FORUM—Math 199B Winter 2017

Questions are in reverse chronological order

- Question March 14

  I have some questions while reading Schaferbook. On page 13, from the last second paragraph, the author states the following as a fact: "any simple algebra A (of arbitrary dimension), regarded as an algebra over its multiplication centralizer C0 (so that C0 = F) is central simple." Do we need to know how to prove this or just accept it as a definition? If we do need to prove it, how could we do so?

- Answer March 14

  You can just assume this. However, I would like to go over this with you after the class on Friday, since as last week, I need to review the definitions. We can try to figure out the proof together.

- Second Question March 9

  Now, I am working on exercise #22. For the second part of the proof, how could I see that those two matrix multiplications are in A(tilde)0? I include a picture of my question in the attachment. Thank you so much for you time!

- Answer to Second Question March 9

  We can work this out together tomorrow after the class if you are free. I have to review the definitions and we can do this together very easily. It is hard to remember the definitons of the module actions etc. and I don't want to spend the time now just to repeat it tomorrow. However, I am happy to go over it with you tomorrow.

- First Question March 9 About exercise 11 of Math 199A problems

  I know that if —x— ¡1, then x is convergent. But I do not know how to prove that y is convergent in Exercise 11. Does it mean that I need to prove —y— ¡ 1? Could you please give me some steps or hints to solve this problem?

- Answer to First Question March 9

```
y is the proposed sum of the infinite series   x+x^2+x^3+...
Note that if x is a real  number, then this is just a geometric
 series, which will converge if 0 < x < 1,  or if absolute value
  of x is  <  1.    In our case, x is a vector with length |x|<1.
    In this case, the partial sum
x+x^2+...+x^n   has length less than |x|+|x|^2+...+|x|^n
(Cauchy Schwarz inequality)   The latter is a geometric
series of real numbers, which converges since |x|<1, so
```

the series x+x^2+x^3+... converges absolutely. (This material is taught in Advanced calculus, Math 140C) Moreover since x commutes with x^k, it will commute with x+x^2+...+x^n and in the limit it will commute with y.

It doesn't make sense to say that x is convergent. x is a fixed vector.

- Question February 1

  I could not solve the #5 question. Could you please give me some clue to do it. Because I just check the book and 7.14 is not related to 7.13. I tried to connected it with 7.15 but I really do not know where the constant 8 comes from.

- Answer to Question February 1

  There are two misprints on page 70 of the meyberg notes. See the next page for the corrections, and the subsequent two pages for my answer.

Furthermore we observe that the left hand side of (7.11) is skew symmetric in the pairs (x,y), (u,v), hence

(7.13) $\{\{xyu\}vw\} - \{u\{yxv\}w\} = \{x\{vuy\}w\} - \{\{uvx\}yw\}$.

In order to prove the fundamental formula

(7.14) $P(P(u)v) = P(u)P(v)P(u)$ for all $u,v \in \mathfrak{J}$,

Exercise 5 Fill in details of the proof of 7.14

we substitute $x \to \{uvu\}, w \to u$ in (7.11) and obtain (note: $\{xyx\} = 2P(x)y$)

(7.15) $8P(P(u)v)y = 2\{uv\{uy\{uvu\}\}\} - \{u\{y\{uvu\}\}u\}$.

Replacing $u \to y$, $y \to u$, $x \to v$, $v \to u$, $w \to v$ in (7.13) gives

$\{y\{uvu\}v\} = 2\{\{vuy\}uv\} - \{v\{uyu\}v\}$.

Substituting this in (7.15) implies

$8P(P(u)v)y = 2\{uv\{uy\{uvu\}\}\} - 2\{u\{\{yuv\}uv\}u\} + 8P(u)P(v)P(u)y$.

Since the homotopy formula (7.9) has as consequence

$\{uv\{uy\{uvu\}\}\} = \{uv\{u\{yuv\}u\}\} = \{u\{vu\{yuv\}\}u\}$,

the foregoing reduces to (7.14).

We have seen that the deduction from the axioms (J.1), (J.2) of all the important formulas in Jordan theory (in particular (7.9), (7.12) and (7.14)) depends heavily on the fact that we were able to cancel by 2. On the other hand, a theory of linear Jordan algebras over fields of characteristic 2 does not lead to results, which are "compatible" with results in the case of char $\neq 2$. So one has to think of something else, which would permit a "nice" theory for arbitrary rings. The best approach so far is via "quadratic Jordan algebras", which where "invented"

2/11/17

Exercise 5

(7.11) $\{xy\{uvw\}\} - \{uv\{xyw\}\} = \{\{xyu\}vw\} - \{u\{yxv\}w\}$

$\{uvu\} = 2P(u)v$; u ; $\{uvu\}$; u ; $\{uvu\}$; u ; $\{uvu\}$; u

Recall $P(x,z|y) = \{xyz\}$

$P(x,x) = 2P(x)$

these are equal

$\{2P(u)v, y, 2P(u)v\} - \{uv\{2P(u)v, y, u\}\} = \{\{2P(u)v, y, u\}vu\}$

$4 \cdot 2P(P(u)v)y$

$= -\{u\{y, 2P(u)x, v\}u\}$

$= -2P(u)\{y, 2P(u)v, v\}$

(7.15) $8\,P(P(u)v)y = 2\{uv\{uy\{uvu\}\}\} - \{u\{y\{uvu\}v\}u\}$

(7.13) $\{\{xyu\}vw\} - \{u\{yxv\}w\} = \{x\{vuy\}w\} - \{\{uvx\}yw\}$

$v\ u\ y\ u\ v$

$\{\{vuy\}uv\} - \{y\{uvu\}v\} = \{v\{uyu\}v\} - \{\{yuv\}uv\}$

equal

(7.13′) $\{y\{uvu\}v\} = 2\{\{vuy\}uv\} - \{v\{uyu\}v\}$

(7.13)'' $\{u\{y\{uvu\}v\}u\} = 2\{u\{\{vuy\}uv\}u\} - \{u\{v\{uyu\}v\}u\}$

$= 8\,P(u)P(v)P(u)y$

substitute (7.13)'' into (7.15)

$8\,P(P(u)v)y = 2\{uv\{uy\{uvu\}\}\} - (2\{u\{\{vuy\}uv\}u\} - 8\,P(u)P(v)P(u)y)$

(7.9) $L(x/y)\,P(x) = P(x)L(y,x) = P(P(x)y,x)$

$\frac{1}{2}\{xy\{xzx\}\} = \frac{1}{2}\{x\{yxz\}x\} = \{P(x)y,z,x\}$

u u v u

$= \frac{1}{2}\{\{xyx\},z,x\}$

$\{uy\{uvu\}\} = \{\{uyu\}v,u\} = \{u\{yuv\}u\}$

$\{uv\{uy\{uvu\}\}\} = \{uv\{u\{yuv\}u\}\} \overset{?}{=} \{u\{\{vuy\}uv\}u\}$

Y

need to prove

then you get $P(P(u)v) = P(u)P(v)P(u)$ (7.14)

$\{uv\{uYu\}\} = \{u\{Yuv\}u\}$

$\therefore\ \{uv\{u\{yuv\}u\}\} = \{u\{\{yuv\}uv\}u\}$ IT WORKS!

- Question January 27

  `Please help me to understand the paper by Denes and Denes for my project`

- Answer to Question January 27

  Attached are my notes after reviewing the paper we talked about. I also attach copies of some of the references, which I downloaded. I don't have enough background in cryptography so I cannot understand the paper. That is why I look at the references to see if it helps. The article by Paige is of special interest to me since he was the chair at UCLA when I was a student there (1956-1964). It is purely mathematical without regard to cryptography.

  The book by Simmons can be bought for 14 cents +3.99 shipping. I also requested two of the references directly from the authors through RESEARCHGATE. One other reference was requested via inter library loan. I will let you know when I receive any of these. They were not available online.

  Files Attached:

  DenesNotes2pp.pdf (1.6 MB)

  [15]Wanless.pdf (282 KB)

  [11]Drapal.pdf (106 KB)

  [5]DenesEtAl.pdf (301 KB)

  [7]DenesEtAl.pdf (121 KB)

  PaigeDuke1949.pdf (2.3 MB)

  QuisquaterEtAl[13+].pdf (233 KB)

  [1]Cawagas.pdf (188 KB)

  [2]ChaumEvertse.pdf (722 KB)

  See the next 2 pages for my notes on the paper in question

Denes & Denes Quasigroups & Related Systems 8 '01 7-14

§1

[2] downloaded to desktop [2] chaum Evertse

plaintext → ← ciphertext

[14] Contemporary Cryptology 1992 G.J. Simmons

Amazon $ 0.14 + 3.99 Feb 9-27

[6] Latin Squares Denes & Keedwell ILL 2/2/17

---

def 1.2 J finite set $+$ $\circ$

$(J,+)$ is a loop identity elt. 0

$J\setminus\{0\}$ is a group $(J\setminus\{0\}, \circ)$

$a \circ (b+c) = a\circ b + a\circ c$

$(b+c)\circ a = b\circ a + c\circ a$

] neofield

L.J. Paige 1947 introduced neofields — his thesis downloaded to desktop.

[1] Cavagar, R 2000 downloaded to desktop

[8] hungarian talent

[4] PUMA - requested from the author 2/2/17

[7] J Comb Th - saved to desktop 2/2/17

[5] Discrete Math - saved to desktop 2/2/17

[10] hungarian

[11] Discrete Math - saved to desktop 2/2/17

§2

[13+] Qusquater Et Al - related paper downloaded

§3

I.M. Wanless - saved to desktop

[15] ~~A/ J. Wanless~~ Elec. J. Combin... 6 1999

[12] Ars Combinatorica 44 1996 137-148
- requested from author

[9] Denes hungarian

- Question January 24

  ```
  Would it be possible that
  you give me some instructions for exercise 3 and 4 like what you did for
  last quarter's problem set?
  ```

- Answer to Question January 24

  See the next 3 pages for discussion of Exercise 3

Discussion of Exercise 3 chapter 7

(7.7) $L(y)P(x) + P(x)L(y) = P(xy, x)$

From the defenition of $P(x)$,

(7.7) is the same as

$$2L(y)L(x)^2 - L(y)L(x^2) + 2L(x)^2L(y) - L(x^2)L(y)$$

$$= 2L(x)L(xy) + 2L(xy)L(x) - L(2x(xy)) \quad (*)$$

replace x by $u+w$

$$2L(y)\left(L(u)^2 + L(u)L(w) + L(w)L(u) + L(w)^2\right)$$

$$- L(y)\left(L(u^2) + L(2uw) + L(w^2)\right)$$

$$+ 2\left(L(w)^2 + L(u)L(w) + L(w)L(u) + L(w)^2\right)L(y)$$

$$- \left(L(u^2) + L(2uw) + L(w^2)\right)L(y)$$

$$= 2\left(L(u)+L(w)\right)\left(L(uy)+L(wy)\right) + 2\left(L(uy)+L(wy)\right)\left(L(u)+L(w)\right)$$

$$-2L\left((u+w)(uy+wy)\right) =$$

$$-2\left(L(u(uy)) + L(w(uy)) + L(u(wy)) + L(w(wy))\right)$$

$$2L(y)L(u)^2 + 2L(y)L(u)L(w) + 2L(y)L(w)L(u) + 2L(y)L(w)^2$$
$$- L(y)L(u^2) - 2L(y)L(uw) - L(y)L(w^2)$$
$$+ 2L(u)^2L(y) + 2L(u)L(w)L(y) + 2L(w)L(u)L(y) + 2L(w)^2L(y)$$
$$- L(u^2)L(y) - 2L(uw)L(y) - L(w^2)L(y)$$

$$= 2L(u)L(uy) + 2L(w)L(uy) + 2L(u)L(wy) + 2L(w)L(wy)$$
$$+ 2L(uy)L(u) + 2L(wy)L(u) + 2L(wy)L(w) + 2L(uy)L(w)$$
$$- 2L(u(uy)) - 2L(w(uy)) - 2L(u(wy)) - 2L(w(wy))$$

The terms labeled ① cancel by ⊛
The terms labeled ② cancel by ⊛

What remains after cancelling the 2 is

$$L(y)L(u)L(w) + L(y)L(w)L(u) - L(y)L(uw)$$
$$+ L(u)L(w)L(y) + L(w)L(u)L(y) - L(uw)L(y)$$

$$= L(w)L(uy) + L(u)L(wy) + L(wy)L(u)$$
$$+ L(uy)L(w) - L(w(uy)) - L(u(wy))$$

apply to v

$$y(u(wv)) + y(w(uv)) - y((uw)v)$$
$$+ u(w(yv)) + w(u(yv)) - (uw)(yv)$$
$$= w((uy)v) + u((wy)v) + (wy)(uv)$$
$$+ (uy)(wv) - (w(uy))v - (u(wy))v$$

voila!

let's rewrite (7.10) using $\{abc\} = P(a,c)\,b$

where by (7.6) $P(x,y) = 2\left(L(x)L(y) + L(y)L(x) - L(xy)\right)$

(7.10) $y\{uvw\} \stackrel{?}{=} \{(yu)vw\} - \{u(yv)w\} + \{uv(yw)\}$

(7.10′) $y(P(u,w)v) \stackrel{?}{=} P(yu,w)v - P(u,w)(yv) + P(u,yw)v$

LHS, RHS_1, RHS_2, RHS_3

To prove (7.10′), we can forget about the 2 in 7.6 !!

$$LHS = y\left(\left(L(w)L(w) + L(w)L(u) - L(wu)\right)v\right)$$
$$= y(u(wv)) + y(w(uv)) - y((wu)v)$$

$RHS_1 =$ etc !!!

- Question January 15

  I am trying to prove Exercise 1 on Meyberg Chapter 7,
  but I'm not sure about my proof.

- Answer to Question January 15

  You have a Jordan algebra F.
  You consider the algebra F with identity adjoined (even if F has
  identity---you can ignore it). You are to prove that this new algebra
  which equals the cartesian product R X F or C X F (R=reals,
  C=complexes)
  still satisfies the Jordan axioms.

  namely if xy=yx and x^2(xy)=x(x^2y) hold in F, then

  (a,x)(b,y)=(b,y)(a,x) and

  (a,x)^2 ((a,x)(b,y))=(a,x) ((a,x)^2(b,y)) also hold

  See page 7 in chapter 1 to recall the product in R X F:

  (a,x)(b,y)=(ab,ay+bx+xy)

  a and b are numbers, x and y are vectors in F.