Jordan algebras

Jordan algebras were introduced by Jordan, von Neumann and Wigner (in a paper published in Annals of Mathematics in 1934) with the aim that this new algebraic system would give a better interpretation of quantum mechanics. This aim was not achieved, but Jordan algebras became an interesting topic.

An algebra J is a ***Jordan algebra*** if $xy = yx$ and $(x^2y)x = x^2(yx)$, for all $x,\ y \in J$. Any Jordan algebra is power-associative.

Let A be an associative or an alternative algebra. If we replace the multiplication xy in A by the ***Jordan product*** $x \circ y = \frac{1}{2}(xy + yx)$ (cf. Section C.24), we obtain a Jordan algebra denoted by $A^{(+)}$.

Let V be a vector space over F, $f\colon V \times V \to F$ a symmetric bilinear form, and $J(V, f) = F \oplus V$. With the multiplication $(\alpha + x)(\beta + y) = (\alpha\beta + f(x, y)) + (\beta x + \alpha y)$, the vector space $J(V, f)$ is a Jordan algebra.

Let A be an algebra with involution $^-\colon a \in A \to \overline{a} \in A$. Let $H(A, {}^-) = \{\, a \in A \mid \overline{a} = a \,\}$. If A is associative or alternative, then $H(A, {}^-)$ is a subalgebra of $A^{(+)}$, hence a Jordan algebra. For the matrix algebra $\mathrm{Mat}_{n\times n}(A)$, we consider the involution given by $\overline{(a_{ij})}^t = (\overline{a_{ji}})$ and the algebra $H(\mathrm{Mat}_{n\times n}(A), {}^{-t})$ that is not necessarily a Jordan algebra. In particular, if C is a Cayley-Dickson algebra and $^-$ denotes its involution, then $H(C, {}^-)$, $H(\mathrm{Mat}_{2\times 2}(C), {}^{-t})$ and $H(\mathrm{Mat}_{3\times 3}(C), {}^{-t})$ are Jordan algebras.

The Jordan algebra J is ***special*** if J is a subalgebra of $B^{(+)}$ for some associative algebra B. Otherwise, J is ***exceptional***. The Jordan algebras $A^{(+)}$, $J(V, f)$, $H(C, {}^-)$, and $H(\mathrm{Mat}_{2\times 2}(C), {}^{-t})$ are special. Also in 1934, Albert proved that $H(\mathrm{Mat}_{3\times 3}(C), {}^{-t})$ is exceptional. In 1956, Shirshov proved that any Jordan algebra with two generators is special, and since $H(\mathrm{Mat}_{3\times 3}(C), {}^{-t})$ has three generators, this result cannot be improved.

C.53.2 Theorem (Albert) *Let J be a finite-dimensional Jordan algebra. Then* $\mathrm{Nil}(J)$ *is nilpotent, and* $J/\mathrm{Nil}(J)$ *is isomorphic to a finite direct sum of simple algebras. Over an algebraically closed field F, each one of these simple algebras is isomorphic to one of the following algebras: F; $J(V, f)$, where f is nondegenerate; $H(\mathrm{Mat}_{n\times n}(A), {}^{-t})$, $n \geq 3$, where A is a composition algebra that is associative for $n > 3$.*

An ***Albert algebra*** is a Jordan algebra J over F such that (for some extension K of F) $J \otimes_F K \cong H(\mathrm{Mat}_{3\times 3}(C), {}^{-t})$. An Albert algebra is exceptional, simple, and has dimension 27 over its center.

C.53.3 Theorem (Zelmanov) *A simple Jordan algebra is isomorphic to one of the following algebras: $J(V, f)$, where f is nondegenerate; $A^{(+)}$, where A is a simple associative algebra; $H(A, {}^-)$, where A is a simple associative algebra with involution ${}^-$; an Albert algebra.*

As in the case of alternative algebras, we can define the quasi-regular radical $\mathrm{Rad}(J)$ of a Jordan algebra J. A subspace K of J is a ***quadratic ideal*** if $2(ka)k - k^2a \in K$ for all $k \in K$ and $a \in J$.

C.53.4 Theorem *Let J be a Jordan algebra. Suppose that J satisfies the minimal condition for quadratic ideals. Then we have:*

(1) (Slinko-Zelmanov) *The radical* $\mathrm{Rad}(J)$ *is nilpotent and has finite dimension.*

(2) (Jacobson-Osborn) *The quotient algebra* $J/\mathrm{Rad}(J)$ *is isomorphic to a finite direct sum of simple Jordan algebras of one of the following forms: a division Jordan algebra; $H(A,^-)$, where A is an associative Artinian algebra with involution ${}^-$, and A is ${}^-$-simple (i.e., A does not contain proper ideals I such that $\overline{I} \subset I$); $J(V, f)$ for f nondegenerate; an Albert algebra.*

For more information, see (Jacobson 1968, Kuzmin and Shestakov 1994, Zhevlakov, Slinko, Shestakov, and Shirshov 1982, Schafer 1995, Lyubich 1992).

C.54 Computational Ring Theory

by Franz Winkler in Linz, Austria

Whenever R is a ring, then by R^* we denote $R \setminus \{0\}$.

C.54.1 Definition A ***Euclidean domain*** D is a commutative integral domain together with a ***degree function*** $\deg\colon D^* \to \mathbb{N}_0$, such that

(1) $\deg(a \cdot b) \geq \deg(a)$ for all $a, b \in D^*$,

(2) (division property) for all $a, b \in D$, $b \neq 0$, there exists a ***quotient*** q and a ***remainder*** r in D such that $a = q \cdot b + r$ and ($r = 0$ or $\deg(r) < \deg(b)$).

Any Euclidean domain is a unique factorization domain.

C.54.2 Theorem *Any two non-zero elements a, b of a Euclidean domain D have a greatest common divisor g which can be written as a linear combination $g = s \cdot a + t \cdot b$ for some $s, t \in D$.*

The elements s, t in the previous theorem are called the ***Bézout cofactors*** of a and b.

A Euclidean domain in which quotient and remainder are computable by algorithms QUOT and REM admits an algorithm for computing the greatest common divisor g of any two elements a, b. This algorithm has originally been stated by Euclid for the domain of the integers. In fact, it can be easily extended to compute not only the gcd but also the Bézout cofactors.

Algorithm 1 Extended Euclidean algorithm

Require: a, b are elements of the Euclidean domain D;
Ensure: g is the greatest common divisor of a, b and $g = s \cdot a + t \cdot b$;
1: $(r_0, r_1, s_0, s_1, t_0, t_1) := (a, b, 1, 0, 0, 1)$;
2: $i := 1$;
3: **while** $r_i \neq 0$ **do**
4: $\quad q_i := \mathrm{QUOT}(r_{i-1}, r_i)$;
5: $\quad (r_{i+1}, s_{i+1}, t_{i+1}) := (r_{i-1}, s_{i-1}, t_{i-1}) - q_i \cdot (r_i, s_i, t_i)$;
6: $\quad i := i + 1$;
7: **end while**
8: $(g, s, t) := (r_{i-1}, s_{i-1}, t_{i-1})$;

In a Euclidean domain we can solve the ***Chinese remainder problem (CRP):***
given: $r_1, \ldots, r_n \in D$ (remainders)
$\quad m_1, \ldots, m_n \in D^*$ (moduli), pairwise relatively prime
find: $r \in D$, such that $r \equiv r_i \bmod m_i$ for $1 \leq i \leq n$.

There are basically two solution methods for the CRP. The first one is usually associated with the name of J. L. Lagrange. The second one is associated with I. Newton and is a recursive solution.

In the Lagrangian solution one first determines u_{kj} such that $1 = u_{kj} \cdot m_k + u_{jk} \cdot m_j$, for $1 \leq j, k \leq n, j \neq k$. This can obviously be achieved by the extended Euclidean algorithm. Next one considers the elements $l_k := \prod_{j=1, j\neq k}^{n} u_{jk} m_j$, for $1 \leq k \leq n$. Clearly $l_k \equiv 0 \bmod m_j$ for all $j \neq k$. On the other hand $l_k = \prod_{j=1, j\neq k}^{n} (1 - u_{kj} m_k) \equiv 1 \bmod m_k$. So $r = \sum_{k=1}^{n} r_k \cdot l_k$ solves CRP.

The disadvantage of the Lagrangian approach is that it yields a static algorithm, i.e., it is virtually impossible to increase the size of the problem by one more pair r_{n+1}, m_{n+1} without having to recompute everything from the start.

The Newton approach is recursive in the sense that one first solves the problem with 2 remainders and 2 moduli, yielding the solution $r_{1,2}$, and then has to solve the problem with remainders $r_{1,2}, r_3, \ldots, r_n$ and moduli $m_1 \cdot m_2, m_3, \ldots, m_n$. So for given remainders r_1, r_2 and moduli m_1, m_2 we want to find an $r \in D$ such that $r \equiv r_i \bmod m_i$ for $i = 1, 2$. The solution of this CRP of size 2 is computed by the Chinese remainder algorithm CRA.

Algorithm 2 Chinese remainder algorithm(Newtonian solution of the CRP)

Require: r_1, r_2, m_1, m_2 are elements of the Euclidean domain D, m_1, m_2 are non-zero and relatively prime;
Ensure: $r \equiv r_1 \bmod m_1$ and $r \equiv r_2 \bmod m_2$;
1: $c := m_1^{-1} \bmod m_2$;
2: $r_1' := r_1 \bmod m_1$;
3: $\sigma := (r_2 - r_1')c \bmod m_2$;
4: $r := r_1' + \sigma m_1$;

A special case of the CRP in the polynomial ring $K[x]$, K a field, is the ***interpolation problem***. All the moduli m_i are linear polynomials of the form $x - \beta_i$.
given: $\alpha_1, \ldots, \alpha_n \in K$,
$\beta_1, \ldots, \beta_n \in K$, such that $\beta_i \neq \beta_j$ for $i \neq j$,
find: $u(x) \in K[x]$, such that $u(\beta_i) = \alpha_i$ for $1 \leq i \leq n$.

Since $p(x) \bmod (x-\beta) = p(\beta)$ for $\beta \in K$, the interpolation problem is a special case of the CRP. The inverse of $p(x)$ in $K[x]_{/\langle x-\beta \rangle}$ is $p(\beta)^{-1}$. So CRA yields a solution algorithm for the interpolation problem, namely the Newton interpolation algorithm. Similarly, the Lagrangian solution to the CRP leads to a Lagrangian solution of the interpolation problem.

The Chinese remainder problem can, in fact, be described in greater generality. Let R be a commutative ring with unity. The abstract Chinese remainder problem is the following:

given $r_1, \ldots, r_n \in R$ (remainders),
$I_1, \ldots, I_n$ ideals in R (moduli), such that $I_i + I_j = R$ for all $i \neq j$;

find $r \in R$, such that $r \equiv r_i \bmod I_i$, for $1 \leq i \leq n$.

The abstract Chinese remainder problem can be treated basically in the same way as the CRP over Euclidean domains. Again there is a Lagrangian and a Newtonian approach and one can show that the problem

always has a solution and if r is a solution then the set of all solutions is given by $r + I_1 \cap \cdots \cap I_n$. i.e., the map $\varphi\colon r \mapsto (r + I_1, \ldots, r + I_n)$ is a homomorphism from R onto $\prod_{j=1}^{n} R_{/I_j}$ with kernel $I_1 \cap \cdots \cap I_n$. However, in the absence of the Euclidean algorithm it is not possible to compute a solution of the abstract CRP. See (Lauer, 1983).

Instead of solving a problem in several homomorphic images and then combining these modular solutions to a solution of the original problem by the Chinese remainder algorithm, one can also attempt to solve a problem in one homomorphic image, say modulo an ideal I, and then *lift* this solution to a solution modulo I^t, for high enough t. The basis for such an approach is the Lifting Theorem.

C.54.3 Theorem (***Lifting Theorem***) *Let I be the ideal generated by $p_1, \ldots, p_l$ in the commutative ring with unity R, $f_1, \ldots, f_n \in R[x_1, \ldots, x_r]$, $r \geq 1$, and $a_1, \ldots, a_r \in R$ such that $f_i(a_1, \ldots, a_r) \equiv 0 \pmod{I}$ for $i = 1, \ldots, n$. Let U be the Jacobian matrix of $f_1, \ldots, f_n$ evaluated at $(a_1, \ldots, a_r)$, i.e., $U = (u_{ij})$, where $u_{ij} = \partial f_i / \partial x_j (a_1, \ldots, a_r)$. Assume that U is right-invertible modulo I, i.e., there is an $r \times n$ matrix $W = (w_{jl})$ such that $U \cdot W \equiv E_n \pmod{I}$ (E_n is the $n \times n$ identity matrix). Then for every $t \in \mathbb{N}$ there exist $a_1^{(t)}, \ldots, a_r^{(t)} \in R$ such that $f_i(a_1^{(t)}, \ldots, a_r^{(t)}) \equiv 0 \pmod{I^t}$ for $1 \leq i \leq n$, and $a_j^{(t)} \equiv a_j \pmod{I}$ for $1 \leq j \leq r$.*

If the ideal I is generated by the prime element p, then the Lifting Theorem guarantees a p-adic approximation of the solution. An important special case of the Lifting Theorem is the Hensel Lemma on p-adic approximation of factors of a polynomial.

C.54.4 Theorem (***Hensel Lemma***) *Let p be a prime number and $a(x), a_1(x), \ldots, a_r(x) \in \mathbb{Z}[x]$. Let $(a_1 \bmod p), \ldots, (a_r \bmod p)$ be pairwise relatively prime in $\mathbb{Z}_p[x]$ and $a(x) \equiv a_1(x) \cdot \cdots \cdot a_r(x) \bmod p$. Then for every natural number k there are polynomials $a_1^{(k)}(x), \ldots, a_r^{(k)}(x) \in \mathbb{Z}[x]$ such that $a(x) \equiv a_1^{(k)}(x) \cdot \cdots \cdot a_r^{(k)}(x) \bmod p^k$ and $a_i^{(k)}(x) \equiv a_i(x) \bmod p$ for $1 \leq i \leq r$.*

The lifting procedure, and also the Hensel Lemma, can be made quadratic, i.e., lifting from equality modulo I^t to equality modulo I^{2t}.

Further details on computational ring theory can be found in a variety of books on computer algebra, e.g., (Gathen and Gerhard 1999) or (Winkler 1996).

C.55 Applications of Rings

by Günter F. Pilz in Linz, Austria

Many results in ring theory enable us to present a ring R as a direct sum of simpler rings R_i. If the transitions between R and $\bigoplus R_i$ is reasonably "smooth", *a direct sum decomposition means the ability to do parallel computations.* Examples are the use of Chinese remainder theorem, the decomposition of the group algebra $\mathbb{C}[G]$, and the Fast Fourier and the Fast Hadamard Transformations. One can see that all these cases are closely related. Real-life applications include compact disc players, which use these fast transforms to decode music signals very efficiently.

But we now turn to another area which seems to be less well-known: rings and dynamical systems. More on this can be found in (Lidl and Pilz 1998).

C.55.1 Example Let a point of mass $m = 1$ be the end of a pendulum of length r (cf. Figure 1). Here, g is gravity and x the radiant measure of α. If b denotes air resistance, Newton's second law tells us that $x = x(t))$ is governed by the differential equation

$$r\ddot{x}(t) + br\dot{x}(t) + g \sin x(t) = 0,$$

For small x, this can be replaced by the linear equation

$$r\ddot{x}(t) + br\dot{x}(t) + gx(t) = 0.$$

For $\mathbf{x}(t) := \begin{pmatrix} x(t) \\ \dot{x}(t) \end{pmatrix}$, we then get $\dot{\mathbf{x}}(t) = \begin{pmatrix} 0 & 1 \\ -g/r & -b \end{pmatrix}\mathbf{x}(t) =: \mathbf{F}\mathbf{x}(t)$.

Suppose now that the pendulum is hanging on a bar which can be turned at an angular speed of $u(t)$ and has the friction coefficient k (between the bar and the rope, cf. Figure 2). For small x, the linear equation has the form

$$r\ddot{x}(t) + br\dot{x}(t) + gx(t) = k(u - \dot{x}).$$

With $\bar{\mathbf{F}} := \begin{pmatrix} 0 & 1 \\ -g/r & -b - k/r \end{pmatrix}$ and $\mathbf{G} := \begin{pmatrix} 0 \\ k/r \end{pmatrix}$, the equation becomes

$$\dot{\mathbf{x}}(t) = \bar{\mathbf{F}}\mathbf{x}(t) + \mathbf{G}u(t).$$

This is a typical example of a ***linear continuous system***. We shall not introduce a formal definition of a system as a 7-tuple here; see e.g., (Kalman, Falb, and Arbib 1969) for precise definitions. The main terms