Let $h_j := (a_1^j, \ldots, a_n^j) \in K^n$, $j \in \mathbb{N}$. Note that $f_i = g_i|\{0, \ldots, n-1\}$ and $(f_1(j), \ldots, f_n(j)) = (g_1(j), \ldots, g_n(j)) = h_j$ for all $j = 1, \ldots, n$. Therefore by exercise 4.21, $g_1, \ldots, g_n$ are linearly independent if and only if h_j, $j = 1, \ldots, n$ generates the *right*-vector space K^n.Suppose that the elements $h_0, \ldots h_m$ are linearly independent in the K*–right* - vector space K^n, but the elements $h_0, \ldots, h_{m+1}$ are not linearly independent, so h_{m+1} and hence h_j for every $j \geq m+1$ is a linear combination of $h_0, \ldots, h_m$. Now again use the exercise 4.21.)

4.23. Let K be a field and let $b_0, \ldots, b_m$ be elements of K, all of which are not equal to 0. Then there exist atmost m distinct elements $x \in K$, which satisfy the equation

$$0 = b_0 \cdot 1 + b_1 x + \cdots + b_m x^m .$$

(**Hint:** If $x_1, \ldots, x_{m+1}$ are distinct elements in K, then by exercises 4.18 and 4.22, the elements $h_j := (x_1^j, \ldots, x_{m+1}^j)$, $0 \leq j \leq m$, are linearly independent over K. — **Remark:** The same result is also true for integral domains, since every integral domain is contained in a field, for example, in its quotient field. With the help of concept of polynomials the above assertion can be formulated as: *A non-zero polynomial of degree $\leq m$ over a field (or an integral domain) K has atmost m zeros in K.)*

Below one can see (simple) test-exercises.

Test-Exercises

T4.1. Let A be a ring. The element $a \in A$ is a basis of the A–module A, if and only if a is a unit in A.

T4.2. For every natural number $m \geq 1$, give a minimal generating system for the $\mathbb{Z}$–module $\mathbb{Z}$ consisting of m elements. **T4.3. a).** The elements $1, a \in \mathbb{R}$ are linearly independent over $\mathbb{Q}$, if and only if a is irrational (i.e. not rational). (**Remark:** Two real numbers b, c, which are linearly independent over $\mathbb{Q}$ are called incommensurable. Classical example: the length of the side and the length of the diagonal of a square are incommensurable, since the real number $\sqrt{2} \in \mathbb{R}$ is irrational.)

b). Let P be the set of all prime numbers $p \in \mathbb{N}^*$. Show that the family $(\log p)_{p \in \mathrm{P}}$ is linearly independent over $\mathbb{Q}$.

T4.4. Let $a, b \in \mathbb{N}^*$ and $d := \gcd(a, b)$. Then the relation submodule $\mathrm{Rel}_{\mathbb{Z}}(a, b)$ of $\mathbb{Z}^2$ is generated by $(bd^{-1}, -ad^{-1}) \in \mathbb{Z}^2$.

T4.5. In the subspace U of the $\mathbb{R}$–vector space $\mathbb{R}^{\mathbb{R}}$ of all funktions from $\mathbb{R}$ into itself, generated by the functions $x \mapsto \sin(x+a)$, $a \in \mathbb{R}$, show that the two functions $x \mapsto \sin x$, $x \mapsto \cos x (= \sin(x + \pi/2))$ form a basis of U.

T4.6. Every $\mathbb{Q}$–vector space $V \neq 0$ is not free over the subring $\mathbb{Z}$ of $\mathbb{Q}$.

T4.7. Let $n \in \mathbb{N}$ and let $x_1, \ldots, x_{n+1} \in V$ be linearly independent elements of a vector space V over the division ring K. Suppose that n elements among $x_1, \ldots, x_{n+1}$ are linearly independent over K. Show that $\mathrm{Dim}_K(\mathrm{Rel}_K(x_1, \ldots, x_{n+1})) = 1$.

T4.8. Let K be a divison ring, V be a finite dimensional K–vector space and let V_i, $i \in I$, be a family of subspaces of V. Then there exists a finite subset J of I such that $\bigcap_{i \in I} V_i = \bigcap_{i \in J} V_i$ and $\sum_{i \in I} V_i = \sum_{i \in J} V_i$.

T4.9. Let K be a division ring and let V be not finite dimensional K–vector space. Construct an infinite sequences $U_0 \subset U_1 \subset \cdots \subset U_i \subset \cdots$ and $W_0 \supset W_1 \supset \cdots \supset W_i \supset \cdots$ of subspaces of V.

T4.10. Let I be a non-empty open interval in $\mathbb{R}$ and let $\mathrm{C}^0_{\mathbb{R}}(I)$ be the $\mathbb{R}$-vector space of all continuous real-valued functions on I. Show that $|\mathrm{C}^0_{\mathbb{R}}(I)| = |\mathbb{R}|$. (**Hint:** The map $\mathrm{C}^0_{\mathbb{R}}(I) \to \mathbb{R}^{\mathbb{Q}}$ defined by $f \mapsto f|\mathbb{Q}$ is injective.)

T4.11. Let A be a ring $\neq 0$ with finitely many elements and let V be an A–module with a generating system of n elements, $n \in \mathbb{N}$. Show that every $n+1$ elements of V are linearly dependent. (**Hint:** Proceed as in the Example given in the class which uses only cardinality argument.)

T4.12. What is the rank of $\mathbb{Q}$ as an abelian group?

T4.13. Let A be an integral domain (which is contained in a field Q). Further, let U be a subgroup of the unit group $A^\times$ of A with an exponent[3]) $m \neq 0$. Then U is cyclic (and finite). In particular, every finite subgroup of $A^\times$ is cyclic; further, the unit group of every finite field (for example, the unit group of a prime ring of characteristic p, p prime, is cyclic.) (**Hint:** The equation $x^m = 1$ has atmost m solutions in A by exercise 4.23. Now use [4]).)

T4.14. Let K be a field, I be a set and let $g \in K^I$ be a function on I into K, such that the image $\mathrm{im}(g)$ is an infinite subset of K. Then the powers g^ν, $\nu \in \mathbb{N}$ of g are linearly independent ovwer K. (For example from this it follows that: the functions $t \mapsto \cos^\nu t$, $\nu \in \mathbb{N}$, from $\mathbb{R}$ to itself are linearly independent; similarly, the functions $x \mapsto x^\nu$, $\nu \in \mathbb{N}$, from K to itself for an arbitrary infinite field K, are linearly independent.)

T4.15. Let L be a division ring, K be a subdivision ring of L and I be a set. For an arbitrary family $(f_j)_{j\in J}$ of functions $f_j \in K^I$ show that: the f_j, $j \in J$, are linearly independent over K if and only if they are linearly independent over L as a family of functions in L^I. (Use the exercise 6 and and exercise 4.12(a).)

T4.16. Let A be a ring and let J be an indexed set with cardinality of the continuum. Then there exists a family x_j, $j \in J$, of A–linearly independent 0-1–sequences in $A^{\mathbb{N}}$. (**Hint:** (H. Brenner) Let P be the set of prime numbers. For a subset $R \subseteq \mathrm{P}$, let $\mathrm{N}(R)$ be the set of those positive natural numbers whose prime divisors belong to R, i.e. $\mathrm{N}(R) = \{n \in \mathbb{N}^* \mid$ prime divisors of $n \subseteq R\}$. Then the family x_R, $R \in \mathfrak{P}(\mathrm{P})$, is linearly independent, where x_R denote the indicator function of $\mathrm{N}(R)$.)

† **Johann Carl Friedrich Gauss (1777-1855)** was born on 30 April 1777 in Brunswick, Duchy of Brunswick (now Germany) and died on 23 Feb 1855 in Göttingen, Hanover (now Germany).

At the age of seven, Carl Friedrich Gauss started elementary school, and his potential was noticed almost immediately. His teacher, Büttner, and his assistant, Martin Bartels, were amazed when Gauss summed the integers from 1 to 100 instantly by spotting that the sum was 50 pairs of numbers each pair summing to 101.

In 1788 Gauss began his education at the Gymnasium with the help of Büttner and Bartels, where he learnt High German and Latin. After receiving a stipend from the Duke of Brunswick- Wolfenbüttel, Gauss entered Brunswick Collegium Carolinum in 1792. At the academy Gauss independently discovered Bode's law, the binomial theorem and the arithmetic- geometric mean, as well as the law of quadratic reciprocity and the prime number theorem.

In 1795 Gauss left Brunswick to study at Göttingen University. Gauss's teacher there was Kaestner, whom Gauss often ridiculed. His only known friend amongst the students was Farkas Bolyai. They met in 1799 and corresponded with each other for many years.

Gauss left Göttingen in 1798 without a diploma, but by this time he had made one of his most important discoveries - the construction of a regular 17-gon by ruler and compasses This was the most major advance in this field since the time of Greek mathematics and was published as Section VII of Gauss's famous work, Disquisitiones Arithmeticae.

Gauss returned to Brunswick where he received a degree in 1799. After the Duke of Brunswick had agreed to continue Gauss's stipend, he requested that Gauss submit a doctoral dissertation to the University of Helmstedt. He already knew Pfaff, who was chosen to be his advisor. Gauss's dissertation was a discussion of the fundamental theorem of algebra.

With his stipend to support him, Gauss did not need to find a job so devoted himself to research. He published the book Disquisitiones Arithmeticae in the summer of 1801. There were seven sections, all but the last section, referred to above, being devoted to number theory.

In June 1801, Zach, an astronomer whom Gauss had come to know two or three years previously, published the orbital positions of Ceres, a new "small planet" which was discovered by G Piazzi, an Italian astronomer on 1 January, 1801. Unfortunately, Piazzi had only been able to observe 9 degrees of its orbit before it disappeared behind the Sun. Zach published several predictions of its position, including one by Gauss which differed greatly from the others. When Ceres was rediscovered by Zach on 7 December 1801 it was almost exactly where Gauss had predicted. Although he did not disclose his methods at the time, Gauss had used his least squares approximation method.

[3]) **Exponent of a group.** Let G be a group with neutral element e. Then the set of integers n with $a^n = e$ for all $a \in G$ forms a subgroup U_G of the additive group of $\mathbb{Z}$, i.e. $U_G := \{n \in \mathbb{Z} \mid a^n = e \text{ for all } a \in G\}$ and hence there is a unique $m \in \mathbb{N}$ such that $U_G = \mathbb{Z}m$. This natural number m is called the exponent of G and usually denoted by $\mathrm{Exp}G$. For example, if G is a finite cyclic group, then $\mathrm{Exp}G = \mathrm{Ord}G$; $\mathrm{Exp}\mathfrak{S}_3 = \mathrm{Ord}\mathfrak{S}_3$; In general: $\mathrm{Exp}G$ *and* $\mathrm{Ord}G$ *have the same prime divisors.* (proof!).

[4]) **Exercise on groups.** Let G be a finite group with neutral elements e. Suppose that for every divisor $d \in \mathbb{N}^*$ of the order $\mathrm{Ord}G$ there are atmost d elements $x \in G$ such that $x^d = e$. Then G is a cyclic group.

In June 1802 Gauss visited Olbers who had discovered Pallas in March of that year and Gauss investigated its orbit. Olbers requested that Gauss be made director of the proposed new observatory in Göttingen, but no action was taken. Gauss began corresponding with Bessel, whom he did not meet until 1825, and with Sophie Germain.

Gauss married Johanna Ostoff on 9 October, 1805. Despite having a happy personal life for the first time, his benefactor, the Duke of Brunswick, was killed fighting for the Prussian army. In 1807 Gauss left Brunswick to take up the position of director of the Göttingen observatory. Gauss arrived in Göttingen in late 1807. In 1808 his father died, and a year later Gauss's wife Johanna died after giving birth to their second son, who was to die soon after her. Gauss was shattered and wrote to Olbers asking him give him a home for a few weeks, to gather new strength in the arms of your friendship - strength for a life which is only valuable because it belongs to my three small children.

Gauss was married for a second time the next year, to Minna the best friend of Johanna, and although they had three children, this marriage seemed to be one of convenience for Gauss.

Gauss's work never seemed to suffer from his personal tragedy. He published his second book, Theoria motus corporum coelestium in sectionibus conicis Solem ambientium, in 1809, a major two volume treatise on the motion of celestial bodies. In the first volume he discussed differential equations, conic sections and elliptic orbits, while in the second volume, the main part of the work, he showed how to estimate and then to refine the estimation of a planet's orbit. Gauss's contributions to theoretical astronomy stopped after 1817, although he went on making observations until the age of 70.

Much of Gauss's time was spent on a new observatory, completed in 1816, but he still found the time to work on other subjects. His publications during this time include Disquisitiones generales circa seriem infinitam, a rigorous treatment of series and an introduction of the hypergeometric function, Methodus nova integralium valores per approximationem inveniendi, a practical essay on approximate integration, Bestimmung der Genauigkeit der Beobachtungen, a discussion of statistical estimators, and Theoria attractionis corporum sphaeroidicorum ellipticorum homogeneorum methodus nova tractata. The latter work was inspired by geodesic problems and was principally concerned with potential theory. In fact, Gauss found himself more and more interested in geodesy in the 1820s.

Gauss had been asked in 1818 to carry out a geodesic survey of the state of Hanover to link up with the existing Danish grid. Gauss was pleased to accept and took personal charge of the survey, making measurements during the day and reducing them at night, using his extraordinary mental capacity for calculations. He regularly wrote to Schumacher, Olbers and Bessel, reporting on his progress and discussing problems.

Because of the survey, Gauss invented the heliotrope which worked by reflecting the Sun's rays using a design of mirrors and a small telescope. However, inaccurate base lines were used for the survey and an unsatisfactory network of triangles. Gauss often wondered if he would have been better advised to have pursued some other occupation but he published over 70 papers between 1820 and 1830.

In 1822 Gauss won the Copenhagen University Prize with Theoria attractionis... together with the idea of mapping one surface onto another so that the two are similar in their smallest parts. This paper was published in 1825 and led to the much later publication of Untersuchungen über Gegenstände der Höheren Geodäsie (1843 and 1846). The paper Theoria combinationis observationum erroribus minimis obnoxiae (1823), with its supplement (1828), was devoted to mathematical statistics, in particular to the least squares method.

From the early 1800s Gauss had an interest in the question of the possible existence of a non-Euclidean geometry. He discussed this topic at length with Farkas Bolyai and in his correspondence with Gerling and Schumacher. In a book review in 1816 he discussed proofs which deduced the axiom of parallels from the other Euclidean axioms, suggesting that he believed in the existence of non-Euclidean geometry, although he was rather vague. Gauss confided in Schumacher, telling him that he believed his reputation would suffer if he admitted in public that he believed in the existence of such a geometry.

In 1831 Farkas Bolyai sent to Gauss his son János Bolyai's work on the subject. Gauss replied *to praise it would mean to praise myself*. Again, a decade later, when he was informed of Lobachevsky's work on the subject, he praised its "genuinely geometric" character, while in a letter to Schumacher in 1846, states that he had the same convictions for 54 years indicating that he had known of the existence of a non-Euclidean geometry since he was 15 years of age (this seems unlikely).

Gauss had a major interest in differential geometry, and published many papers on the subject. Disquisitiones generales circa superficies curva (1828) was his most renowned work in this field. In fact, this paper rose from his geodesic interests, but it contained such geometrical ideas as Gaussian curvature. The paper also includes Gauss's famous theorema egregrium: *If an area in* $\mathbb{R}^3$ *can be developed (i.e. mapped isometrically) into another area of* $\mathbb{R}^3$ *, the values of the Gaussian curvatures are identical in corresponding points.*

The period 1817-1832 was a particularly distressing time for Gauss. He took in his sick mother in 1817, who stayed until her death in 1839, while he was arguing with his wife and her family about whether they should go to Berlin. He had been offered a position at Berlin University and Minna and her family were keen to move there. Gauss, however, never liked change and decided to stay in Göttingen. In 1831 Gauss's second wife died after a long illness.

In 1831, Wilhelm Weber arrived in Göttingen as physics professor filling Tobias Mayer's chair. Gauss had known Weber since 1828 and supported his appointment. Gauss had worked on physics before 1831, publishing Über ein neues allgemeines Grundgesetz der Mechanik, which contained the principle of least constraint, and Principia generalia theoriae figurae fluidorum in statu aequilibrii which discussed forces of attraction. These papers were based on Gauss's potential theory, which proved of great importance in his work on physics. He later came to believe his potential theory and his method of least squares provided vital links between science and nature.

In 1832, Gauss and Weber began investigating the theory of terrestrial magnetism after Alexander von Humboldt attempted to obtain Gauss's assistance in making a grid of magnetic observation points around the Earth. Gauss was excited by this prospect and by 1840 he had written three important papers on the subject: Intensitas vis magneticae terrestris ad mensuram absolutam revocata (1832), Allgemeine Theorie des Erdmagnetismus (1839) and Allgemeine Lehrsätze in Beziehung auf die im verkehrten Verhältnisse des Quadrats der Entfernung wirkenden Anziehungs- und Abstossungskräfte (1840). These papers all dealt with the current theories on terrestrial magnetism, including Poisson's ideas, absolute measure for magnetic force and an empirical definition of terrestrial magnetism. Dirichlet's principle was mentioned without proof.

Allgemeine Theorie... showed that there can only be two poles in the globe and went on to prove an important theorem, which concerned the determination of the intensity of the horizontal component of the magnetic force along with the angle of inclination. Gauss used the Laplace equation to aid him with his calculations, and ended up specifying a location for the magnetic South pole.

Humboldt had devised a calendar for observations of magnetic declination. However, once Gauss's new magnetic observatory (completed in 1833 - free of all magnetic metals) had been built, he proceeded to alter many of Humboldt's procedures, not pleasing Humboldt greatly. However, Gauss's changes obtained more accurate results with less effort.

Gauss and Weber achieved much in their six years together. They discovered Kirchhoff's laws, as well as building a primitive telegraph device which could send messages over a distance of 5000 ft. However, this was just an enjoyable pastime for Gauss. He was more interested in the task of establishing a world-wide net of magnetic observation points. This occupation produced many concrete results. The Magnetischer Verein and its journal were founded, and the atlas of geomagnetism was published, while Gauss and Weber's own journal in which their results were published ran from 1836 to 1841.

In 1837, Weber was forced to leave Göttingen when he became involved in a political dispute and, from this time, Gauss's activity gradually decreased. He still produced letters in response to fellow scientists' discoveries usually remarking that he had known the methods for years but had never felt the need to publish. Sometimes he seemed extremely pleased with advances made by other mathematicians, particularly that of Eisenstein and of Lobachevsky.

Gauss spent the years from 1845 to 1851 updating the Göttingen University widow's fund. This work gave him practical experience in financial matters, and he went on to make his fortune through shrewd investments in bonds issued by private companies.

Two of Gauss's last doctoral students were Moritz Cantor and Dedekind. Dedekind wrote a fine description of his supervisor *... usually he sat in a comfortable attitude, looking down, slightly stooped, with hands folded above his lap. He spoke quite freely, very clearly, simply and plainly: but when he wanted to emphasise a new viewpoint ... then he lifted his head, turned to one of those sitting next to him, and gazed at him with his beautiful, penetrating blue eyes during the emphatic speech. ... If he proceeded from an explanation of principles to the development of mathematical formulas, then he got up, and in a stately very upright posture he wrote on a blackboard beside him in his peculiarly beautiful handwriting: he always succeeded through economy and deliberate arrangement in making do with a rather small space. For numerical examples, on whose careful completion he placed special value, he brought along the requisite data on little slips of paper.*

Gauss presented his golden jubilee lecture in 1849, fifty years after his diploma had been granted by Hemstedt University. It was appropriately a variation on his dissertation of 1799. From the mathematical community only Jacobi and Dirichlet were present, but Gauss received many messages and honours.

From 1850 onwards Gauss's work was again of nearly all of a practical nature although he did approve Riemann's doctoral thesis and heard his probationary lecture. His last known scientific exchange was with Gerling. He discussed a modified Foucalt pendulum in 1854. He was also able to attend the opening of the new railway link between Hanover and Göttingen, but this proved to be his last outing. His health deteriorated slowly, and Gauss died in his sleep early in the morning of 23 February, 1855.