Integer Valued Polynomials on Maximal Orders in Division Algebras

Keith Johnson

7 October, 2019

Two Problems

Notation

$M_n(R)$ will denote the ring of $n \times n$ matrices with entries in the ring R. $R[x]$ will denote the R-module of polynomials with coefficients in R.

Problem

Describe the Z-module of polynomials $f(x) \in \mathbb{Q}[x]$ for which $f(\mathbb{Z}) \subseteq \mathbb{Z}$. (We will denote this $\mathbb{Z}$-module by $Int(\mathbb{Z})$).

Problem

Describe the $\mathbb{Z}$-module of polynomials $f(x) \in \mathbb{Q}[x]$ for which $f(M_n(\mathbb{Z})) \subseteq M_n(\mathbb{Z})$. (We will denote this $\mathbb{Z}$ module by $Int(M_n(\mathbb{Z}))$).

Examples

$$\frac{x(x+1)}{2} \in \mathrm{Int}(\mathbb{Z})$$

(Either x or $x+1$ is even.)

$$\frac{x^2(x+1)^2(x^2+x+1)}{2} \in \mathrm{Int}(M_2(\mathbb{Z}))$$

(This follows from the Cayley-Hamilton theorem over $\mathbb{F}_2$:

Theorem

(Cayley-Hamilton) If $A \in M_n(R)$ then a is a root of the monic, degree n polynomial $ch_A(x) = det(xI - A) \in R[x]$.)

The $\mathbb{Z}$-module structure of $\mathrm{Int}(\mathbb{Z})$ is described by

Theorem

(Gregory, 1668) The polynomials

$$\left\{ \binom{x}{n} = \frac{x(x+1)\dots(x+(n-1))}{n!} : n = 0, 1, 2, \dots \right\}$$

are all in $\mathrm{Int}(\mathbb{Z})$, and form a regular basis as a $\mathbb{Z}$-module.

For $\mathrm{Int}(M_n(\mathbb{Z}))$ we have

Theorem

(Frisch, 2005) If $f(x) = g(x)/c$ with $g(x) \in \mathbb{Z}[x]$ and $c \in \mathbb{Z}$, then $f(x)$ maps $M_n(\mathbb{Z})$ to itself if and only if $g(x)$ is divisible modulo $c\mathbb{Z}[x]$ by all monic polynomials in $Z[x]$ of degree n.

which converts the problem into one of computing LCM's in $\mathbb{Z}/m\mathbb{Z}[x]$ but doesn't provide a basis.

Integral closure

Theorem

(Loper-Werner, 2012)The integral closure of $Int(M_n(\mathbb{Z}))$ consists of those polynomials in $\mathbb{Q}[x]$ which are in $Int(A)$ for every A the ring of integers in an extension field of Q of degree n.

Localization

Up to this point all of the results and calculations described have been stated globally, i.e. with base field $\mathbb{Q}$ and ring of integers $\mathbb{Z}$ however all of this can be localized with respect to a prime p (and global results can be recovered from these using the Chinese remainder theorem).
From here on we will be considering only this local situation. The reason for this is the following embedding theorem:

Embedding Theorem

Theorem

If D is a division algebra of dimension n^2 over a local field K and K' is a field extension of degree n then K' can be embedded in D as a maximal commutative subfield.

Since this applies to each of the extension fields in the Loper-Werner theorem this leads to:

Theorem

A polynomial $f(x) \in \mathbb{Q}_p[x]$ is in the integral closure of $Int(M_n(\mathbb{Z}_p))$ if and only if it is in the ring $Int(A)$ of polynomials in $D[x]$ which are integer valued on A, the maximal order in D, a division algebra of degree n^2 over $\mathbb{Q}_p$.

Local Division Algebras

For n a positive integer and K a local field of characteristic p, a division algebra of dimension n^2 over K can be constructed as $D = K[\omega, \pi]$ subject to the relations $\omega^{p^n-1} = 1$, $\pi^n = p$ and $\omega \cdot \pi = \pi \cdot \omega^p$. The subfield $K[\omega]$ is the unique unrammified degree n extension of K and sits in D as a maximal commutative subfield. If B is the ring of integers in K then the maximal order in D, i.e. the subring of elements which are roots of monic polynomials with coefficients in B is $B[\omega, \pi]$.

p-orderings

If S is a subset of $\mathbb{Z}$ then a p-ordering of S is a sequence $\{a_i; i = 0, 1, 2, \dots\} \subseteq S$ with the property that for each k the element a_k minimizes the p-adic valuation (i.e. the number of times divisible by p) of the product

$$\prod_{i=0}^{k-1}(a_k - a_i).$$

The sequence of minimal values of the p-adic valuations occurring in this definition is called the p-sequence of S and depends only on S, not on the particular p-ordering used to compute it. We will denote it by $\{\alpha_S(k) : k = 0, 1, 2, \dots\}$.
These are useful because:

Theorem

(Bhargava) If $\{a_i : i = 0, 1, 2, \dots\}$ is a p-ordering of S then the polynomials $\prod_{i=0}^{k-1}(x - a_i)/p^{\alpha_S(k)}$ form a regular basis for Int(S).

How to compute p-orderings in $\mathbb{Z}$

p-orderings have the following properties which in many cases allow them to be recursively constructed:

Lemma

1. *If* $\{a_i : i = 0, 1, 2, \dots\}$ *is a p-ordering of* S *then* $\{a_i + b : i = 0, 1, 2, \dots\}$ *is a p-ordering of the set* $S + b$ *and the p-sequence of* $S + b$ *is the same as that of* S*.*
2. $\{a_i : i = 0, 1, 2, \dots\}$ *is a p-ordering of* S *then* $\{ca_i : i = 0, 1, 2, \dots\}$ *is a p-ordering of the set* cS *and the p-sequence of* $S + b$ *is* $\alpha_{pS}(k) = \alpha_S(k) + k \cdot \nu_p(c)$*.*
3. *If* S *is the disjoint union of two subsets* S_1 *and* S_2 *and these sets have the property that* $\nu_p(a - b) = 0$ *for any* $a \in S_1$*,* $b \in S_2$ *then the p-sequence of* S *is the disjoint union of those of* S_1 *and* S_2 *shuffled into increasing order and a p-ordering of* S *can be obtained as the disjoint union of ones for* S_1 *and* S_2 *sorted using the same shuffle as for the p-sequences.*

Notation

We denote the sequence whose k-th term is $c \cdot k$ by $(c \cdot k)$, so that the sequence in part 2 of the lemma is $\alpha_S + (\nu_p(c) \cdot k)$.
We denote the shuffle of two sequence by $\wedge$, so that the sequence in part 3 of the lemma is $\alpha_{S_1} \wedge \alpha_{S_2}$.

Example

For $S = \mathbb{Z}$ and $p = 2$ take $S_1 = 2\mathbb{Z}$ and $S_2 = 2\mathbb{Z} + 1$. Since S_2 is a translate of S_1, which is a multiple of $\mathbb{Z}$ we have

$$\alpha_{S_2} = \alpha_{S_1} = \alpha_{\mathbb{Z}} + (k)$$

and so

$$\alpha_{\mathbb{Z}} = \alpha_{S_1} \wedge \alpha_{S_2} = (\alpha_{\mathbb{Z}} + (k)) \wedge (\alpha_{\mathbb{Z}} + (k)).$$

Since the two sequences in the shuffle are the same their shuffle product is the sequence which each term repeated twice, hence we have the recursive formula

$$\alpha_{\mathbb{Z}}(2k) = \alpha_{\mathbb{Z}}(2k+1) = \alpha_{\mathbb{Z}}(k) + k$$

which determines $\alpha_{\mathbb{Z}}$ uniquely once we note that the sequence starts $\{0, 0, 1, \dots\}$. It continues

$$\{0, 0, 1, 1, 3, 3, 4, 4, 7, 7, 8, 8, \dots\}$$

and a straight forward induction shows that $\alpha_{\mathbb{Z}}(k) = \sum_{i>0} \lfloor k/2^i \rfloor$.

p-orderings in local division algebras

If D is a local division algebra with prime π then the definition of p-ordering and p-sequence extend to subsets of the maximal order in D. The defining condition for a p-ordering becomes that the a_k minimize $\nu_\pi(f(a_0, \ldots, a_{k-1})(a_k))$ where $f(a_0, \ldots, a_{k-1})$ is theminimal polynomial of $a_0, \ldots, a_{k-1}$. Bhargava's theorem extends to this situation as does the computational lemma, with the restrictions that part 2 holds only if c is in the center of D and part 3 requires that the sets S_1 and S_2 are closed under conjugation.

Result for $p = 2$, $n = 2$

Let A be the maximal order in D with $\omega^3 = 1$, $\pi^2 = 2$, $\pi\omega\pi^{-1} = \omega^2$. The sets

$$T_1 = \{z \in A : z \equiv 0 \pmod{\pi}\}$$

$$S = \{z \in A : z \equiv \omega, \omega^2 \pmod{\pi}\}$$

are each closed with respect to conjugation,

$$A = T_1 \cup (T_1 + 1) \cup S$$

and $\nu_2(a - b) = 0$ if a and b are in distinct parts of this partition. If

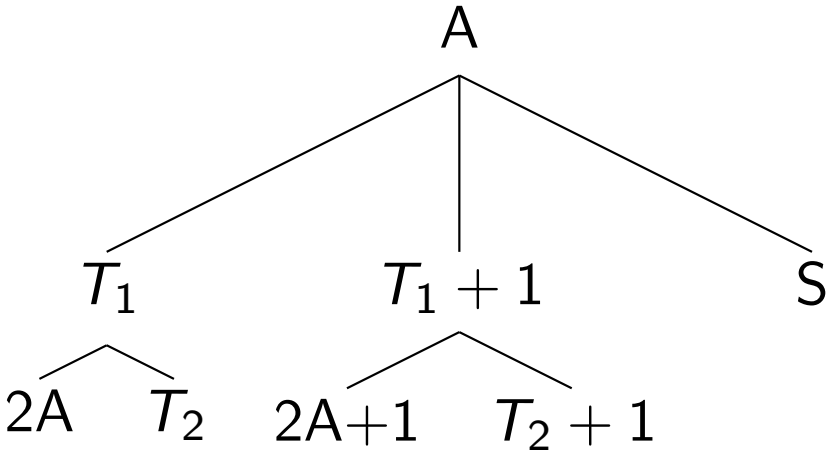
$$T_2 = \{z \in T_1 : z \not\equiv 0 \pmod{2}\}$$

then T_2 and $2A$ are closed under conjugation,

$$T_1 = T_2 \cup 2A$$

and $\nu_2(a - b) = 1$ if a and b are in distinct parts of this partition.

This decomposition can be represented by the tree diagram



This gives the recurrence

$$\alpha_A = ((\alpha_A + (n)) \wedge (\alpha_{T_2} - (n))) \wedge ((\alpha_A + (n)) \wedge (\alpha_{T_2} - (n))) \wedge \alpha_S.$$

The sequences α_S and α_{T_2} can be computed by directly constructing regular bases for Int(S) and Int(T_2) (which is possible because the elements of S and T_2 have characteristic polynomials which are irreducible modulo p).

Consequences

This recurrence formula provides a fast method of computing α_S. The first few terms are

$$0, 0, 0, 0, 1, 1, 2, 2, 2, 2, 4, 4, 4, 4, 5, 5, 6, 6, 6, 6, 8, 8, 10, 10, 10, 10, \ldots$$

and so on. $\alpha_A(1000000) = 499990$.
By comparing this with a computation of part of a basis for $\mathrm{Int}(M_2(\mathbb{Z}))$ it shows that the lowest degree element in the integral closure but not in $\mathrm{Int}(M_2(\mathbb{Z}))$ occurs in degree 10, and by computing part of a π ordering of A it shows that $x(x^2+2x+2)(x-1)(x^2+1)(x^2-x+1)(x^2+x+1)/4$ is an example.
This recurrence formula also reveals the asymptotic behaviour of α_A. A lemma of Michael Fekete shows that for any set X the limit $\lim_{k\to\infty} \alpha_X(k)/k$ always exists, and for A it turns out that

$$\lim_{k\to\infty} \frac{\alpha_A(k)}{k} = \frac{1}{2}$$

.

Further Results

The case $n = 2$, $p > 2$ behaves much like the case $p = 2$. The set T_2 gets replaced by $p - 1$ sets, all translates of one of them, and S gets replaced by $(p^2 - 1)/2$ sets, again all translates of one of them. This produces the recurrence

$$\alpha_A = (((\alpha_A + (n)) \wedge (\alpha_T - (n))^{\wedge^{p-1}}) + (n))^{\wedge^p} \wedge (\alpha_S^{\wedge^{(p^2-p)/2}})$$

The case $n > 2$ is more subtle, and is the subject of Asmita Sodhi's thesis which she will tell us about in the near future.