Beste Herman,

Hier volgt mijn bijdrage voor je Liber Amicorum. Je belangstelling voor getaltheorie is groot, zoals bv. tot uitdrukking komt in je bijdragen over het berekenen van nulpunten van de Riemann Zeta-functie, het weerleggen van het vermoeden van Mertens, je bijdragen over bevriende getallen, je werk op het terrein van de toegepaste en toepasbare getaltheorie, ja zelfs gezondheidszorg. Ik heb wat lopen zoeken naar een geschikt onderwerp voor je Liber Amicorum, en meen dat gevonden te hebben in de Stelling van Hua. Recentelijk zijn daar nl. toepassingen op cryptografisch terrein uit voortgekomen, maar ook theoretisch valt er nieuws te melden.

Waar gaat het om?

In 1949 bewees Hua dat elke bijectieve afbeelding f van een delingsring A op een delingsring B welke niet alleen de optelling respecteert maar waarbij ook het beeld van de multiplikatieve inverse van een willekeurig niet-nul element a van A samenvalt met de multiplikatieve inverse van het beeld van die a, terwijl tevens de "1" op de corresponderende "1" wordt afgebeeld, in feite een isomorfie van ringen ofwel een anti-isomorfie van ringen is.

In boeken valt zulks bij Artin [1] en bij Jacobson [7] na te lezen. Artin past Hua's resultaat toe om een bewijs voor een fundamentele stelling in de projectieve meetkunde te verkrijgen, zie blz. 85 van zijn boek. Jacobson vermeldt bovendien thema's verwant met Hua's resultaat, zie de eerste drie bladzijden van diens boek.

Bij Bourbaki, zie [2] blz. 146, is Hua's vondst in een opgave terug te vinden, echter alleen daar, waar het commutatieve lichamen betreft van oneven karakteristiek doch waarbij tevens de nodige voorwaarde f(1) = 1 niet genoemd staat. In [5] poogt Gow Bourbaki's manco te repareren, daarbij ook wat nieuws vermeldend. Doch hij blijkt onbekend te zijn met Hua's Stelling, hetgeen tot uiting komt in (citaat) : "In conclusion, we suspect that it is quite likely that this question (d.w.z. Hua's Stelling, (R.v.d.W)) has already been discussed in the literature, although we have not seen anything ourselves". Voor bijdragen van recente datum, waarin onderwerpen á la Hua aan de orde komen, kan je terecht bij [3], [4] en [8]. In [8] staat vermeld dat de zogeheten inversie-afbeelding in eindige lichamen geschikt zijn voor cryptografische doeleinden onder verwijzing daarbij naar zekere elektronische literatuur.

De problematiek van afbeelden van de "1" op de "1" wordt in onderstaande Stelling 3 geheel omzeilt, maar de explicite waarde van f(1) speelt wel degelijk een rol op de achtergrond. Bovendien is juist in Stelling 3 het geordende product van drie elementen van belang terwijl in Hua's Stelling "slechts" het geordende product van twee elementen wordt beschouwd.

Het is wellicht verrassend dat zulks, zo ben ik van mening, leidt tot wat elegantere uitspraken dan die welke aangetroffen worden in bestaande thematiek rond Hua's resulaat.
In detail gaat het hierom:

Definitie 1.
Laat op een zekere niet-lege verzameling V twee binaire operaties + en . gedefinieerd zijn die voldoen aan drie eisen, nl.
1) V is een abelse groep t.o.v. de operatie + (met 0 zij het eenheidselement van deze groep genoteerd);
2) de operaties + en . staan tot elkaar in verbinding via (a + b).c = (a.c) + (b.c), a.(b + c) = (a.b) + (a.c) voor alle alle a,b,c uit V;
3) er bestaat een element in V, genoteerd als 1, dat voldoet aan 1.a = a = a.1 voor alle a uit V.
Dan heet V een delingsring indien ook voldaan is aan:
4) 1 is verschillend van 0;
5) de verzameling der ongelijk-nul elementen van V met 0 uit V, is een (niet-noodzakelijk abelse) groep t.o.v. de operatie.

Opmerking.
In plaats van (a.b) + d schrijven we a.b + d, idem dito a + b.d voor a + (b.d) , en dergelijke. Kleine letters staan telkens voor elementen uit een delingsring.

Als voorbeelden van delingsringen heeft men bv.: de verzameling der reële getallen, de verzameling der rationele getallen t.o.v. de gebruikelijke operaties + en. Natuurlijk ook de verzameling der complexe getallen met de daar heersende bekende operaties binaire operaties “optellen” en “vermenigvuldigen”. Een voorbeeld van een delingsring waarvoor de “vermenigvuldigingsoperatie” niet commutatief is, is de zogeheten quaternionen-delingsring H, bestaande uit alle (2 x 2) - matrices met complexe coëfficiënten met (beschrijvend): linksboven een willekeurig element a uit de complexe getallen C, rechtsboven een willekeurig element b uit C, linksonder -(de complex geconjugeerde van b) en rechtsonder de complex geconjugeerde van a. Uiteraard der zaak vigeren in H hier de gebruikelijke optelling- en vermenigvuldigingsoperaties voor matrices.

Met het oog op het vervolg noemen we zonder bewijs enkele rekenregels en eigenschappen die bij dit verhaal over een zekere delingsring D, een rol spelen:
a) Bij iedere a uit D is er precies één element in D te vinden, genoteerd -a, zodat a + (-a) = 0; voorts geldt -(-a) = a;

b) voor iedere a uit D geldt a.0 = 0 = 0.a;
c) geoorloofde notatie: a.d.f staat voor (a.d).f, voor alle a,d en f uit D; inductief net zo voor meer dan drie elementen uit D;
d) (s.r) + ((-s).r) = (s + (-s)).r = 0.r = 0 voor alle s en r uit D; hieruit volgt (-s).r = -(s.r) en dus ook (-1).r = =(1.r) = -r;
e) (-s).(-r) + ((-s.r) = 0 = (s.r) + ((-s).r); en dus (-s).(-r) = s.r voor alle s en r uit D;
f) D heeft geen nuldelers, d.w.z. uit a.b = 0 voor zekere a en b uit D volgt steeds dat tenminste één der a, b gelijk is aan 0.

Definitie 2.
Beschouw een afbeelding f van een delingsring naar zichzelf die voldoet aan aan de volgende drie eisen:
A) f(a + b) = f(a) + f(b) voor alle a en b uit D;
B) f(d) is ongelijk aan 0 voor alle d ongelijk aan 0 uit D;
C) Uit t.r = 1 voor zekere t en r uit D volgt steeds dat f(t).f(r) = 1 waar is. Zo'n f noem ik een endomorfisme. Geldt voor f ook nog dat aan f(1) = 1 is voldaan dan spreek ik over een Jordan-endomorfisme.

Opmerking.
Uit het voorgaande valt af te leiden dat voor zo'n endomorfisme f geldt die: f(1).f(1) = 1, dat f(0) = 0, dat (-1).f(a) = -f(a), dat
f(a) +f(-a) = f(a + (-a)) = f(0) = 0 en dat dus -f(a) = f(-a), dit alles voor alle a uit D. Omdat na te rekenen valt dat (f(1) + (-1)). (f(1) + 1) gelijk is aan 0,
zien we dat de waarde van f(1) gelijk is aan 1 of aan -1; immers, D heeft geen nuldelers.

In de nu volgende Stelling 3 staat te lezen dat elk endomorfisme van een delingsring een zeker type “behoud” dan wel “anti-behoud” oplevert ten opzichte van de operatie, onafhankelijk van de waarde van f(1).

Stelling 3.
Zij f een endomorfisme van een delingsring D. Dan is tenminste één der twee volgende uitspraken waar:
a) f(a.b.c) = f(a).f(b).f(c) voor alle a,b en c uit D;
b) f(a.b.c) = f(c).f(b).f(a) voor alle a,b en c uit D.

Schets van het bewijs van Stelling 3.
We weten dat f(1) = 1 of f(1) = -1 geldt. Splits als volgt.
Stel f(1) = 1.. Dan geldt volgens Hua, dat
ofwel voor alle a en b uit D is f(a.b) = f(a).f(b) vervuld,

ofwel voor alle a en b uit D is f(a.b) = f(b).f(a) vervuld.
In de reeds genoemde boeken van Jacobson en Artin staat het bewijs van Hua's Stelling zonder omhaal afgedrukt, technisch en doorwrocht (sommigen zouden zeggen: “nogal getruukt en bepaald niet mooi”). Maar dat bewijs gaat nergens een, zeg, tweedejaarsstudentenniveau te boven. Het bewijs van Stelling 3 voor het geval f(1) = 1 volgt nu vrijwel onmiddellijk.
Stel f(1) = -1. Definieer de afbeelding g van D naar zichzelf door middel van g(a) = f(-a) met a uit D. Dan is g een Jordan endomorfisme! Dus geldt voor g de Stelling van Hua, waaruit door omschrijven naar f het bewijs voor Stelling 3 volgt. Dit omschrijven is nogal een technische klus die ik je bespaar. Hiermee is Stelling 3 geheel bewezen.

Er zijn een tweetal gevolgen, afhankelijk van het feit of een zeker natuurlijk n even of oneven is.

Gevolg 4. Laat f een afbeelding zijn waarvan sprake is in Stelling 3. Dan geldt voor elke oneven gehele n tenminste 3, dat
ofwel voor alle a1, a2, ... , an uit D geldt f(a1.a2.a3. ... .an) = f(a1) .f(a2). ... f(an);
ofwel voor alle a1, a2, ... , an uit D geldt f(a1.a2.a3. ... .an) = f(an) ... f(a3).f(a2).f(a1) (volledig retrograde, om zo te zeggen).

Het bewijs van Gevolg 4 (wat ik hier niet geef) volgt gemakkelijk via mathematische inductie door f(a1.a2.a3. ... .an) te schrijven als f(a1.a2.(a3. ... .an)), daarbij het resultaat van Stelling 3 toepassende; immers het aantal a's in de productuitdrukking a3. ... .an is oneven.

Gevolg 5. Laat f een afbeelding zijn waarvan sprake is in Stelling 3. Dan geldt voor elke even gehele n tenminste 2, dat
ofwel voor alle a1,a2, ..., an uit D geldt f(a1.a2. ... .an) = f(1).f(a1).f(a2). ... .f(an),
ofwel voor alle a1,a2, ... ,an uit D geldt f(a1.a2. ... .an) = f(1).f(an). ... . f(a2).f(a1) (volledig retrograde dus weer voor de rij der a’s).

Het bewijs van Gevolg 5, (wat ik hier, net zo als voor Gevolg 4, niet geef) volgt eveneens via mathematische inductie, maar is nogal behoorlijk technisch van aard. Ditmaal wordt Stelling 3 toegepast op de situatie f(a1.a2. ... .an) = f(b.c.an), waarbij b staat voor het geordende product van de eerste n-2 geordende rij elementen der ai’s, c staat voor het “één-naar-laatste” element a(n-1). Immers het aantal ai’s in de productuitdrukking a1.a2. ... . a(n-2) is even en tenminste gelijk aan 2 of anders is n=2 het geval. Voor n=2 beschouwen we Stelling 3 toegepast op de situatie f(a1.a2) = f(1.(a1.a2)) voor

alle a1,a2 uit D tezamen met de opmerking dat f(1).u = u.f(1) geldt voor alle u uit D. Voor even n tenminste gelijk aan 4 en f(1) = 1 kan voor het te verkrijgen bewijs rechtstreeks gebruik gemaakt worden van het verkregen resultaat onder Stelling3, terwijl voor het geval dat de even n tenminste gelijk is aan 4 en f(1) de waarde -1 heeft, weer de omschrijving via het Jordan endomorfisme g middels g(a) = f(-a) voor alle a uit D dient te worden aangeroepen.

Slotopmerking.
In de formulering van Stelling 3 is sprake van een afbeelding f van een delingsring naar zichzelf. Op een voor de hand liggende manier kan men f definiëren op een delingsring wier beelden alle in een andere delingsring liggen. Aldus worden volledig analoge resultaten verkregen.

Literatuur.
[1] E.Artin, Geometric Algebra, Interscience Publ., 1957.
[2] N.Bourbaki, Algébre I, Herrmann, 1951.
[3] A.Caranti, F.Dalla Volta, M.Sala and F.Villani, Imprimitive permutation groups generated by round functions and key-alterating block ciphers; electronisch: CoRR abs/math/0606022 (2006).
[4] D.Goldstein, R.Guralnick, L.Small and E.Zelmanov, Inversion-invariant additive subgroups of division rings; Pacific Journal of Math., vol.227 (2006), blz. 287-294.
[5] R.Gow, A problem of Bourbaki on field theory, Bull.Irish Math.Soc., vol.35 (1995), blz. 75-76.
[6] L.-K,Hua, On the automorphisms of a sfield, Proc. of the Nat.Ac. Sciences USA, vol.35, (1949), blz. 386-389.
[6a] L.-K.Hua, Some properties of a sfield, Proc.of the Nat.Ac. of Sciences USA, vol.35 (1949), blz. 533-537.
[7] N.Jacobson, Structure and Representations of Jordan Algebras, AMS Colloquium Publications, vol.39 ,1968.
[8] S. Mattarei, Inverse-closed additive subgroups of fields, Israel Journ. of Math., vol. 159 (2007), blz. 343-347.

Herman, ik wens jou en je familie het allerbeste in de toekomst en we spreken elkaar vast wel weer op bijeenkomsten over wiskunde of anderszins.

Rob van der Waall