רבעון למתמטיקה

ללמוד ולמחקר

בעריכת דב ירדן

כרך 4 ירושלים, ניסן תש״י, אפריל 1950 חוברת 1

תכן

כתבת המערכת: דב ירדן, כנסת החדשה, ירושלים

המחיר 250 מיל

פולינומים דיפרנציאליים סופיים

שמשון עמיצור

1. יהי K שדה (לאו דוקא קומוטטיבי) אשר מגדרת בו גזירה, כלומר, התאמה $a \to a'$ המקיימת: 1. $(a+b)'=a'+b'$. 2. $(ab)'=a'b+ab'$. האבר a' המתאים לאבר a נקרא ה נ ג ז ר ת של a. ק ו נ ס ט נ ט ה בשדה K היא אבר אשר הנגזרת שלו היא אפס. קבוצת כל הקונסטנטות מהוה שדה חלקי הנקרא שדה הקונסטנטות של K.

בעזרת הגזירה המגדרת ב K בונים אנו את חוג הפולינומים הדיפרנציאליים K[t] מעל K, באפן הבא[1]: מסתכלים בקבוצת כל הפולינומים בתו t: $t^na_0+t^{n-1}a_1+\dots+a_n$ עם מקדמים מתוך השדה K הכתובים מימין לחזקות של t. את הכפל של אברי השדה K בתו t מגדירים: $at=ta+a'$ לכל $a\in K$. (השויון והסכום מגדרים ככל חוג פולינומים).

יהי $p(t)=t^na_0+t^{n-1}a_1+\dots+a_n$ באשר $a_0\neq 0$. האבר a_0 הוא ה מ ק ד ם ה ע ל י ו ן של $p(t)$ והחזקה n היא מ ע ל ת הפולינום $p(t)$[2]. הפולינום $p(t)$ הוא פ ו ל י נ ו ם מ ת ו ק ן כאשר $a_0=1$.

ענין מיוחד יש בפולינומים $g(t)$ אשר האידיאל הימני הנוצר על ידי $g(t)$ בחוג K[t] הוא אידיאל דו-צדדי. קבוצת פולינומים זו מזדהה עם קבוצת הפולינומים $g(t)$ בעלי התכונה הבאה: (א) לכל פולינום $a(t)$ קים פולינום $b(t)$ כך ש: $a(t)g(t)=g(t)b(t)$. ברור שאם פולינום $g(t)$ מקים את (א) אזי גם הפולינום $g(t)a$, $a\in K$, מקים אותה תכונה, ולכן די להסתכל רק בפולינומים המתוקנים המקימים את הדרישה (א). נגדיר בעקבות Jacobson[3]:

הגדרה: פולינום $g(t)$ הוא פ ו ל י נ ו ם ס ו פ י אם $g(t)$ הוא פולינום מתוקן אשר האידיאל הימני הנוצר על ידי $g(t)$ בחוג K[t] הוא אידיאל דו-צדדי (דהינו: $g(t)$ מקים את הדרישה (א)).

Jacobson[3] הראה שהחוג K[t] איננו מכיל פולינומים סופיים מלבד היחידה, כאשר השדה K הוא בעל כרכטריסטיקה אפס והגזירה המגדרת ב K איננה גזירה פנימית[4]. אם הגזירה בשדה K היא גזירה פנימית המגדרת על ידי אבר x אזי קבוצת הפולינומים הסופיים בחוג K[t] מתלכדת עם קבוצת כל הפולינומים בעלי הצורה: $(t-x)^m+(t-x)^{m-1}c_1+\dots+c_m$, באשר המקדמים c_i שיכים למרכז[5] של השדה K.

מטרתנו בעבודה זו היא למצא את כל הפולינומים הסופיים בחוג K[t] כאשר השדה K הוא בעל כרכטריסטיקה סופית.

---

1) פרטי הבניה נמצאים:
O. Ore, Theory of non-commutative polynomials, Ann. of Math. 34 (1933), pp. 480-508.

2) מעלת פולינום האפס היא 1-.

3) N. Jacobson, Pseudo-linear transformations, Ann. of Math. 38 (1937), pp. 484-507.

4) הגזירה $a \to a'$ היא גזירה פנימית, אם קים אבר $x\in K$ כך ש $a'=ax-xa$ לכל $a\in K$, ואומרים שהגזירה הפנימית מגדרת על ידי האבר x.

5) המרכז של חוג R הוא קבוצת אברי R המתחלפים עם כל אברי החוג.

2. **משפט 1.** הפולינום $h(t)$ הוא פולינום סופי, כאשר ורק כאשר $h(t)$ מתחלף עם כל אחד מאברי החוג $K[t]$.

הוכחה. ברור שאם פולינום $h(t)$ מתחלף עם כל החוג $K[t]$, הוא מקים את הדרישה (א) ולכן $h(t)$ הוא פולינום סופי.

להפך: יהי $h(t)=t^n+t^{n-1}a_1+\dots+a_n$ פולינום סופי. לכל $a\in K$ קים פולינום $a_1(t)$ אשר: $ah(t)=h(t)a_1(t)$. משויון המעלות של שני אגפי השויון האחרון רואים כי הפולינום $a_1(t)$ הוא אבר a_1 בשדה K. המקדם העליון של $ah(t)$ הוא a והמקדם העליון של $h(t)a_1$ הוא a_1 ולכן $a=a_1$, כלומר: $ah(t)=h(t)a$, $h(t)$ מתחלף עם כל אברי השדה K. כמו כן קים פולינום $b(t)$ בחוג $K[t]$ אשר: $th(t)=h(t)b(t)$. אף כאן משויון המעלות של שני אגפי המשואה מקבלים שהפולינום $b(t)$ הוא פולינום מהמעלה הראשונה, כלומר: $th(t)=h(t)(tb_0+b_1)$. המקדם העליון של האגף הימני הוא b_0 והפולינום באגף השמאלי הוא פולינום מתוקן ולכן $b_0=1$. חשוב מפורש של השויון האחרון נותן:

$$h(t)(t+b_1)=(t^n+t^{n-1}a_1+\dots+a_n)(t+b_1)=(t^{n+1}+t^na_1+\dots+ta_n)+$$
$$+(t^{n-1}a_1'+\dots+a_n')+(t^nb_1+\dots+a_nb_1)=th(t)$$

לכן:

$$t^{n-1}a_1'+\dots+a_n'+t^nb_1+\dots+a_nb_1=0$$

מכאן: $b_1=0$, כלומר $th(t)=h(t)t$. הפולינום $h(t)$ מתחלף אפוא עם כל אברי החוג $K[t]$.

מהמשפט האחרון אנו למדים שאלת מציאת כל הפולינומים הסופיים של החוג $K[t]$ אקויולנטית למציאת כל הפולינומים המתוקנים השיכים למרכז של החוג $K[t]$. המשפטים הבאים מטפלים במציאת המרכז של החוג $K[t]$.

ידוע[1] החוג $K[t]$ הוא חוג בעל אלגוריתמוס ימני (ושמאלי), כלומר, לכל שני פולינומים $h(t)$, $k(t)\neq 0$ קימים שני פולינומים $q(t)$, $r(t)$ אשר $h(t)=k(t)q(t)+r(t)$ כאשר מעלת $r(t)$ קטנה ממעלת $k(t)$. נוכיח:

משפט-עזר 1. אם הפולינומים $h(t)$, $k(t)\neq 0$ שיכים למרכז של החוג $K[t]$ אזי גם הפולינומים $q(t)$, $r(t)$ שיכים למרכז של $K[t]$.

הוכחה. הפולינומים $h(t)$ ו $k(t)$ מתחלפים עם כל $a\in K$. לכן:

$$ah(t)-h(t)a=k(t)(aq(t)-q(t))a+ar(t)-r(t)a=0$$

ולכן:

$$k(t)(aq(t)-q(t)a)=r(t)a-ar(t)$$

מעלת האגף הימני שוה לכל היותר למעלת הפולינום $r(t)$ ואם $aq(t)-q(t)a\neq 0$ אזי מעלת האגף השמאלי היא לכל הפחות במעלת $k(t)$ הגדולה ממעלת $r(t)$, מה שלא יתכן. לכן $aq(t)-q(t)a=0$, ומכאן $r(t)a-ar(t)=0$.

כיון ש $h(t)$ ו $k(t)$ מתחלפים עם t נקבל:

$$th(t)-h(t)t=k(t)(tq(t)-q(t)t)+tr(t)-r(t)t=0$$

חשוב קל מראה שמעלת הפולינום $tr(t)-r(t)t$ שוה לכל היותר למעלת $r(t)$, ולכן אפשר לקבל בדרך דומה כי: $tq(t)-q(t)t=0$ וכן $tr(t)-r(t)t=0$, מה שהיה להוכיח.

נסמן ב M את המשותף של המרכז של K ושל שדה הקונסטנטות של K. כלומר $c\in M$ כאשר ורק כאשר $c'=0$ וכן $ac=ca$ לכל $a\in K$.

משפט-עזר 2. פולינום $g(t)=t^na_0+t^{n-1}a_1+\dots+a_n$ מתחלף עם t כאשר ורק כאשר $a_i'=0$, $i=0,1,\dots,n$.

ההוכחה נובעת מיד מהעובדה כי: $g(t)t-tg(t)=t^na_0'+t^{n-1}a_1'+\dots+a_n'$.

השדה M מוכל במרכז של החוג $K[t]$, כי M מתחלף עם כל אברי K וכן $c'=ct-tc=0$ לכל $c\in M$. נוכיח:

משפט 2. אם המרכז של החוג $K[t]$ מכיל פולינומים ממעלה שונה מאפס אזי קים פולינום מתוקן $g(t)$ ממעלה $\neq 0$ ואשר המרכז של $K[t]$ מתלכד עם קבוצת כל הפולינומים בעלי הצורה:

$$g(t)^mc_0+g(t)^{m-1}c_1+\dots+c_m \qquad (ב)$$

באשר $c_i\in M$.

הוכחה. יהי $h(t)$ פולינום השיך למרכז $K[t]$. נכתב: $h(t)=k(t)c$ באשר $k(t)$ פולינום מתוקן והאבר c הוא המקדם העליון של $h(t)$ (לכן $c\neq 0$). נראה כי $c\in M$ והפולינום $k(t)$ שיך למרכז של $K[t]$. כי לכל $a\in K$ יהיה: $ah(t)-h(t)a=ak(t)c-k(t)ca=0$. חשוב המקדם הראשון של האגף השמאלי נותן: $ac-ca=0$. כמו כן:

$$0=th(t)-h(t)t=tg(t)c-g(t)ct=tg(t)c-g(t)tc-g(t)c'$$

ואם $g(t)=t^n+t^{n-1}a_1+\dots+a_n$ הרי המקדם של t^n באגף הימני יהיה: $0=a_1c-a_1c-c'=-c'$, זאת אומרת $c'=0$ לכן $c\in M$. כיון ש $c\neq 0$ ושיך למרכז של $K[t]$ יהיה גם $k(t)=h(t)c^{-1}$ שיך למרכז של $K[t]$.

נעבר להוכחת המשפט. יהי $g(t)$ פולינום בעל מעלה מינימלית השונה מאפס השיך למרכז של $K[t]$. נוכל להניח, לאור מה שהוכח זה עתה, שהפולינום $g(t)$ הוא פולינום מתוקן. (קים פולינום כזה כי הנחנו שהמרכז של $K[t]$ מכיל פולינומים ממעלה $\neq 0$). נוכיח לראשונה כי כל פולינום $h(t)$ השיך למרכז של $K[t]$ הוא בעל הצורה (ב). זאת נוכיח בדרך אינדוקציה לגבי מעלת הפולינום $h(t)$. אבר c שיך למרכז של $K[t]$ אם $ac=ca$ לכל $a\in K$ וכן $c'=ct-tc=0$, זאת אומרת אם $c\in M$, ולכן הפולינומים ממעלה אפס השיכים למרכז $K[t]$ הם בעלי הצורה (ב). נניח שהדבר נכון לגבי פולינומים שמעלתם קטנה מ n, ויהי $h(t)$ פולינום ממעלה n השיך למרכז (ברור שהמשפט נכון באפן ריק אם מרכז $K[t]$ איננו מכיל פולינומים ממעלה n), אזי קימים שני פולינומים $q(t)$, $r(t)$ אשר $h(t)=g(t)q(t)+r(t)$ באשר מעלת $r(t)$ קטנה ממעלת $q(t)$. ממשפט-עזר 1 נובע שהפולינום $r(t)$ שיך למרכז של $K[t]$ ובגלל המינימליות של מעלת $g(t)$ נקבל כי: $r(t)=c_m\in M$. מעלת $q(t)$ קטנה ממעלת $h(t)$ ולכן על סמך הנחת האינדוקציה נקבל:

$g(t)=g(t)^{m-1}c_0+\dots+c_{m-1}$ באשר $c_i\in M$ ולכן

$h(t)=g(t)^mc_0+\dots+g(t)c_{m-1}+c_m$, מה שהיה עלינו להראות.

מאידך גיסא, כיון שהפולינום $g(t)$ ואברי M שיכים למרכז של $K[t]$ הרי כל פולינום בעל הצורה (ב) אף הוא שיך למרכז של $K[t]$. ובזה מסתימת הוכחת המשפט.

הפולינום $g(t)$ נקבע באפן חד ערכי עד לידי חבור אבר של השדה M. כי אם $g_1(t)$ הוא פולינום המקים את המשפט הקודם, יהיו מעלות $g_1(t)$ ו $g(t)$ שוות, כי g פולינום ב g_1 ו g_1 פולינום ב g. וכיון ששניהם מתוקנים ו g_1 הוא מטפוס (ב), יהיה: $g_1(t)=g(t)+c$ באשר $c\in M$. להפך, אם $g_1(t)=g(t)+c$, $c\in M$ ברור כי גם $g_1(t)$ יקים את תנאי משפט 2.

3. הבעיה שלנו מצטמצמת אפוא במציאת פולינום מתוקן $g(t)$ בעל מעלה מינימלית גדולה מאפס המתחלף עם כל אברי $K[t]$.

נניח מעתה שהשדה K הוא בעל כרכטריסטיקה $p\neq 0$. במקרה זה, ההתאמה $a\to a^{(m)}$ באשר $m=p^e$ היא גזירה בשדה K, כי: $(a+b)^{(m)}=a^{(m)}+b^{(m)}$, וכן

$$(ab)^{(m)}=\sum_{i=0}^{m}\binom{m}{i}a^{(i)}b^{(m-i)}=a^{(m)}b+ba^{(m)}$$

כי: $\binom{m}{i}=\binom{p^e}{i}=0 \mod p$ לכל $0<i<p^e$.

ידוע[1] (משפט Leibnitz):

$$at^n=t^na+\binom{n}{1}t^{n-1}a'+\dots+\binom{n}{n}a^{(n)} \qquad \text{(I)}$$

ולכן כאשר $m=p^e$ נקבל:

$$at^m=t^ma+a^{(m)} \qquad \text{(II)}$$

כיון שההתאמה $a\to a^{(m)}$, $m=p^e$, היא גזירה בשדה K לכן על סמך (I) ו (II) נקבל:

$$at^{nm}=t^{nm}a+\binom{n}{1}t^{(n-1)m}a^{(m)}+\binom{n}{2}t^{(n-2)m}a^{(2m)}+\dots+a^{(nm)} \qquad \text{(III)}$$

הזהות (III) מוכיחה כי אם h הוא פולינום ב t^m באשר $m=p^e$, כלומר $h=h(t^m)$ אז לכל $a\in K$ גם $ah(t^m)$ הוא פולינום ב t^m. המיוחד, קבוצת כל הפולינומים ב t^m, $m=p^e$ מהוה חוג חלקי של $K[t]$.

כל מספר $n=rp^e$, $r>1$ אפשר לכתבו בצורה: $n=(sp+i)p^e$ באשר $1<i<p$. ולכן

$$t^n=t^{ip^e}(t^{p^{e+1}})^s.$$

מכאן רואים שכל פולינום $h(t)\neq 0$ המכיל רק חזקות של t שהן כפולות אמתיות של $m=p^e$ ולא של p^{e+1} אפשר להציגו בצורה:

$$h(t)=t^{sm}h_o+t^{(s-1)m}h+\dots+h_s \qquad \text{(ג)}$$

באשר $1<s<p$ והמקדמים $h_o\neq 0, h_1,\dots,h_s$ הם פולינומים ב $t^{p^{e+1}}$. קל להוכח שההצגה (ג) היא חד ערכית.

כמו כן, כל פולינום $g(t)\neq 0$ בחוג $K[t]$ אפשר לפרק:

$$g(t)=h(t)+k(t) \qquad \text{(ד)}$$

באשר

$$k(t)=\sum_{i=0}^{e}t^{p^i}a_i+a,\quad e\gtrless 0 \qquad \text{(ד')}$$

ובאשר הפולינום $h(t)\neq 0$ אם $g(t)$ איננו מטפוס הפולינום $k(t)$. במקרה זה $h(t)$ מכיל חזקות של t שהן כפולות אמתיות של p^e. למשל, אם $e=0$; $k(t)$ מכיל את המחוברים של $g(t)$ שמעלתם לכל היותר 1, והפולינום $h(t)$ מכיל את המחוברים של $g(t)$ שמעלתם גדולה מ 1 (אם ישנם כאלה!). אף כאן קל להוכח כי לכל מספר e שעבורו הפרוק (ד) יתכן – הפרוק הוא חד ערכי. לכשנסתכל להבא בפרוקים מטפוס (ד) נתכון למספר e מכסימלי שעבורו יתכן פרוק מטפוס (ד). ואזי הפולינום $h(t)$ כולל חזקות של t שהן כפולות אמתיות של p^e אך לא של p^{e+1}, ולכן הפולינום $h(t)$ נתן להצגה (ג).

---

6) במקרה זה, המקדמים הם פולינומים ב $t^{p^{e+1}}$. ומותר לזהות את המקדמים הללו כי ההצגות (ג) ו (ד) הן חד ערכיות וכן כל פולינום ah_j לכל $a\in K$ הוא פולינום ב $t^{p^{e+1}}$, ו $ak(t)$ הוא פולינום מטפוס (ד').

יהי $g(t)$ פולינום השיך למרכז של $K[t]$, שמעלתו גדולה מאפס. אנו רוצים להוכיח שאם הפולינום $g(t)$ אינו בעל הצורה (ד'), אזי המרכז של $K[t]$ מכיל פולינום שמעלתו קטנה משל $g(t)$ וגדולה מאפס. כי אם $g(t)$ אינו בעל הצורה (ד') נוכל לפרקו כב (ד) ואת $h(t)$ כמו ב (ג), ונקבל:

$$g(t)=t^{sm}h_o+t^{(s-1)m}h_1+\dots+h_s+k(t)$$

כאשר $h_o\neq 0$, $1<s<p$ והמקדמים $h_o, h_1, \dots, h_s$ הם פולינומים ב $t^{p^{e+1}}$.

הפולינום $g(t)$ מתחלף עם כל $a\in K$. לכן:

$$a(t^{sm}h_o+t^{(s-1)m}h_1+\dots+h_s+k(t))=(t^{sm}h_o+t^{(s-1)m}h_1+\dots+h_s+k(t))a$$

נזהה את המקדמים[6] של t^{sm} ונקבל $ah_o=h_oa$. ממשפט עזר 2 רואים כי מקדמי $g(t)$ הם קונסטנטות. לכן גם מקדמי h_o שהם חלק ממקדמי $g(t)$ הם קונסטנטות ועל סמך אותו משפט עזר מתברר שהפולינום $h(t)$ מתחלף גם עם t. מכאן שהפולינום h_o שיך למרכז של $K[t]$. אם h_o איננו קונסטנטה אזי הוא הפולינום הדרוש, דהינו: פולינום ממעלה גדולה מאפס וקטנה ממעלת $g(t)$ השיך למרכז של $K[t]$. כאשר מעלת h_o היא אפס, אזי $h_o=c\in M$. נזהה את המקדמים של $t^{(s-1)m}$ בשויון האחרון ונקבל על סמך (III):

$$sa^{(m)}c+ah_1=h_1a \qquad (h_o=c\neq 0)$$

נסתכל בפולינום t^msc+h_1. פולינום זה מעלתו גדולה מאפס, כי $sc\neq 0$. אך ברור שמעלתו קטנה ממעלת $g(t)$. הפולינום t^msc+h_1 שיך למרכז של $K[t]$, כי: לכל $a\in K$ נקבל על סמך (II):

$$a(t^msc+h_1)=t^masc+a^{(m)}sc+ah_1=t^msca+h_1a=(t^msc+h_1)a$$

כי s ו c שיכים למרכז של K. כמו כן: $(sc)'=sc'=0$ והמקדמים של h_1 הם קונסטנטות כי הם חלק ממקדמי $g(t)$ ולכן נובע ממשפט עזר 2 שהפולינום t^msc+h_1 מתחלף עם k. בזה הוכחנו כי הפולינום t^msc+h_1 שיך למרכז והוא הפולינום הדרוש.

יהי $g(t)$ פולינום מתוקן השיך למרכז של $K[t]$ בעל מעלה מינימלית גדולה מאפס (הפולינום של משפט 2). כיון שהמרכז של $K[t]$ אינו מכיל פולינומים שמעלתם קטנה ממעלת $g(t)$ וגדולה מאפס, לכן לאור מה שהוכחנו זה עתה מתקבל כי הפולינום $g(t)$ הוא מטפוס (ד'), דהינו:

$$g(t)=t^{p^e}+t^{p^{e-1}}a_1+\dots+ta_e+b \qquad \text{(ה)}$$

הפולינום $g(t)$ מתחלף עם t. לכן יוצא ממשפט עזר 2 כי - $a_i'=b'=0$. לכל $a\in K$ קים $ag(t)=g(t)a$. זהוי המקדמים של החזקות של t בשני אגפי הזהות האחרונה נותן על סמך (II): $aa_i=a_ia$, $i=1,\dots,e$ ולכן שיכים המקדמים a_i לשדה M. כמו כן:

$$0=ag(t)-g(t)a=a^{(p^e)}+a^{(p^{e-1})}a_1+\dots+a'a_e+ab-ba$$

לכן אברי K הם פתרונות המשואה הדיפרנציאלית:

$$z^{(p^e)}+z^{(p^{e-1})}a_1+\dots+z'a_e+zb-bz=0 \qquad (ה')$$

מאידך גיסא, אם אברי K הם פתרונות משואה דיפרנציאלית מטפוס (ה') אשר מקדמיה a_i שיכים ל M ו b הוא קונסטנטה, אזי הפולינום $g(t)$ המגדר ב (ה) מתחלף עם אברי החוג $K[t]$. כי t מתחלף עם $g(t)$, מה שמתקבל בעזרת משפט עזר 2. וכיון שאברי K הם פתרונות המשואה (ה'), הרי חשבון קל בעזרת (II) מראה שהפולינום $g(t)$ מתחלף גם עם כל אברי השדה K. ובזה הוכחנו:

משפט 3. המרכז של החוג $K[t]$ מכיל פולינומים ממעלה גדולה מאפס, אם ורק אם אברי השדה K הם פתרונות של משואה דיפרנציאלית מטפוס (ד) וכאשר המשואה (ה') היא בעלת מעלה מינימלית אזי הפולינום $g(t)$ המגדר ב (ה) מקים את תנאי משפט 2.

שלושת המשפטים שהוכחנו נותנים את פתרון הבעיה שהצגנו, והיא מציאת כל הפולינומים הסופיים בחוג $K[t]$ מעל השדה K בעל כרכטריסטיקה $p\neq 0$. והפתרון הוא לכן:

משפט 4. החוג $K[t]$ מכיל פולינומים סופיים מלבד היחידה כאשר ורק כאשר אברי K הם פתרונות של משואה דיפרנציאלית מטפוס (ה'). כאשר המשואה (ד) היא בעלת מעלה מינימלית, יהיה הפולינום $g(t)$ המגדר ב (ה) פולינום סופי וקבוצת כל הפולינומים הסופיים ב $K[t]$ היא קבוצת כל הפולינומים מהצורה:

$$g(t)^m+g(t)^{m-1}c_1+\dots+c_m$$

באשר $c_i \in M$.

הערה. אם נסמן את הגזירה $a \to a'$ ב D, יהיו גם D^m, $m=p^e$ גזירות בשדה K ונוכל להביע את העובדה שאברי K הם פתרונות (ה') באופן הבא: אחת הגזירות מהטפוס:

$$D^{p^e}+D^{p^{e-1}}a_1+\dots+Da,$$

היא גזירה פנימית ב K ומגדרת על ידי b, באשר $b'=bD=0$.

4. נסמן ב K_b את שדה כל האברים המתחלפים עם b, ונסמן ב C_b את שדה כל הקונסטנטות המתחלפות עם b. אם $b'=0$ תהיה הגזירה $a \to a'$ מגדרת גם בשדה K_b. כי לכל $a \in K_b$ מתקים:

$$a'b=a'b+ab'=(ab)'=b'a+ba'=ba'$$

ולכן גם $a' \in K_b$. המקדמים a_i במשואה (ה') שיכים ל M ולכן גם ל C_b. לכן מקבלים אנו שאברי K_b הם פתרונות המשואה הדיפרנציאלית:

$$z^{(p^e)}+z^{(p^{e-1})}a_1+\dots+z'a_e=0 \qquad (A)$$

באשר מקדמי המשואה שיכים לשדה C_b. מכאן[7] השדה K_b הוא מודול ימני (ושמאלי) מעל C_b בעל ממד לכל היותר p^e, כלומר:

---

7) ש. עמיצור, שמושים לתורת המשואות הדיפרנציאליות הליניאריות, רבעון למתמטיקה כרך 1, עמ' 48, משפט 1.

$$(K_b:C_b)\leq p^e.$$

במיוחד, כאשר K שדה קומוטטיבי, אזי $K_b=K$ ו $C_b=C$ ונקבל אפוא שאם החוג $K[t]$ מכיל פולינומים סופיים אזי $(K:C)<\infty$.

מצד שני הראה Jacobson[8] שכאשר שדה קומוטטיבי K הוא בעל גזירה עם שדה קונסטנטות C באשר $(K:C)=p^e$ אזי אברי K הם פתרונות משואה דיפרנציאלית מטפוס (A) ומשואה זו היא מינימלית. לכן:

תוצאה. יהי K שדה קומוטטיבי בעל כרכטריסטיקה $p\neq 0$. החוג $K[t]$ מכיל פולינומים סופיים מלבד היחידה כאשר ורק כאשר $(K:C)=p^e<\infty$. הפולינומים הסופיים נקבעים לפי משפט 4.

5. הבעיה שטפלנו בה היא מקרה פרטי של הבעיה הבאה:

יהי K שדה (לאו דוקא קומוטטיבי) בעל אוטומורפיזם S ובעל S-גזירה. כלומר K הוא בעל אוטומורפיזם S והתאמה $a\to a_S$, באשר:

$$1)\ (a+b)_S=a_S+b_S,\quad 2)\ (ab)_S=a_Sb^S+ab_S\ .$$

באשר b^S היא תמונת b באוטומורפיזם S. אף כאן מציינים אנו ב $K[t]$ את חוג כל הפולינומים ב t עם מקדמים מתוך K הכתובים מימין לחזקות של t, והכפל מגדר ב $K[t]$ על ידי: $at=ta^S+a_S$ לכל $a\in K$. פולינום $g(t)$ הוא פולינום סופי ב $K[t]$ אם $g(t)$ פולינום מתוקן והאידיאל הימני הנוצר על ידי $g(t)$ הוא אידיאל דו צדדי. הבעיה הכללית היא למצוא את כל הפולינומים הסופיים בחוג $K[t]$. חשיבותם של הפולינומים הסופיים היא שמושם בתורת המטריצות מעל השדה K (עין Jacobson[3]).

Jacobson פתר את הבעיה בשני מקרים[9]: א) $K[t]$ הוא חוג הפולינומים הליניאריים למחצה, דהינו $a_S=0$ וקים $at=ta^S$ לכל $a\in K$. ב) חוג הפולינומים הדיפרנציאלי ($a^S=a$) מעל שדה בעל כרכטריסטיקה אפס. בעבודה זו הבאנו פתרון לבעיה כאשר $K[t]$ הוא חוג הפולינומים הדיפרנציאליים מעל שדה בעל כרכטריסטיקה סופית. ועדין הבעיה הכללית נשארה פתוחה.

---

8) N. Jacobson, Abstract derivation and Lie algebras, Trans. Am. Math. Soc. 42 (1937), pp. 206-224.

9) עין למשל ב 3) או בספרו של Jacobson: Theory of rings פרק III הוצאת Am. Math. Soc.

Finite differential polynomials

Shimshon Amitsur

(Summary)

The object of the present communication is to determine the finite differential polynomials over a quasi-field of characteristic $p\neq 0$. The case of characteristic zero was determined by Jacobson[3].

Let K be a quasi-field of characteristic $p\neq 0$ with a derivation $a\to a'=aD$. Denote by $K[t]$ the ring of all diferential polynomials over K, that is, $K[t]$ is the ring of all polynomials in t with coefficients in K written on the right of the powers of t and the multiplication is defined in $K[t]$ by: $at=ta+a'$ for each $a\in K$.

A polynomial $g(t)$ is a finite polynomial if the right ideal $g(t)K[t]$ is a two sided ideal and the highest coefficient of $g(t)$ is 1. The following result is proved: The ring $K[t]$ contains finite polynomials exept the unity if and only if the elements of K satisfy a differential equation of the type:

(A) $$z^{(p^e)}+z^{(p^{e-1})}a_1+\dots+z'a_e+zb-bz=0$$

where $b'=a_i'=0$ and the coefficients a_i commutes with the elements of K. That is, the derivation $D^{p^e}+D^{p^{e-1}}a_1+\dots+Da_e$ is an inner derivation in K.

Let equation (A) be a differential equation of minimum degree of that type which is satisfied by the elements of K. Then, the polynomial $g(t)=t^{p^e}+t^{p^{e-1}}a_1+\dots+ta_e+b$ is a finite polynomial and each polynomial $h(t)\neq 1$ is finite if and only if $h(t)=g(t)^m+g(t)^{m-1}c_1+\dots+c_m$ where c_i are constants which belongs to the centre of K. The set of the finite polynomials of $K[t]$ coincides with the set of the polynomials with the highest coefficient 1 which belong to the centre of $K[t]$.

Let K be a commutative field of characteristic $p\neq 0$, then by a theorem of Jacobson[8] we obtain the following corollary:

The ring of all differential polynomials $K[t]$ over a commutative field of characteristic $p\neq 0$ contains finite polynomials of degree $m>0$ if and only if $(K:C)=p^e<\infty$, where C is the field of constants of K. The finite polynomial of minimum non-zero degree is of degree p^e.

משפט Wolstenholme והכללותיו

נתן אליוסף (קבקר)

1. הדבר המציין את הגישה לבעיות הקשורות למשפט Wolstenholme במאמר זה הוא כי אני משתמש באופן שיטתי בעובדה כי באי-כח מחלקות השאריות הזרות ל-m יוצרים חבורה.

2. במאמר זה אשתמש בסימנים הבאים:

(א) HW יסמן את הספר:
Hardy-Wright: An Introduction to the Theory of Numbers, 1938.

(ב) p יציין מספר ראשוני א י ז ו ג י .

(ג) m יציין מספר טבעי, $Z(m)$ את קבוצת $\varphi(m)$ המספרים הקטנים מ-m וזרים לו. $Z(m)=t_1,\dots,t_{\varphi(m)}$.

(ד) $S_k(m)=\sum_{t\in Z(m)} 1/t^k$; $T_k(m)=\sum_{t\in Z(m)} t^k$ כלומר: $S_k(m)=T_{-k}(m)$.

(ה) מספרי Bernoulli יסומנו לפי דרכו של E. Lucas.

(ו) C-S יסמן את משפט Clausen-Staudt על מספרי Bernoulli.

פרק ראשון: $T_k(m) \bmod m$.

3. אם $t\in Z(m)$ יש לקונגרואנציה $tx\equiv 1 \bmod m$ פתרון יחיד אם נדרוש $1\leq x\leq m-1$.
לפתרון הזה נקרא $\frac{1}{t}$ וברור כי $\frac{1}{t}\in Z(m)$, וכמו-כן כי $Z(m)=\frac{1}{t_1},\dots,\frac{1}{t_{\varphi(m)}}$.

מכאן, למשל:

משפט: $S_k(m)\equiv T_k(m) \bmod m$.

בגלל משפט זה מספיק יהיה, בפרק זה, לטפל ב $T_k(m)$.

4. משפט: אם $m>2$ אז $S_{2a-1}(m)\equiv T_{2a-1}(m)\equiv 0 \bmod m$.

ה ו כ ח ה : ברור כי $T_{2a-1}(m)=\sum_t (m-t)^{2a-1}$.

א) נניח כי m אי־זוגי. $T_{2a-1}(m)\equiv -\sum_t t^{2a-1}\equiv -T_{2a-1}(m) \bmod m$. לכן $m|2T_{2a-1}(m)$. מכיון ש- m אי־זוגי נובעת הטענה מיד.

ב) m זוגי.

$$T_{2a-1}(m)=\sum_t \sum_{i=0}^{2a-1}(-1)^i\binom{2a-1}{i}m^{2a-1-i}t^i$$

ולכן:

$$\frac{2T_{2a-1}(m)}{m}=m^{2a-2}\varphi(m)+\sum_{i=1}^{2a-2}(-1)^i m^{2a-2-i}T_i(m)=\text{מספר שלם}$$

מאחר ש-m זוגי, ואף $\varphi(m)$ זוגי כאשר $m>2$ לכן:

$$\frac{2T_{2a-1}(m)}{m}\equiv T_{2a-2}(m) \bmod 2$$

אם m זוגי, כל איברי $Z(m)$ הם אי־זוגיים ומספרם $\varphi(m)$ ולכן

$$T_{2a-2}(m)\equiv\sum_t 1=\varphi(m)\equiv 0 \bmod 2.$$

בזה הוכח המשפט במלואו.

5. נשאר אפוא לטפל ב-$T_{2a}(m)$. רוב הטפול הבא כחו יפה עבור $T_k(m)$ כאשר איזוגי.

6. נניח כי $m=p^e$.

$Z(p^e)$ מכיל את המספרים הקטנים מ-p^e פרט לאלה המתחלקים ב-p. לכן:

$$T_k(p^e)=[1^k+\dots+(p^e-1)^k]-p^k[1^k+\dots+(p^{e-1}-1)^k] \qquad (1)$$

אם נשתמש בנוסחת Bernoulli נקבל:

$$(k+1)T_k(p^e)=p^{ek}\varphi(p^e)+\sum_{i=1}^{k}\binom{k+1}{i}p^{ei}B_{k+1-i}(1-p^{k-i}) \qquad (2)$$

אם נביא בחשבון כי $\frac{1}{k+1}\binom{k+1}{i}=\frac{1}{i}\binom{k}{i-1}$ נוכל לכתוב:

$$T_k(p^e)=p^{ek}\frac{\varphi(p^e)}{k+1}+p^eB_k(1-p^{k-1})+\sum_{i=2}^{k}\frac{1}{i}\binom{k}{i-1}p^{ei}B_{k+1-i}(1-p^{k-i}) \qquad (3)$$

על-פי C-S מכילים מספרי Bernoulli את p במכנה בחזקה שאינה עולה על הראשונה, לכן ב-(3) כדי שכל מחובר בסכום יתחלק ב-p^e נחוץ כי $\frac{p^{ei-1}}{i}\equiv 0 \mod p^e$. אם i אינו מתחלק ב-p הדבר ברור כי $i\geq 2$. אחרת נניח כי $i=p^nj$ כאשר j זר ל-p. צריך אפוא להתקיים $ep^nj-1-n\geq e$ כלומר $e(p^nj-1)\geq n+1$. זה בודאי יתקיים אם $p^n-1\geq n+1$ או $p^n\geq n+2$. אי-שויון זה מתקיים כאשר $n=1$ ולא כל-שכן כאשר n גדול יותר. לכן מתחלק הסכום ב-(3) ב-p^e. באופן דומה רואים כי המחובר הראשון ב-(3) מתחלק ב-p^e. נשאר:

$$T_k(p^e)\equiv p^eB_k \mod p^e \qquad (4)$$

מכאן, על סמך C-S נקבל:

משפט: א) אם $p-1\nmid k$ יהיה $T_k(p^e)\equiv 0 \mod p^e$.

ב) אם $p-1|k$ יהיה $T_k(p^e)\equiv\varphi(p^e) \mod p^e$.

ג) תמיד $T_k(p^e)\equiv 0 \mod p^{e-1}$.

7. הערה: את החלק א) של המשפט ב-§6 נוכל לקבל בלי C-S בצורה הבאה:

יש שרש פרימיטיבי g mod p^e כך שנוכל לכתוב (בעזרת משפט Euler-Fermat):

$$(g^k-1)T_k(p^e)\equiv(g^k-1)\sum_{s=0}^{\varphi(p^e)-1}(g^s)^k\equiv g^{k\varphi(p^e)}-1\equiv 0 \mod p^e$$

נשאר להוכיח כי $g^k-1\not\equiv 0 \mod p$. ואמנם, אילו היה $g^k\equiv 1 \mod p$ היינו מקבלים $g^{k\cdot p^{e-1}}\equiv 1 \mod p^e$. מכיון ש-$g$ שרש פרימיטיבי נובע כי $\varphi(p^e)|kp^{e-1}$ כלומר $p-1|k$ בנגוד להנחה.

8. נגמור קודם את המקרה של המספר הראשוני 2. נניח כי $m=2^e n$ וכי n אי-זוגי. נוכיח כי:

$$T_{2a}(2^e n)\equiv 2T_{2a}(2^{e-1}n) \mod (2^e n) \quad \text{כאשר } e\geq 2 \qquad (5)$$

הוכחה:

$$T_{2a}(m)=\sum_t t^{2a}=\sum_{t<m/2} t^{2a}+\sum_{t>m/2} t^{2a}=\sum_{t<m/2}\{t^{2a}+(m-t)^{2a}\}$$

$$T_{2a}(m)\equiv 2\sum_{t<m/2} t^{2a} \mod m \qquad (6)$$

אם $e\geq 2$ הרי כל t הקטן מ-$m/2=2^{e-1}n$ וזר ל-m זר גם ל-$m/2$ וגם ההפך נכון, לכן $T_{2a}(2^{e-1}n)=\sum_{t<m/2} t^{2a}$. בזה הוכח (5).

אם נשתמש ב-(5) e-1 פעמים נקבל:

$$T_{2a}(2^e n)\equiv 2^{e-1}T_{2a}(2n) \mod (2^e n) \qquad (7)$$

נציב n=1 בתוך (7) ונקבל: $T_{2a}(2^e)\equiv 2^{e-1} \mod 2^e$ מה שמתאים לחלק ב' של המשפט ב-§6 עבור המקרה p=2.

נניח כי n>1. כמו (6) נוכל לכתוב:

$$T_{2a}(2^e n)\equiv 2^e\sum_{t<n/2} t^{2a} \mod (2^e n)$$

משפט: אם $m=2^e n$ (n>1 אי-זוגי) אז $T_{2a}(m)\equiv 0 \mod 2^e$.

9. נניח כי p^e מופיע כגורם בהצגה הקנונית של m (כמכפלת מספרים ראשוניים) ונסמן $m=p^e m_1$ ($p\nmid m_1$). כמו-כן נסמן $Z(m_1)=\{t_1,\dots,t_{\varphi_1}\}$ כאשר $\varphi_1=\varphi(m_1)$.

נבנה את המטריצה:

$$M(e)=\begin{pmatrix} t_1 & \dots & t_{\varphi_1} \\ m_1+t_1 & \dots & m_1+t_{\varphi_1} \\ \dots & \dots & \dots \\ (p^e-1)m_1+t_1 & \dots & (p^e-1)m_1+t_{\varphi_1} \end{pmatrix}$$

כאן $t_{\varphi_1}=m_1-1$,$t_1=1$ ולכן, למשל, $(p^e-1)m_1+t_{\varphi_1}=p^e m_1-1=m-1$.

נסמן על-ידי $M_k(e)$ את סכום כל איברי המטריצה $M(e)$ כשכל איבר לקוח בחזקת k. המטריצה $M(e)$ מכילה את כל המספרים הקטנים מ-m וזרים ל-m_1. כדי לקבל את $Z(m)$ יש למחוק את כל האיברים המתחלקים ב-p, כלומר את המספרים $pt_1,\dots,pt_{\varphi_1},\dots$. האחרון יהיה $p^e m_1-p$ כלומר $p[(p^{e-1}-1)m_1+t_{\varphi_1}]$. מכאן רואים שמהמטריצה $M(e)$ יש למחוק את איברי המטריצה $pM(e-1)$ (כפל מספר המטריצה). מכאן נובע:

$$T_k(m)=M_k(e)-p^k M_k(e-1) \qquad (8)$$

נחשב את $M_k(e)$. נחבר את האיברים בעמוד ה-r כשכל אחד לקוח בחזקת k

ואחר כך את סכום כל העמודים. נציב לתוך (8) ונביא בחשבון את (1). נקבל:

$$T_k(m)=p^eT_k(m_1)(1-p^{k-1})+\sum_{j=1}^{k}\binom{k}{j}m_1{}^jT_{k-j}(m_1)T_j(p^e) \qquad (9)$$

10. נעבור אל $T_k(m) \bmod p^e$ בעזרת (9). נציב את (4) ונקבל:

$$T_k(m)\equiv p^{e-1}\sum_{j=1}^{k}\binom{k}{j}m_1{}^jT_{k-j}(m_1)\cdot pB_j \bmod p^e.$$

את הסכום נוכל להעריך $\bmod p$. בגלל C-S אין זה חשוב מה הם ערכי $m_1{}^j$ ו-$T_{k-j}(m_1)$ פרט למחוברים שעבורם $p-1|j$. בשביל מחוברים אלה יהיה $m_1{}^j\equiv 1 \bmod p$ ואם $k-j\neq 0$ יהיה $T_{k-j}(m_1)=\sum_t t^{k-j}\equiv\sum_t t^k=T_k(m_1) \bmod p$. המקרה $k=j$ יתכן רק אם $p-1|j$. לכן נצטרך להבחין בין שני מקרים:

א) $p-1\nmid k$.

$$T_k(m)\equiv p^eT_k(m_1)\sum_{j=1}^{k}\binom{k}{j}B_j=p^eT_k(m_1)[(1+B)^k-1]=p^eT_k(m_1)(B_k-1)\equiv 0 \bmod p^e.$$

ב) $p-1|k$ ($T_0(m_1)=\varphi(m_1)$).

$$T_k(m)\equiv p^eT_k(m_1)\sum_{j=1}^{k}\binom{k}{j}B_j-p^eT_k(m_1)\binom{k}{k}B_k+p^e\varphi(m_1)B_k \bmod p^e$$

אם נחשב את הבטוי השמאלי כמו במקרה א) נקבל:

$$T_k(m)\equiv p^{e-1}\varphi(m_1)pB_k \bmod p^e$$

על-סמך C-S: $pB_k\equiv -1 \bmod p$ ולכן: $T_k(m)\equiv (m) \bmod p^e$.

משפט: א) אם $p-1\nmid k$ יהיה $T_k(m)\equiv 0 \bmod p^e$.
ב) אם $p-1|k$ יהיה $T_k(m)\equiv (m) \bmod p^e$.
ג) תמיד $T_k(m)\equiv 0 \bmod p^{e-1}$.

הערה: כדי ש-$T_k(m)\equiv 0 \bmod p^e$ כאשר $p-1|k$ הכרחי ומספיק כי יהיה מספר ראשוני p' המחלק את m והמקיים $p'\equiv 1 \bmod p$.

11. בעזרת המשפט של §8 נקבל על-סמך §10:

משפט א': אם $m=2^e\prod p_i^{e_i}$ ההצגה הקנונית של m ואם $m\neq 2^e$ יהיה $T_k(m)\equiv 0 \bmod m$ אז ורק אז אם כל p_i המקיים $p_i-1|k$ יהיה עבורו גם $p_i'|m$ המקיים $p_i'\equiv 1 \bmod p_i$.

משפט ב': אם כל $p|m$ מקיים את התנאי $p-1|k$ אז $T_k(m)\equiv\varphi(m) \bmod m$.

את המשפט הכללי נקבל אם נשתמש במושג הבא:

הגדרה: מספר ראשוני p יקרא בשם מספר ראשוני סנגולרי לגבי הזוג המסודר m,k אם (i) $p|m$ (ii) $p-1|k$ (iii) אין $p'|m$ המקיים $p'\equiv 1 \bmod p$. את מכפלת המספרים הראשוניים הסנגולריים נסמן על-ידי $P_k(m)$. אם אין מספרים ראשוניים סנגולריים נקח: $P_k(m)=1$. בסך-הכל נקבל:

משפט ג': $T_k(m)\equiv 0 \bmod m/P_k(m)$.

ה ע ר ה : המשפט ההפוך ל-ג' גם-כן נכון, כלומר אם $T_k(m)\equiv 0 \bmod m/A$ נובע כי $P_k(m)|A$.

פרק שני: $T_{2a-1}(m) \bmod m^2$.

12. מ-§4 נקבל $2T_{2a-1}(m)/m\equiv m^{2a-2}\varphi(m)+(2a-1)T_{2a-2}(m) \bmod m$. לכן, אם $a>1$ יהיה:

$$2T_{2a-1}(m)\equiv(2a-1)mT_{2a-2}(m) \bmod m^2 \qquad (10)$$

מכאן, על-סמך §11 נקבל:

משפט: אם m אי־זוגי, $T_{2a-1}(m)\equiv 0 \bmod m^2/Q_a(m)$; ואם m זוגי, $T_{2a-1}(m)\equiv 0 \bmod m^2/2Q_a(m)$. כאן מציין $Q_a(m)$ את מכפלת המספרים הראשוניים הסנגולריים לגבי הזוג המסודר m, $2a-2$ אשר אינם מחלקים את $2a-1$. פה $a>1$. אם $a=1$, הרי $T_1(m)=m\varphi(m)/2$ ולכן רק $T_1(m)\equiv 0 \bmod m^2/\prod p_i$.

13. לפי משפט Fermat-Euler נקבל:

$$S_{2a-1}(m)=\sum_t 1/t^{2a-1}\equiv\sum_t t^{\varphi(m^2)(2a-1)}/t^{2a-1}$$

$$=\sum t^{(2a-1)[\varphi(m^2)-1]}=T_{(2a-1)[\varphi(m^2)-1]} \bmod m^2$$

לכן, לפי (10) נקבל:

$$2S_{2a-1}(m)\equiv-(2a-1)mT_{(2a-1)[\varphi(m^2)-1]-1} \bmod m^2$$

די לטפל ב-T רק $\bmod m$. לכן לפי משפט Fermat-Euler ולפי §3 נובע כי

$$T_{(2a-1)[\varphi(m^2)-1]-1}\equiv T_{(2a-1)\varphi(m^2)-2a}\equiv\sum 1/t^{2a}=S_{2a}(m)\equiv T_{2a}(m).$$

בסך-הכל:

$$2S_{2a-1}(m)\equiv-(2a-1)mT_{2a}(m) \bmod m^2 \qquad (11)$$

אם נסמן על-ידי $R_a(m)$ את מכפלת המספרים הראשוניים הסנגולריים לגבי הזוג המסודר m, $2a$ אשר אינם מחלקים את $2a-1$, נקבל:

משפט: אם m אי־זוגי, $S_{2a-1}(m)\equiv 0 \bmod m^2/R_a(m)$; ואם m זוגי, $S_{2a-1}(m)\equiv 0 \bmod m^2/2R_a(m)$.

ה ע ר ה : המשפט ההפוך גם-כן נכון, כלומר מתוך $S_{2a-1}(m)\equiv 0 \bmod m^2/A$ עבור m אי־זוגי או $S_{2a-1}(m)\equiv 0 \bmod m^2/2A$ עבור m זוגי נובע כי $R_a(m)|A$.

14. נרשום את המשפט של §13 בשביל מקרים מיוחדים. L יסמן את משפט Leudesdorf.

משפט א': אם $m=2^e$ נובע $S_{2a-1}(m)\equiv 0 \mod m^2/4$.

ה ע ר ה : זאת הכללה של HW(8.7.5) שהוא אחד המקרים של L.

משפט ב': אם $a=1$ יהיה $p=3$ המספר הראשוני האיזוגי היחידי המקיים $2a|p-1$. באופן כזה נקבל את שאר המקרים של L. (ראה (8.7.1-4) של HW).

משפט ג': ההערה למשפט ב-§13 כראה שהמשפט המזכר שם איננו רק הכללה של L אלא גם כי הוא ההכללה <u>הטובה ביותר האפשרית</u>. רואים גם ש-L אינו מראה על ההתחלקות החזקה ביותר, שתתן את השארית הנדונה בכל מקרי HW.

15. אם אין מספר ראשוני סנגולרי לזוג המסודר $m,2a$ יהיה $S_{2a-1}(m)\equiv 0 \mod m^2$, עבור m איזוגי. זה יהיה, למשל, אם $m=p^e$ כאשר $2a\nmid p-1$.

משפט: אם $m=p^e$ אז $S_{2a-1}(m)\equiv 0 \mod m^2$ כאשר $2a\nmid p-1$.

ה ע ר ה 1 . אם $a=e=1$ זהו משפט Wolstenholme. (ראה משפט 115 HW).

ה ע ר ה 2 . אם $2a<p-1$ בודאי יהיה $2a\nmid p-1$. זהו משפט 131 HW, כאשר $e=1$.

16. את משפט Wolstenholme עצמו אפשר לקבל בקלות בלי C-S ובלי המושג של שרש פרימיטיבי, בצורה הבאה:

נסמן:

$$S=\sum_{n=1}^{p-1}\frac{1}{n}=\sum_{n=1}^{p-1}\frac{1}{p-n}$$

$$2S=\sum_{n=1}^{p-1}\left(\frac{1}{n}+\frac{1}{p-n}\right)=p\sum_{n=1}^{p-1}\frac{1}{n(p-n)}=-pS'$$

אם $p>2$ די להראות כי הסכום האחרון מתחלק ב-p. ואמנם $\mod p$ נקבל:

$$S'\equiv\sum_{n=1}^{p-1}1/n^2\equiv\sum_{n=1}^{p-1}n^2=\frac{(p-1)p(2p-1)}{6}\equiv 0 \mod p$$

כאשר $p>3$. (ראה גם §3).

(השוה להוכחת זכאי ברבעון זה, כרך 3, עמ' 58).

Extensions of Wolstenholme's Theorem

Nathan Eljoseph

(Summary)

N o t a t i o n s . Let $S_k(m)$ and $T_k(m)$ resp. denote the expressions $\sum_t 1/t^k$ and $\sum_t t^k$ where $t \in Z(m)$ and $Z(m)$ is the group of the integers less than m and coprime to m. An odd prime p is called a singular prime of the ordered pair m,k if (i) $p|m$, (ii) $p-1|k$, (iii) there is no $p'|m$ for which $p' \equiv 1 \bmod p$. The product of the singular primes is denoted by $P_k(m)$. If there is no singular prime then $P_k(m)=1$.

In this paper the following theorems are proved:

G r o u p A .

Theorem 1. $T_k(m) \equiv 0 \bmod m/P_k(m)$.

Theorem 2. If $T_k(m) \equiv 0 \bmod m/A$ then $P_k(m)|A$. Hence, Theorem 1 supplies a best possible divisor of $T_k(m)$.

Theorem 3. $S_{2a-1}(m) \equiv 0 \bmod m$. This is a special case of Theorem 1.

Theorem 4. If for each $p|m$ (odd p) $p-1|k$ then $T_k(m) \equiv \varphi(m) \bmod m$.

G r o u p B .

Theorem 5. For an odd m, $S_{2a-1}(m) \equiv 0 \bmod m^2/R_a(m)$ and for an even m, $S_{2a-1}(m) \equiv 0 \bmod m^2/2R_a(m)$. Here $R_a(m)$ is the product of the singular primes of the ordered pair m,2a not dividing 2a-1 (or 1 if there is no such prime).

Theorem 6. If for an odd m, $S_{2a-1}(m) \equiv 0 \bmod m^2/A$, or for an even m, $S_{2a-1}(m) \equiv 0 \bmod m^2/2A$, then $R_a(m)|A$.

It is easily seen that Theorem 5 is an extension of Wolstenholme's and Leudesdorf's Theorems. Theorem 6 shows that this extension is the best possible one. It also shows that for a=1 Leudesdorf's Theorem is not the best extension possible of Wolstenholme's Theorem in all its five cases. (See: Hardy-Wright, An Introduction to the Theory of Numbers, Chap. 8).

Method of Proof: $T_k(p^e)$ is calculated by means of Bernoulli's Theorem and the nature of $T_k(p^e) \bmod p^e$ follows using the Clausen-Staudt Theorem on the numbers of Bernoulli. The theorems of Group A are obtained with the help of the following identity:

$$T_k(m)=p^e T_k(m_1)(1-p^{k-1})+\sum_{j=1}^{k}\binom{k}{j} m_1^{\,j} T_{k-j}(m_1) T_j(p^e) \text{ where } m=m_1p^e \text{ and } p\nmid m_1.$$

The theorems of Group B follow from those of Group A by the following congruence: $2S_{2a-1}(m) \equiv -(2a-1)mT_{2a}(m) \bmod m^2$.

A simple proof of Wolstenholme's Theorem is added. Let $S=\sum_{n=1}^{p-1}\frac{1}{n}$ then $2S=\sum_{n=1}^{p-1}\left(\frac{1}{n}+\frac{1}{p-n}\right)$ or $2S=p\sum_{n=1}^{p-1}\frac{1}{n(p-n)}$. We are to prove that $\sum_{n=1}^{p-1}\frac{1}{n(p-n)} \equiv 0 \bmod p$ or $\sum_{n=1}^{p-1} 1/n^2 \equiv 0 \bmod p$. But, mod p the integers 1,2,...,p-1 form a multiplicative group, hence $\sum_{n=1}^{p-1} 1/n^2 \equiv \sum_{n=1}^{p-1} n^2 = (p-1)p(2p-1)/6 \equiv 0 \bmod p$ for $p>3$.

הוכחה פשוטה למשפט לוידסדורף
במקרים של מודול בלתי מתחלק ב6

שלמה זכאי ודב ירדן

משפט לוידסדורף. מונה השבר

$$S=\sum_{x=1}^{m}{}'\frac{1}{x}=\sum_{(x,m)=1;\,1\leq x\leq m}\frac{1}{x}$$

מתחלק ב $\left.\begin{matrix} m^2 \\ m^2/3 \\ m^2/4 \\ m^2/2 \\ m^2/6 \end{matrix}\right\}$ אם

(1) $(m,6)=1$

(2) $(m,6)=3$

(3) $m=2^a$

(4) $m=2^a(6n\pm1)$, $a\ 0,\ n\ 0$

(5) $6|m$

הוכחה.

$$S=\sum_{x=1}^{m/2}{}'\left(\frac{1}{x}+\frac{1}{m-x}\right)=m\sum_{x=1}^{m/2}{}'\frac{1}{x(m-x)}=mS'$$

$$S'=\sum_{x=1}^{m/2}{}'\frac{1}{x(m-x)}=S''$$

$$S''=\sum_{x=1}^{m/2}{}'\frac{1}{y(m-y)},\quad y=qx \Leftrightarrow x<\frac{m}{q},\quad y=qx-m \Leftrightarrow x>\frac{m}{q},\quad (q,m)=1$$

$$(q^2-1)S'=q^2S''-S'=\sum_{x=1}^{m/2}{}'\left(\frac{q^2}{y(m-y)}-\frac{1}{x(m-x)}\right)$$

$$=\sum_{x=1}^{m/2}{}'\frac{q^2xm-q^2x^2-ym+y^2}{y(m-y)\cdot x(m-x)}$$

$$=m\left(\sum_{x=1}^{m/q}{}'\frac{q-1}{(m-y)x(m-x)}+\sum_{x=m/q}^{m/2}{}'\frac{(q-3)qx+2m}{\cancel{y(m-y)x}(m-x)}\right)$$

$$S'=\frac{m}{q+1}\left(\sum_{x=1}^{m/q}{}'\frac{1}{x(m-x)(m-qx)}+\frac{1}{q-1}\sum_{x=m/q}^{m/2}{}'\frac{(q-3)qx+2m}{x(m-x)(qx-m)(2m-qx)}\right)$$

בשביל $q=2,3$ נקבל בהתאמה

$$S_2'=\frac{m}{3}\sum_{x=1}^{m/2}{}'\frac{1}{x(m-x)(m-2x)}$$

$$S_3'=\frac{m}{4}\left(\sum_{x=1}^{m/3}{}'\frac{1}{x(m-x)(m-3x)}+m\sum_{x=m/3}^{m/2}{}'\frac{1}{x(m-x)(3x-m)(2m-3x)}\right)$$

המקרים (1), (2) נובעים ישר מתוך S_2'. המקרה (3) נובע ישר מתוך S_3'.
המקרה (4) נובע מתוך S_3' ומשפט-העזר הבא:

משפט-עזר 1. המונה בסכום השברים

$$\sum_{x=1}^{m/3}{}' \frac{1}{x(m-x)(m-3x)},\quad m=2^a(6n\pm1),\ n>0$$

הוא מספר זוגי.

הואיל ומכנה כל שבר הוא מספר אי-זוגי, די להוכיח

משפט-עזר 2. המספר $\varphi(m,m/3)$ של המספרים הזרים ל-m וקטנים מ-$m/3$ הוא מספר זוגי, אם $m=2^a(6n\pm1)$, $n>0$.

הוכחה. נוכיח לראשונה כי קים
$$\varphi(m,m/3)=\sum_{d|u}\mu(d)z(d),\quad u=6n\pm1$$
(μ - פונקצית מביוס) באשר $z=z_m(d)$ מסמן את מספר המספרים אי-הזוגיים המתחלקים ב-d וקטנים מ-$m/3$. באמת, $\varphi(m,m/3)$ שוה בעליל להבדל בין מספר כל המספרים אי-הזוגיים הקטנים מ-$m/3$ לבין אותם מהם שאינם זרים ל-m. הבדל זה שוה ל-$z(1)-z(p)$; אם $u=p^b$; ל-$z(1)-[z(p)+z(q)]+z(pq)$, אם $u=p^bq^c$; ל-$z(1)-[z(p)+z(q)+z(r)]+[z(pq)+z(pr)+z(qr)]-z(pqr)$, אם $u=p^bq^cr^e$, p,q,r מספרים ראשוניים שונים, וכן הלאה. במקרה של τ גורמים ראשוניים שונים נקבל $\tau+1$ סכומים, חיוביים ושליליים לסרוגין, של מחוברים חיוביים. הסכום ה-ρ-י ($\rho=0,\dots,\tau$) מכיל את כל המחוברים $z(x)$, באשר x שוה למכפלת ρ גורמים ראשוניים שונים. מספר המחוברים בסכום ה-ρ-י הוא $\binom{\tau}{\rho}$.[1]
המספרים אי-הזוגיים $d_1,\dots,d_z$ המתחלקים במחלק d של u וקטנים מ-$m/3$ מהוים סדרה חשבונית בעלת אבר ראשון d, הבדל $2d$ ואבר אחרון $d_z=(m-d)/3$ או $d_z=(m-5d)/3$ (כי אחד מבין שלושת האברים העוקבים $m-d, m-3d, m-5d$ מוכרח להתחלק ב-3, ו-$m-3d$ אינו מתחלק ב-3). מכאן
$$z=z(d)=(2^{a-1}(u/d)\pm1)/3$$
אם $a=1$, יהיה $z(d)=\frac{(u/d)\pm1}{3}$ זוגי לכל מחלק של u. במקרה זה הסכום $\sum_{d|u}\mu(d)z(d)$ זוגי. אם $a>1$, יהיה $m\geqslant4u>3u\geqslant3d$, כלומר $d<m/3$ ו-$z(d)$ הוא אי-זוגי $\neq0$ לכל מחלק של u. מספר המחוברים של $\sum_{d|u}\mu(d)$, ולכן גם של $\sum_{d|u}\mu(d)z(d)$, הוא 2^τ, באשר τ הוא מספר המספרים הראשוניים השונים המוכלים ב-u. במקרה של $a>1$ מכיל אפוא הסכום $\sum_{d|u}\mu(d)z(d)$ מספר זוגי של מחוברים אי-זוגיים, ועל כן הוא שוב זוגי, מה שמשלים את הוכחת המשפט.

---

1) השויון בין ההבדל הנ"ל לבין הסכום של $\tau+1$ הסכומים האלה נובע מהעובדה כי כל מספר הזר ל-u מופיע בסכומים המדוברים פעם אחת בלבד, ולעומת זאת כל מספר שאינו זר ל-u, ז"א המתחלק ב-λ (בדיוק) מהמספרים $p,q,r,\dots$, מופיע בסכום ה-ρ-י $(-1)^\rho\binom{\lambda}{\rho}$ פעמים, ולכן בסה"כ $\sum_{\rho=0}^{\lambda}(-1)^\rho\binom{\lambda}{\rho}=(1-1)^\lambda=0$ פעמים.

Simple proof of Leudesdorf's theorem
in cases of a modul non-divisible by 6

Shlomo Zakay and Dov Jarden

(Summary)

Zakay's method of proving the theorem of Wolstenholme (Riveon Lematematika 3, p. 58-59) is here generalized to prove Leudesdorf's theorem, in cases of a modul non-divisible by 6. The proof follows immediately from certain identities, in cases of an odd modul or of a modul being a power of 2, but it requires an auxiliary lemma otherwise.

הוכחה אלטרנטיבית למשפט אכויבלנציה בנוגע לאכסיומות של המספרים הטבעיים

ברוך גרמנסקי

א. בעבודה זו אנחנו נותנים הוכחה אלטרנטיבית למשפט על האכויבלנציה של מערכת האכסיומות א. לביסוס המספרים הטבעיים המובאת בעבודתי "מערכת אכסיומות חדשה לביסוס תורת המספרים הטבעיים" (הופיעה ב"רבעון למתמטיקה" כרך 3 (1949), עמ' 65) עם מערכת האכסיומות של פ א נ ו . לשם השלמות אנחנו מביאים פה גם אותם חלקי ההוכחה שאינם שונים בהרבה מהחלקים המקבילים בעבודתי הנזכרת.

מ ע ר כ ת ה א כ ס י ו מ ו ת א . עצמים יסודיים: קבוצה A ויחס דו-מקומי R בין אברי הקבוצה הזאת. אם yRx אנו אומרים ש"y ע ו ק ב את x" או ש "y הוא עוקב של x". כמו-כן אומרים אנו ש x הוא קודם בלתי-אמצעי של y.

1. A היא קבוצה בלתי-ריקה.
2. לכל אבר x של A, $x\varepsilon A$, מתאים אבר y של A, $y\varepsilon A$, אחד ויחיד, באופן שקים yRx.
3. אם I היא קבוצה חלקית של A המקימת את התנאים: א) I היא בלתי-ריקה. ב) אם $x\varepsilon I$ ו yRx אז גם $y\varepsilon I$;–אזי I מכילה בדיוק אבר אחד שאינו מוכל בקבוצה I' של כל האברים y של A המקימים את התנאים $x\varepsilon I$, yRx, $y\varepsilon I$.

נקרא לכל קבוצה חלקית I של A המקימת את התנאי ב) של האכסיומה 3. של מערכת האכסיומות א. קבוצה חלקית א י נ ד ו ק ט י ב י ת של A ונעיר שהקבוצה I' היא קבוצה חלקית של הקבוצה I.

ב. אנחנו מוכיחים עכשיו את האכויבלנציה של מערכת האכסיומות א. עם מערכת האכסיומות של פ א נ ו . נביא את המערכת של פאנו בצורה הבאה (שנתן לה א. ל נ ד א ו (Grundlagen der Analysis, 1930, p. 2) בשנויים קלים):

מ ע ר כ ת ה א כ ס י ו מ ו ת ש ל פ א נ ו . עצמים יסודיים: קבוצה B ויחס דו-מקומי S בין אברי הקבוצה B. (אם ySx אנחנו שוב אומרים ש "y ע ו ק ב את x" או ש "y הוא עוקב של x" או ש "x הוא קודם בלתי-אמצעי של y".)

1. ישנו אבר מסוים "1" בתוך B, $1\varepsilon B$ המקים את התנאי של "משואה" בנעלם ξ, $1S\xi$ אין פתרון בתוך B.
2. מן yRu ו-yRv נובע $u=v$.
3. לכל אבר x של B, $x\varepsilon B$, מתאים אבר y של B, $y\varepsilon B$, אחד ויחיד, באופן שקים ySx.
4. (אכסיומת האינדוקציה השלמה). אם J היא קבוצה חלקית של B המקימת את התנאים: א) $1\varepsilon J$. ב) אם $x\varepsilon J$ ו-ySx אז גם $y\varepsilon J$;–אזי $J=B$.

ג. נוכיח קודם שמהמערכת א. נובעת מערכת האכסיומות של פ א נ ו על ידי כך שנראה שאם נציג במערכת האכסיומות האחרונה A במקום B ו R במקום S, אזי תהפך מערכת זאת לתוצאה ממערכת האכסיומות א. נוכיח תחילה שהאכסיומה 1. של מערכת האכסיומות של פאנו היא תוצאה ממערכת האכסיומות 1. לשם כך נגדיר את האבר 1 של A בתור אותו אבר יחיד של A שאינו מוכל בתוך A'. (פרוש הדבר הזה הוא שאנחנו לוקחים בתור הקבוצה I של האכסיומה 3. של מערכת האכסיומות א. את הקבוצה A כולה לאחר שהיא אינה ריקה (לפי האכסיומה 1. של אותה מערכת) ולאחר שהיא באופן מובן מאליו אינדוקטיבית, כלומר, מקימת גם את התנאי ב) של האכסיומה 3. של מערכת זאת ויוצרים את הקבוצה A' המתאימה לקבוצה זאת.) אנחנו טוענים עכשיו שלתנאי $1R\xi$ אין פתרון בין אברי A. כי לו היה קים פתרון x, $\xi=x$, בתוך A לתנאי $1R\xi$, כי אז היה 1 עוקב של האבר x של A ואז הוא היה צריך להיות מוכל בתוך A' בנגוד להגדרתו. לכן, אם נציג במקום האבר "1" של האכסיומה 1. של מערכת האכסיומות של פאנו את האבר "1" בזה עכשיו הגדרנו אותו (ואת A במקום B ואת R במקום S) תהא אכסיומה זו קימת. על ידי כך הראינו שהאכסיומה 1. של מערכת האכסיומות של פאנו היא תוצאה ממערכת האכסיומות א.

נעיר פה שאם A ו R מקימים את מערכת האכסיומות א. בכלל, האבר היחיד של קבוצה I (המקימת את התנאים א) ו ב) של האכסיומה 3. של מערכת האכסיומות א.) שאינו מוכל ב I' הוא האבר היחיד ה א י נ י צ י א ל י של I, כלומר האבר היחיד של I שאין לו קודם בלתי-אמצעי בתוך I. קודם כל, לו אין קודם בלתי-אמצעי בתוך I, כי לו היה לו קודם בלתי-אמצעי בתוך I כי אז הוא היה העוקב של אבר זה של I ואז היה מוכל בתוך I' בנגוד

להגדרתו. וכל אבר אחר של I מוכל בתוך I' ולכן הוא עוקב של אבר מסוים של I, כלומר יש לו קודם בלתי-אמצעי בתוך I.

ד. נוכיח עכשיו בדרך הכלילה שהאכסיומה 2. של פאנו נובעת ממערכת האכסיומות א. נניח לשם כך שיש לכל הפחות שני קודמים בלתי-אמצעיים שונים u ו-v לאבר y של A: $u \neq v$, $v \in A$, $u \in A$, yRv, yRu. ניצור את הקבוצה החלקית המינימלית Q של A המקימת את שני התנאים: א) $v \in Q$, $u \in Q$. ב) אם $x \in Q$ ו-yRx אז גם $y \in Q$, כלומר Q היא קבוצה חלקית אינדוקטיבית של A. פרוש הדבר הוא שאנחנו יוצרים את קבוצת השיתוף Q של כל אותן הקבוצות החלקיות של A המקימות את שני התנאים הנזכרים זה עתה. נקח בתור הקבוצה I של האכסיומה 3. של מערכת האכסיומות א. את הקבוצה Q ונסתכל באבר היחיד של Q שאינו מוכל בתוך Q'. נוכח בזה שהאבר הזה יכול להיות רק האבר u או האבר v של Q. כי לו היה זה אבר אחר של Q, כי אז לא היתה Q הקבוצה החלקית המינימלית של A המקימת את שני התנאים הנזכרים לעיל. באמת יכולנו להשמיט אבר זה מ-Q מבלי שהקבוצה המתקבלת על ידי כך תפסיד את קיום שני התנאים הנזכרים. זה נובע מתוך העובדה שהאבר הנידון בזה איננו שוה לפי ההנחה לא ל-u ולא ל-v ואיננו עוקב לשום אבר של Q. נוכח עכשיו שאבר זה איננו יכול להיות לא u ולא v ונבוא כך לידי סתירה עם האכסיומה 3. של מערכת האכסיומות א. נניח, למשל, שהוא שוה ל-u, כלומר ש-u הוא האבר היחידי של Q שאין לו קודם בלתי-אמצעי. מכאן נובע שלכל אבר אחר של Q, וביניהם גם ל-v, יש קודם בלתי-אמצעי בתוך Q. נסתכל עכשיו בקבוצה החלקית $I=Q'=Q-\{u\}$ שהיא קבוצה חלקית אינדוקטיבית של A. נוכיח ש-$I=I'$. כי בתור אבר של הקבוצה $Q-\{u\}$ שאין לו קודם בלתי-אמצעי בא בחשבון רק עוקב של u, האבר האניציאלי שהשמטנו אותו מ-Q. כי הרי זהו משפט כללי שאם נתונה קבוצה חלקית של A המקימת את התנאים א) ו-ב) של האכסיומה 3. של המערכת א., אזי בתור האבר היחידי של I' שאינו מוכל בתוך $(I')'$ בא בחשבון רק העוקב של האבר היחידי של I שאינו מוכל בתוך I'. ההוכחה למשפט זה היא זו שכל אבר אחר של I', מלבד העוקב של האבר היחידי של I שאין לו קודם בלתי-אמצעי בתוך I, יש לו קודם בלתי-אמצעי בתוך I ולכן גם בתוך I', הואיל ואת קודמו הבלתי-אמצעי לא השמטנו מ-I כדי לקבל את I'. עכשיו לפי האכסיומה 2. של מערכת האכסיומות א. האבר היחידי של A העוקב את u הוא y, ול-y יש קודם בלתי-אמצעי בתוך Q' והוא v. הוכח אפוא ש-$Q'=(Q')'$, והואיל ו-Q' היא קבוצה בלתי-ריקה הגענו לידי סתירה עם האכסיומה 3. של מערכת האכסיומות א. לכן הוכח שבתור האבר של Q שאינו מוכל בתוך Q' אינו בא בחשבון לא אבר של Q השונה מ-u ו-v ולא האבר u של Q. באותו אופן נוכל להוכיח שגם האבר v של Q אינו בא בחשבון בתור אבר כזה. לכן הגענו שוב לידי סתירה עם האכסיומה 3. של מערכת האכסיומות א. הוכח אפוא שאין בתוך A יותר מקודם בלתי-אמצעי אחד לשום אבר של A, כלומר שהאכסיומה 2. של מערכת האכסיומות של <u>פאנו</u> היא תוצאה ממערכת האכסיומות א.

ה. הואיל והאכסיומה 3. של מערכת האכסיומות של פאנו מזדהית עם האכסיומה 2. של מערכת האכסיומות א. אם נציג את A במקום B ואת R במקום S, נשאר לנו להוכיח רק את אכסיומת האינדוקציה השלמה של פאנו. נניח לשם כך ש-J היא קבוצה חלקית של A המקימת את שני התנאים של אכסיומת האינדוקציה של <u>פאנו</u>. אז היא מקימת גם את שני התנאים של האכסיומה 3. של מערכת האכסיומות א. נניח עכשיו בדרך השלילה ש-$J \neq A$. אזי ישנו אבר z של A שאינו מוכל בתוך J: $z \notin J$, $z \in A$. אנחנו יוצרים את הקבוצה החלקית <u>המינימלית</u> K של A המקימת את שני התנאים: א) $z \in K$. ב) אם $x \in K$ ו-yRx, אז גם $y \in K$, כלומר K היא קבוצה חלקית אינדוקטיבית של A. פרוש הדבר הזה הוא שוב שאנחנו לוקחים את קבוצת השיתוף K של כל אותן הקבוצות החלקיות של A המקימות את שני התנאים הנזכרים זה עתה. אזי אנחנו מוכיחים כמו בסעיף הקודם שבתור האבר היחידי של K שאינו מוכל בתוך K', כלומר בתור האבר האיניציאלי של K, בא בחשבון רק z. בהתאם לאכסיומה 3. של מערכת האכסיומות א. יש בקבוצה K אבר איניציאלי והאבר האיניציאלי הזה הוא לכן z. נסתכל עכשיו בקבוצה החלקית $J+K$ של A. זאת היא קבוצה חלקית של A המקימת את שני התנאים של האכסיומה 3. של מערכת האכסיומות א. לכן היא מקימת גם את האכסיומה הזאת. האבר z של הקבוצה הזאת איננו יכול להיות עוקב של שום אבר של J. כי z איננו מוכל בתוך J. כמו-כן האבר 1 של J איננו עוקב של שום אבר של K הואיל ואין לו בכלל קודמים בתוך A. נמצא אפוא שלשני האברים 1 ו-z אין קודמים בלתי-אמצעיים בתוך $J+K$, כלומר שאלה הם שני אברים איניציאליים של $J+K$, כלומר שב-$J+K$ יש שני אברים שאינם מוכלים בתוך $(J+K)'$. וזה עומד בסתירה לאכסיומה 3. של מערכת האכסיומות א. לכן הוכח כי $J=A$. ובזה הוכח שאכסיומת האינדוקציה השלמה של <u>פאנו</u> היא תוצאה ממערכת האכסיומות א. ובזה השלמנו את החצי הראשון של הוכחת האכביבלנציה של מערכת האכסיומות א. עם מערכת האכסיומות של <u>פאנו</u>, דהיינו את ההוכחה שמערכת האכסיומות האחרונה היא תוצאה ממערכת האכסיומות הראשונה.

ו. נוכיח עכשיו שמערכת האכסיומות א. היא תוצאה ממערכת האכסיומות של פאנו, כלומר שאם נציב במערכת האכסיומות הראשונה B במקום A ו-S במקום R תהפכנה האכסיומות של מערכת זו למסקנות מהאכסיומות של המערכת של <u>פאנו</u>. אם נעשה כך, אז האכסיומה 1. של המערכת א. היא מסקנה מהאכסיומה 1. של המערכת של <u>פאנו</u>, הואיל וב-B כלול האבר "1".

האכסיומה 2. של המערכת א. מזדהית באותה הנחה עם האכסיומה 3. של המערכת של פאנו. נשאר לנו אפוא רק להוכיח שהאכסיומה 3. של המערכת א. היא מסקנה מהאכסיומות של המערכת של פאנו. נסתכל עכשיו בכל אותן הקבוצות החלקיות האינדוקטיביות של B (כלומר אותן הקבוצות החלקיות של B ביחד עם כל אבר x של B שהן מכילות אותו הן מכילות גם כל אבר של B המקים את התנאי: ySx) המכילות את האבר 1 ושלכן 1 הוא אצלן אבר איניציאלי, כלומר אבר שאין לו קודם בלתי-אמצעי בתוך הקבוצה החלקית הנידונה של B, ונראה שהקבוצות החלקיות האלה של B מקימות את האכסיומה 3. של המערכת א., כלומר שהאבר "1" הוא האבר האיניציאלי היחידי אצל כל אחת מהן. כמו-כן אנחנו טוענים שאם כל אותן הקבוצות החלקיות האינדוקטיביות של B המכילות את האבר x של B בתור אבר איניציאלי מקימות את האכסיומה 3. של מערכת א., כלומר, מכילות את האבר x הזה בתור האבר האיניציאלי היחידי שלהן ואם ySx, אז גם כל אותן הקבוצות החלקיות האינדוקטיביות של B המכילות את האבר y של B בתור אבר איניציאלי מקימות את האכסיומה 3. של מערכת האכסיומות א., כלומר, מכילות את y זה בתור האבר האיניציאלי היחידי שלהן. אם נסתכל עכשיו בקבוצה החלקית J של B המכילה את כל האברים האיניציאליים של כל אותן הקבוצות החלקיות האינדוקטיביות של B המקימות את האכסיומה 3. של המערכת א., כלומר, המכילות כל אחת אבר איניציאלי יחיד, נראה שקבוצה חלקית J זו של B מקימת את שני התנאים: א) $1 \in J$. ב) אם $x \in J$ ו-ySx, אז גם $y \in J$, כלומר, את שני התנאים של אכסיומת האינדוקציה של פאנו. לפי אכסיומה זו יהיה קים J=B. ופרוש הדבר הזה הוא שכל אותן הקבוצות החלקיות האינדוקטיביות של B המכילות את האבר הרצוני n של B בתור אבר איניציאלי מקימות את האכסיומה 3. של מערכת האכסיומות א. אבל זהו תוכן האכסיומה הזאת, כי כל קבוצה חלקית אינדוקטיבית בלתי-ריקה של B מוכרחה להכיל לכל הפחות אבר איניציאלי אחד. דבר זה נובע מהמשפט הנובע מהאכסיומה של פאנו שלכל קבוצה חלקית של B יש אבר קטן ביותר (משפט זה מוכח בספר הנזכר של לנדאו, עמ' 13). כי אבר קטן ביותר זה הוא אבר איניציאלי של אותה קבוצה חלקית, הואיל ולו היה לו קודם בלתי-אמצעי בתוך קבוצה חלקית זאת, לא היה הוא האבר הקטן ביותר של הקבוצה החלקית הנידונה. לכן נשאר לנו רק להוכיח את שתי הטענות הנזכרות לעיל, או את קיום שני התנאים א) ו-ב) הנזכרים זה עתה בנוגע לקבוצה החלקית J של B.

בנוגע לתנאי א) יש קודם כל לומר שיש רק קבוצה חלקית אינדוקטיבית אחת של B המכילה את האבר "1" של B בתור אבר איניציאלי, והיא הקבוצה B בעצמה. זה נובע מהאכסיומה של האינדוקציה השלמה, הואיל והקבוצה הזאת ממלאה את שני התנאים של האכסיומה הזאת. ואילו הקבוצה B מקימת את האכסיומה 3. של מערכת האכסיומות א. מכיון ש-1 הוא לפי מסקנה הנובעת בנקל ממערכת האכסיומות של פאנו האבר האיניציאלי היחידי של B (ראה משפט 3. של הספר הנזכר של לנדאו, עמ' 3). לכן הוכחנו שהמספר 1 שיך ל-J. נניח עכשיו שכל הקבוצות החלקיות האינדוקטיביות של B המכילות את האבר x של B בתור אבר איניציאלי מקימות את האכסיומה 3. של מערכת האכסיומות א. ונוכיח שאם ySx אז גם כל הקבוצות החלקיות האינדוקטיביות של B המכילות את האבר y של B בתור אבר איניציאלי מקימות אכסיומה זו. (יש רק קבוצה חלקית אינדוקטיבית של B אחת ויחידה המכילה את האבר x או y של B בתור אבר איניציאלי, כפי שקל להוכח שוב מאכסיומת האינדוקציה השלמה; אבל אין אנחנו צריכים להשתמש פה במשפט זה.) נסתכל בקבוצה חלקית אינדוקטיבית של B המכילה את y בתור אבר איניציאלי ונקרא לה K. צריך להוכיח ש-y הוא האבר האיניציאלי היחידי של K. האבר x של B איננו כלול בתוך K, הואיל ו-y הוא אבר איניציאלי של K. נסתכל בקבוצה החלקית $K+\{x\}$ של B. זוהי קבוצה חלקית אינדוקטיבית של B. כי K היא אינדוקטיבית לפי ההנחה והעוקב של x, הוא y, כלול בתוך K. אנחנו טוענים ש-x הוא אבר איניציאלי של $K+\{x\}$. כי לו היה כלול ב-$K+\{x\}$ אבר קודם בלתי-אמצעי של x, כי אז היה מוכרח להיות כלול ב-K, הואיל ולפי מסקנה הנובעת מהאכסיומות של פאנו כל שני אברים x ו-y של B המקימים את התנאי ySx הם שונים זה מזה: $x \neq y$ (ראה משפט 2 של הספר הנזכר של לנדאו, עמ' 3). ואז היה כלול ב-K, הואיל והיא קבוצה חלקית אינדוקטיבית של B, גם האבר x, מה שלא נכון כפי שהוכחנו זה עתה. עכשיו נובע מהנחתנו ש-x הוא האבר האיניציאלי היחידי של $K+\{x\}$. לכן y הוא האבר האיניציאלי היחידי של K. כי כל אבר אחר z של K, $z \neq y$, הוא בעל קודם בלתי-אמצעי בתוך $K+\{x\}$ ולכן גם בתוך K הואיל וקודמו הבלתי-אמצעי של z הוא אבר השונה מ-x, מפני של-x יש לפי אכסיומה 3. של פאנו רק עוקב אחד ויחידי והוא y. הוכח אפוא שאם כל הקבוצות החלקיות האינדוקטיביות של B המכילות את האבר x של B בתור אבר איניציאלי מכילות אותו בתור איניציאלי יחיד ו-ySx אזי גם כל הקבוצות החלקיות האינדוקטיביות של B המכילות את האבר y בתור אבר איניציאלי מכילות אותו כאבר איניציאלי יחיד. כך הוכח גם קיום התנאי ב) לגבי הקבוצה החלקית J של B. ולכן הוכח, לפי האמור למעלה, שהאכסיומה 3. של מערכת האכסיומות א. היא תוצאה ממערכת האכסיומות של פאנו ועל ידי כך הושלם גם החצי השני של התפקיד שעמד לפנינו, והוא להוכיח

שמערכת האכסיומות א. נובעת ממערכת האכסיומות של פאנו, כלומר הוכח שמערכת האכסיומות א. אכביבלנטית למערכת האכסיומות של פאנו.

ז. לבסוף נבנה עכשיו את סדרת המספרים הטבעיים מתוך מערכת האכסיומות א. את המספר 1 קבלנו כבר לעיל על ידי כך שבנינו, בהתאם לאכסיומה 3. של מערכת זו את האבר האיניציאלי היחידי של הקבוצה היסודית A של מערכת האכסיומות א. באותו אופן נוכל לבנות מספר "2" על ידי כך שנקח את האבר האיניציאלי היחידי של הקבוצה החלקית 'A של A, אבר "3" על ידי כך שנקח את האבר האיניציאלי היחידי של הקבוצה החלקית '(A') של A. אם נמשיך כך בלי גבול נקבל סדרה של "מספרים" ...,1,2,3 שקל להוכח בזה שהיא מזדהית עם סדרת המספרים הטבעיים במובן הרגיל של המלים האלה.

An alternative proof of a theorem of equivalence
concerning axioms of natural numbers

Baruch Germansky

(Summary)

In the proof of the theorem of equivalence in question brought in the Riveon Lematematika 3 (1949), p. 65, the author uses the proposition of connexity of the set of natural numbers relatively to the primitive relation R (of succession) of the set of axioms of Peano. In this paper a direct proof of the theorem in question is given.

RIVEON LEMATEMATIKA

A QUARTERLY JOURNAL

INTENDED TO PROMOTE MATHEMATICAL RESEARCH
AMONG STUDENTS OF MATHEMATICS

DOV JARDEN, EDITOR

Volume 4 — Jerusalem, April 1950 — Number 1

CONTENTS

Editor's address: Dov Jarden, Kneset Hachadasha, Jerusalem, Israel