ЗБІРНИК

МАТЕМАТИЧНО-ПРИРОДОПИСНО-ЛЇКАРСЬКОЇ СЕКЦІЇ

Наукового Товариства імени Шевченка.

ТОМ XV. ВИПУСК II.

ПІД РЕДАКЦІЄЮ

Дра ВОЛОДИМИРА ЛЕВИЦЬКОГО, Дра ІВАНА РАКОВСЬКОГО
і Дра СТЕФАНА РУДНИЦЬКОГО.

SAMMELSCHRIFT

DER MATHEMATISCH-NATURWISSENSCHAFTLICH-ÄRZTLICHEN SEKTION

DER ŠEVČENKO-GESELLSCHAFT DER WISSENSCHAFTEN in LEMBERG.

BAND XV. HEFT II.

REDIGIERT VON

Dr. WLADIMIR LEWYĆKYJ, Dr. IWAN RAKOWŚKYJ
u. Dr. STEPHAN RUDNYĆKYJ.

У ЛЬВОВІ, 1913.

Накладом Наукового Товариства ім. Шевченка.

Здрукарні Наукового Товариства імени Шевченка.

ЗМІСТ.

INHALT.

Студії з теорії конґруенцій.

(Studien aus der Kongruenzentheorie).

НАПИСАВ

Др. Микола Чайковський.

Опираючись на клясичній теорії конґруенцій, даній Gauss'ом в „Disquisitiones arithmeticae“[1]), можемо розвязувати тільки такі конґруенції, які мають самі дійсні корінї. Щоби одначе перевести розвязку конґруенцій вповнї, треба за почином Galois[2]) ввести рід мнимих величин, які тут ґратимуть подібну ролю, що звичайні мнимі числа $a + bi$ ($i^2 = -1$) в теорії рівнань. Отсю думку перевели новійші математики (головно Американцї: Cole, Moore і Dickson[3]), будуючи теорію „поля Galois“; вона відповідає подекуди теорії альґебраічних тїл.

На тій основі переведена тут теорія конґруенцій третього й четвертого степеня з первочисельним модулом. Тим предметом займав ся вже Cauchy[4]), але тільки в тїснім обсягу дійсних розвязок. Щоби одначе могти тут перевести повну теорію згаданих конґруенцій, подаємо в першій части нашої розвідки теорію поля Galois в тім видї, як її опісля будемо примінювати до нашої теми.

I. Теорія поля Galois.

§. 1.

1. З елєментарної теорії чисел звісно, що всї числа природного ряду

$$0,\ 1,\ 2,\ 3,\ \ldots\ m-1,\ m,\ m+1,\ \ldots \qquad (1)$$

[1]) Lipsiae 1801, — Werke Bd. I, Leipzig, 1870.

[2]) Sur la théorie des nombres, 1831.

[3]) Dickson, Linear groups with an exposition of the Galois Field theory. Липск, 1901.

[4]) Cauchy, Exercices de Mathématiques, IV. Année, Paris 1829. — Oeuvres, S. II, T. IX. Paris 1891.

розпадають ся після модула m на m кляс; кожда з них містить в собі безконечно богато чисел, пристайних поміж собою (mod. m), так що замість всіми числами природного ряду, можемо в деяких проблемах математики оперувати клясами непристайних поміж собою чисел

$$K_0,\ K_1,\ K_2,\ \ldots\ K_{m-1} \qquad (2)$$

заєдно їх репрезентантами, т. є системою яких небудь чисел, вибраних довільно по одному з кождої кляси. Коли сю систему становлять числа

$$0,\ 1,\ 2,\ \ldots,\ m-1, \qquad (2a)$$

то називаємо їх числами модула m або системою найменших останків модула m і пишемо се так: [mod. m]. До кляси K_0 належать всї многократи модула.

2. Визначну ролю в теорії чисел грає повна система останків первочисельного модула p:

$$0,\ 1,\ 2,\ \ldots,\ p-1; \qquad (2aa)$$

її назвемо полем Galois степеня p і означимо $GF[p]$.

Взагалї називаємо полем, тїлом або обсягом вимірности систему, яка має ту прикмету, що її елементи, лучені з собою при помочи операцій додаваня і множеня, дають на вислїд опять числа тої системи. Таким полем є система (2aa); вона має ще й ту прикмету, що скількість елементів, які в нїй містять ся, є скінчена; се слїдує рівно-ж з елементарної теорії чисел. Поле Galois степеня p має отже загалом такі прикмети:

1) При помочи операції додаваня одержуємо з кождих двох елементів того поля, a і b, третїй елемент s однозначно; так само при помочи множеня (тут мусимо одначе виключити елемент 0) однозначно елемент m:

$$a + b = s, \qquad a\,b = m.$$

2) Обі операції (додаваня й множеня) є злучні, т. є коли $(a+b)$ є сумою чисел a і b, а $(a\,b)$ їх добутком, то

$$\big((a+b)+c\big) = \big(a+(b+c)\big) \text{ і } \big((a\,b)\,c\big) = \big(a\,(b\,c)\big)$$

3) З

$$a + b = d \qquad \text{і} \qquad a + c = d$$

або

$$a\,b = e \qquad \text{і} \qquad a\,c = e$$

слїдує:

$$b = c.$$

4. Обі операції є переміннi, т. є

$$(a+b) = (b+a) \qquad \text{і} \qquad (a\,b) = (b\,a).$$

5) Врешті додаване в получену з множенем є роздїльне:

$$a\,(b+c) = a\,b + a\,c.$$

Коли за комбінуючу операцію приймемо додаване, то елементи ряду (2aa) творять скінчену ґрупу порядку p; беручи-ж за основу операцію множеня, одержимо з чисел

$$1,\ 2,\ 3,\quad .,\ p-1 \qquad (2aa^*)$$

рівно-ж скінчену ґрупу порядку $p-1$. Систему (2aa*) назвемо зредукованим полем Galois і зазначимо її $GF[p]^*$. До неї належать всї числа, перві супроти модула.

В обох разах є поле Galois перемінною ґрупою.

Елемент 0 грає супроти множеня особливу ролю; іменно, яке-б не було x, є завсїди:

$$0.\ x = 0 \qquad \text{і} \qquad x.\ 0 = 0,$$

і навпаки: коли добуток двох чисел належить до кляси K_0, то принайменше один з чинників мусить належати до сеї кляси.

3. З прикмет ґрупи слїдує, що до кождого елемента a в $GF[p]$ єствує один і тільки один такий елемент b, який доданий до a дасть число з кляси K_0:

$$a + b \equiv 0 \pmod{p};$$

його значимо

$$b \equiv -a \pmod{p}.$$

Проте є в $GF[p]$ можлива до переведеня операція відниманя.

Подібно є в $GF[p]^*$ завсїди можлива операція дїленя; слїдує се з т. зв. теореми Fermat'a. Випишім іменно $GF[p]^*$ і помножім всї його числа одним з поміж них:

$$1.\ a,\ 2.\ a, \qquad (p-1).\ a,$$

то через те зрепродукуємо його, тільки в иншім порядку. Добуток всїх його чисел є пристайний (mod. p) до добутка всїх чисел ряду (2aa*), бо в склад обох добутків входять репрезентанти тих самих кляс $K_1,\ K_2,\quad K_{p-1}$:

$$1.\ a.\ 2.\ a.\ 3.\ a \qquad (p-1).\ a \equiv 1.\ 2.\ 3 \qquad (p-1) \pmod{p}$$

або

$$(p-1)!\ (a^{p-1} \quad 1) \equiv 0 \pmod{p}.$$

Добуток $(p-1)!$ є супроти модула p первий, отже мусить бути

$$a^{p-1} \equiv 1 \pmod{p}. \qquad (3)$$

Отсей вірець є характеристичний для $GF[p]^*$. З нього слїдує, що до кождого числа a в $GF[p]^*$ дасть ся дібрати таке число a', що добуток тих обох чисел буде належати до кляси K_1:

$$a\,a' \equiv 1 \pmod{p}.$$

Бо помножім сю конґруенцію через a^{p-2}, то се дасть:

$$a' \equiv a^{p-2} \pmod{p};$$

a є супроти модула p перве, отже і a^{p-2} належить до $GF[p]^*$.

Число a' називаємо відворотностю числа a' в $GF[p]^*$ або його товаришем (Sozius) і значимо символічно:

$$a' \equiv \frac{1}{a} \pmod{p}.$$

4. Прикмети 1) — 5) і взорець Fermat'a є характеристичні для кождого скінченого поля[1]). Покажемо, що коли система p елементів, де p є перве число, має ті всі прикмети, то вона творить скінчене поле, отже коли скількість елементів поля є первим числом, то його можна вважати полем Galois степеня p.[2])

Нехай будуть

$$A, B, C, \ldots, L \tag{4}$$

даними p елементами. Виберім з поміж них який небудь елемент H і утворім ряди

$$H+A,\ H+B,\ H+C,\ \ldots\ H+L, \tag{4a}$$
$$A+H,\ B+H,\ C+H,\ \ldots\ L+H, \tag{4б}$$

то вони оба є ідентичні — не вважаючи на порядок членів — з рядом (4) — (прикмета 1). Проте в першім з них мусить містити ся один елемент $H+I$, рівний елементови H з (4),

$$H+I=H,$$

а в другім елемент $J+H$, також рівний H:

$$J+H=H.$$

Звідси слїдує:

$$G+(H+I)=(G+H)+I=G+H$$
$$(J+H)+K=J+(H+K)=H+K$$

(прикмета 2), т. зн.: який би не був елемент M, то в ряді (4) єствує завсїди такий елемент I, який доданий до M з правої сторони не змінить його, — і такий елемент J, який доданий до M з лївої сторони рівно-ж не викличе в нїм нїякої зміни:

$$M+I=M,$$
$$J+M=M.$$

Врештї після прикмети 3) маємо: для $M=J$ з першого рівнаня

$$J+I=J$$

і для $M=I$ з другого:

$$J+I=I,$$

отже

$$J=I.$$

---

[1]) Під „скінченим полем“ розуміємо тут систему, вложену із скінченого числа елементів — у відріжненю від „скінчених алгебраічних тїл“, де скінченість лежить у тім, що при помочи основи, вложеної із скінченого числа величин, можемо представити кожду величину того тїла. — Пор. Weber, Algebra, I. §. 150, II. §. 80. (endlicher Kongruenzkörper).

[2]) Пор. пр. Borel-Drach, Théorie des nombres et l'algèbre supérieure (d'après les conferences par M. J. Tannery), Paris 1895, Note II, стр. 343.

Єствує проте в ряді (4) один і тільки один такий елемент I, який доданий з лївої або з правої сторони до котрого небудь иншого елемента, не змінить його. Отсей елемент відповідає клясї K_0 в $GF[p]$.

Возьмім тепер знова довільний елемент A і творім ряд:

$$A,\ (A+A),\ ((A+A)+A),\ .$$

якого числа будемо в скороченю називати:

$$A,\ 2A,\ 3A,\ \ .,\ mA,\ \ .; \qquad (4в)$$

на основі прикмети 1) містить він в собі тільки ті елементи, які є в (4), і є обмежений, отже його елементи будуть повторювати ся. Нехай на $(q+1)$-ім місцї стоїть елемент рівний першому; тодї возьмім під розвагу тільки q перших членів. — Коли-б ряд (4в) не вичерпував ще всїх елементів (4), то возьмім один з нових елементів B і при його помочи творім новий ряд:

$$A+B,\ 2A+B,\ 3A+B,\ \ .,\ qA+B;$$

на його $(q+1)$-ім місцї буде стояти рівно-ж елемент з тої самої кляси, що перший елемент. Всї члени того ряду є відмінні від ряду (4) — (прикмета 3). — Коли ще тепер не зрепродукований цїлий ряд (4), то творимо при помочи нового елемента C третїй такий самий ряд, аж врешті вичерпаємо всї елементи з (4); кождий з частинних рядів буде мати таку саму скількість членів, т. є q, отже

$$p = kq,$$

а що ми приймили p перве, то $k=1$, отже $p=q$, т. зн. ряд (4в) вичерпує всї елементи.

Рядом (4в) маємо здефінїоване і множене, отже тою дорогою можемо перевести всї дальші анальогії; мусимо ще тільки доказати, що коли модул m є зложений, то повна система чисел [mod. m] не творить поля Galois. Бракує тут іменно теореми Fermat'a. Добутки всїх чисел обох рядів

$$1,\ 2,\ \ .,\ m-1,$$
$$1a,\ 2a,\ \ .,\ (m-1)a,$$

є — що правда — пристайні до себе (mod. m), отже:

$$(m-1)!\ (a^{m-1}-1) \equiv 0 \ (\text{mod. } m),$$

зате кінцева замітка з уст. 2. не має тут примінення, бо m і $(m-1)!$ мають $HCП > 1$, отже модул m можна також представити як добуток двох чисел $< m$.

Натомість, коли уставимо в ряд всї елементи

$$a_0,\ a_1,\ a_2,\ \ .,\ a_{\varphi(m)-1},$$

перві супроти модула m (їх є $\varphi(m)$ — теорема Gauss'a), то при помочи якого небудь з них можемо утворити добуток

$$a_0,\ a_1,\qquad a_{\varphi(m)-1}\ [a^{\varphi(m)}-1]\equiv 0 \pmod{m},$$

з якого слїдує

$$a^{\varphi(m)}\equiv 1 \pmod{m}, \tag{5}$$

бо чинник перед [ ] є первий супроти m. Се т. зв. **узагальнена теорема Fermat'a**.

Звідси слїдує, що система p елементів, які сповнюють прикмети 1) — 5), є ідентична з $GF[p]$.

5. З огляду на неважність теореми Fermat'a для зложених модулів, мусимо зазначити, що:

1) Лїнїйна конґруенція

$$a\,x\equiv b \pmod{m} \tag{6}$$

є тільки тоді рішима, коли $HCП$ чисел a і m містить ся і в b.

2) Коли d є $HCП$ чисел a і b, то конґруенцію можемо скоротити через d, лишаючи модул незмінений.

3) Коли d є $HCП$ чисел a, b і m, то обі сторони конґруенції можемо скоротити через d; модул можемо рівно-ж скоротити або лишити без зміни.

4) Коли $(a,\ m)=1$, то конґруенція (6) має тільки одну розвязку. Бо рівнозначне з нею Діофантове рівнанє

$$a\,x-m\,y=b,$$

не дасть ся нїяк скоротити; воно є рішиме, а вартости на x творять аритметичний поступ з ріжницею m, т. є всї є поміж собою пристайні (mod. m).

5) Коли $(a,\ m)=d$, конґруенція має d ріжних розвязок, бо з конґруенції (6) слїдує

$$\frac{a}{d}\,x\equiv\frac{b}{d}\left(\text{mod. }\frac{m}{d}\right), \tag{6a}$$

Тут є $\left(\frac{a}{d},\ \frac{m}{d}\right)=1$, отже конґруенція має одну розвязку — назвім її z —, а всї її прочі розвязки є $\equiv z\ \left(\text{mod. }\frac{m}{d}\right)$. Натомість (6) може мати ще й инші розвязки, бо числа, непристайні до себе $\left(\text{mod. }\frac{m}{d}\right)$ не, мусять бути непристайні (mod. m). Отже, коли $x\equiv z\ \left(\text{mod. }\frac{m}{d}\right)$ є розвязкою конґруенції (6a), то (6) має такі корінї

$$x\equiv z+i\ \frac{m}{d} \pmod{m}$$

$$(i=0,\ 1,\qquad d-1),$$

бо вставивши се в (6) одержимо

$$a\left(z+i\frac{m}{d}\right)=a\,z+i.\frac{a}{d}.m\equiv a\,z\equiv b \pmod{m}.$$

§. 2.

6. До тепер обговорили ми головні прикмети поля Galois степеня p і виказали, що повна система останків модула m творить тільки тоді поле Galois, коли m є первим числом. Тепер займемо ся конструкцією обширнїйших піль Galois і докажемо, що їх степенем може бути тільки **степень первого числа**, p^n.

Альґебраічний многочлен степеня m, якого сочинники є числами з $GF[p]$:

$$F(x) = a_0 x^m + a_1 x^{m-1} + \quad + a_m \pmod{p}, \qquad (1)$$

а a_0 не належить до кляси K_0, називаємо **функцією m-того степеня** в $GF[p]$. За сочинники $a_0, a_1, \ldots, a_m$ можемо приймати всї числа $GF[p]$ з виймком $a_0 \equiv 0 \pmod{p}$, отже скількість всїх функцій m-ого степеня в $GF[p]$ є $p^m(p-1)$. Коли-ж чинник a_0 добудемо перед скобку і всї функції, що ріжнять ся тільки тим постійним чинником, будемо вважати одною й тою самою функцією, то скількість всїх ріжних функцій є p^m, проте:

В $GF[p]$ є p^m **ріжних функцій m-того степеня.**

7. Функцію $F(x)$ називаємо **заведимою** або **незведимою** в $GF[p]$, відповідно до того, чи можливе або ні розложити її на добуток

$$F(x) \equiv g(x)\, h(x) \pmod{p} \qquad (2)$$

двох иншим функцій в $GF[p]$, степенїв низших як степень функції $F(x)$, а висших як 0. — Чинники $g(x)$ і $h(x)$ є заведимі або ні; коли вони оба заведимі, то функція $f(x)$ m-того степеня дасть ся остаточно розложити на m лінїйних чинників:

$$f(x) \equiv (x - \alpha_1)(x - \alpha_2) \quad (x - \alpha_m) \pmod{p} \qquad (3)$$

Коли положимо $x \equiv$ одному з α, тоді буде

$$f(\alpha_i) \equiv 0, \pmod{p},$$

отже $\alpha_1, \alpha_2, \ldots, \alpha_m$ **є коріннями конґруенції**

$$f(x) \equiv 0 \pmod{p}. \qquad (4)$$

В елєментарній теорії конґруенцій доказують ся такі твердження:

I. (основна теорема): **Конґруенція m-того степеня з первим модулом не може мати більше як m ріжних або однакових чинників**[1]).

II. Ліва сторона конґруенції є (mod. m) дїлима кождим „коріневим чинником“ $x - \alpha_i$.

III. **Сочинники конґруенції є основними симетричними функціями її корінїв.**

IV. **Многократні корінї конґруенції є заразом коріннями її похідних.**

---

[1]) Може їх мати менше як m.

V. Коли функцію $f(x)$ розложити на добуток двох инших (3), і коли (4) мав m корінів, то обі конґруенції:

$$g(x) \equiv 0 \text{ і } h(x) \equiv 0 \pmod{p}$$

мають як раз по тільки корінів, кілько виносить їх степень.

VI. Конґруенція

$$x^{p-1} \equiv 1 \pmod{p} \tag{5}$$

мав за коріні всї числа $GF[p]$.

З V. і VI. слїдує спосіб визначування фактичної скількости корінів даної конґруенції (4): методою Евклїда вишукуємо $HCП$ функцій $f(x)$ і $x^{p-1} - 1 \pmod{p}$; він містить в собі всї коріні даної конґруенції, отже його степень подав скількість її корінів. — Отся метода походить від Libri[1].

Із сказаного слїдує, що як при рівнанях, так і тут **зведимість і рішимість конґруенцій** (mod. p) **є ідентичні понятя.**

Про рішимість (зведимість) конґруенцій можемо рішати на основі таких тверджень:

I. Щоби конґруенція (4) була рішима, є конечне і достаточне, щоби циклїчний визначник Δ степеня $p-1$, утворений із сочинників функцій $f(x)$, був $\equiv 0 \pmod{p}$.

II. Конґруенція (4) мав точно r ріжних корінів, коли ряд визначника Δ є r.[2]).

III. Виріжник незведимої в $GF[p]$ функції є $\equiv (-1)^{n-1} \pmod{p}$; коли $f(x)$ розпадаєть ся на r незведимих (mod. p) чинників, є її виріжник $\equiv (-1)^{n-r} \pmod{p}$.[3]).

8. Займаючи ся **квадратними функціями** в $GF[p]$, приходимо до понять **квадратних останків і не-останків.**

Скількість всїх квадратних функцій в $GF[p]$ є p^2, бо в

$$f(x) = x^2 + ax + b \tag{6}$$

можуть a і b приймати всї вартости з $GF[p]$.

Повну квадратну конґруенцію

$$x^2 + ax + b \equiv 0 \pmod{p} \tag{6a}$$

---

[1]) Mémoires de Mathématiques, I. p. 164.

[2]) Коли даний визначник Δ степеня k і всї його підвизначники степенів 1, 2, 3, . . . l мають вартість 0 зґл. $\equiv 0 \pmod{p}$, а бодай один з підвизначників ряду $l+1$ є $\equiv 0$ зґл. $\neq 0$, тоді кажемо, що Δ має ряд (Rang) $k-l$ (Kronecker, Frobenius).

[3]) Теореми I—II: Rados, Zur Theorie der Kongruenzen höheren Grades, Crelle's Journ. 89. (1886), p. 258—260; Kronecker, ibid. p. 320; Gegenbauer, Wiener Ber. 95. 2 (1887), p. 165—169, 610—617. — Теорема III. Stickelberger, Verhandlungen des I. intern. math. Kongresses in Zürich, 1897, p. 186; Voronoï, Verh. des III. int. math. Kongr. in Heidelberg, 1904, p. 186.

розвязуємо подібно як квадратне рівнанє. Сочинник a можемо заступити яким небудь паристим числом, що належить до тої самої кляси: $a \equiv 2a'$ (mod. p), отже напишемо:

$$(x + a')^2 \equiv a'^2 - b \text{ (mod. } p), \tag{6б}$$

проте повну конґруенцію зводимо на двочленну

$$y^2 \equiv s \text{ (mod. } p). \tag{7}$$

Вона може бути рішима або ні; в першім разї називаємо s **квадратним останком**, в другім **квадратним не-останком** модула p; коли-б було $s \equiv 0$, то конґруенція мала би один подвійний корінь $y \equiv 0$. Виключивши се, бачимо, що теорема Fermat'a наводить нас на такі крітерії рішимости конґруенції (7): коли

$$s^{\frac{p-1}{2}} \equiv 1 \text{ (mod. } p), \tag{8а}$$

то конґруенція є рішима; вона є нерішима, коли

$$s^{\frac{p-1}{2}} \equiv -1 \text{ (mod. } p). \tag{8б}$$

Кожде число $GF[p]^*$ мусить сповнювати (для $p > 2$) **одну і тільки одну з тих двох формулок**; їх називаємо **крітеріями Euler'a**. Їх заступив **Legendre** символом $\left(\frac{s}{p}\right)$, именно є:

$$\left(\frac{s}{p}\right) \equiv s^{\frac{p-1}{2}} \text{ (mod. } p), \tag{9}$$

отже: 1) коли s є кв. останком, маємо

$$\left(\frac{s}{p}\right) = +1;$$

2) в разї не-останка:

$$\left(\frac{s}{p}\right) = -1.$$

3) Коли-ж для повности допустимо і $s \equiv 0$, то

$$\left(\frac{s}{p}\right) = 0.$$

Вартість символа $\left(\frac{s}{p}\right)$ називаємо **квадратним характером** числа s супроти модула p, отже: $\left.\begin{matrix}\text{останки}\\ \text{не-останки}\end{matrix}\right\}$ мають кв. характер ± 1, числа кляси K_0 характер 0.

Скількість останків і не-останків кождого модула є однакова і виносить по $\frac{p-1}{2}$. Добуток двох останків або двох й не-останків є останком, добуток останка й не-останка не-останком, бо

$$\left(\frac{s}{p}\right) \cdot \left(\frac{t}{p}\right) = \left(\frac{st}{p}\right). \tag{9а}$$

В дальшім будемо потрібувати крітерій для кв. характеру чисел ± 1, ± 2, ± 3; вони є:

$+1$ є завсїди останком; -1 останком для первочисельних модулїв $p \equiv 1 \pmod 4$, не-останком для $p \equiv -1 \pmod 4$, т. зн.

$$\left(\frac{+1}{p}\right) = +1, \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \tag{9б}$$

Для ± 2:

$p =$	$8n+1$	$8n+3$	$8n+5$	$8n+7$
$\left(\frac{2}{p}\right) =$	$+1$	-1	-1	$+1$
$\left(\frac{-2}{p}\right) =$	$+1$	$+1$	-1	-1

Для ± 3:

$p =$	$12n+1$	$12n+5$	$12n+7$	$12n+11$
$\left(\frac{3}{p}\right) =$	$+1$	-1	-1	$+1$
$\left(\frac{-3}{p}\right) =$	$+1$	-1	$+1$	-1

9. Анальоґічно до квадратних останків і не-останків дефінїюємо останки й не-останки всїх инших степенів. Именно, коли двочленна конґруенція

$$y^n \equiv s \pmod p \tag{10}$$

є рішима, s є n-тим (степенним) останком; коли вона нерішима, s є n-тим (степенним) не-останком. (Приймаємо, що s не є многократю модула).

Коли s належить до кляси K_1, маємо т. зв. одиничну конґруенцію (Einheitskongruenz):

$$x^n \equiv 1 \pmod p; \quad (n \geq 3) \tag{11}$$

вона є анальоґічна до рівнань подїлу кола. Її розвязки будемо називати n-тими коріннями одиниці (mod. p).

Коли r є найменшим виложником, для якого є $z^r \equiv 1 \pmod p$, тоді кажемо, що z належить (mod. p) до виложника r. Коли $r = p-1$, z є первісним n-тим коренем одиниці (mod. p); коли $r < n$, корінь називаємо непервісним. В такім разї є $n = k \cdot r$.

Нехай буде $n = p-1$; тоді — на основі теореми Fermat'a — є всї числа $GF[p]$ n-тими коріннями одиниці, та не всї вони належать до виложника $p-1$; пр. квадратні останки належать до виложника $\frac{p-1}{2}$. Коли ніяка низша степень числа g, аж щойно $(p-1)$-ша, є $\equiv 1 \pmod p$, тоді називаємо g первісним коренем конґруенції (12) або первісним коренем числа p.

Всї корінї, спільні обом конґруенціям

$$x^{\alpha} \equiv 1 \text{ і } x^{\beta} \equiv 1 \pmod{p} \tag{11a}$$

є корінями конґруенції

$$x^{\delta} \equiv 1 \pmod{p}, \tag{11б}$$

де $\delta = (\alpha, \beta)$.[1]) Отже, коли α і β є перві супроти себе, то обі конґруенції (11а) не мають спільних корінїв крім $x \equiv 1$.

Виложники, до яких належать (mod. p) числа $GF[p]^*$, є подїльниками числа $p-1$.

До кождого подїльника d числа $p-1$ належить (mod. p) $\varphi(d)$ чисел з $GF[p]^*$. До виложника $p-1$ належить (mod. p) $\varphi(p-1)$ чисел, т. зн. кожде число p має $\varphi(p-1)$ первісних корінїв.

Коли g є одним із первісних корінїв числа p, то ряд

$$1, g, g_2, \quad ., g^{p-2} \tag{12}$$

є ідентичний — не вважаючи на порядок чисел — з $GF[p]^*$, отже всї ті числа є поміж собою рїжні. Отже до кождого числа з $GF[p]^*$ належить одна із $p-1$ перших степенїв числа g, т. зн. один із виложників від 0 до $p-2$. Коли знайдемо, що

$$s \equiv g^{\sigma} \pmod{p}, \tag{13}$$

то σ називаємо показчиком числа p (при основі g):

$$\sigma \equiv \operatorname{ind}_g s$$

зґл.
$$\sigma \equiv \operatorname{ind}_g s \pmod{p-1}, \tag{14}$$

бо виложники повторюють ся що $p-2$.

Теорія показчиків є анальоґічна з теорією льоґаритмів; вона дуже придатна до розвязки двочленних конґруенцій.

Конґруенція (10) є рішима, коли

$$s^{\frac{p-1}{d}} \equiv 1 \pmod{p}, \tag{15}$$

де $d = (p-1, n)$; вона має тоді d корінїв. Назвім $y_0 \equiv g^{\eta_0}$ один з її корінїв, то прочі корінї будуть

$$y_0, \alpha y_0, \alpha^2 y_0, \quad ., \alpha^{d-1} y^0,$$

де $\alpha \equiv g^{\frac{p-1}{d}}$ Формулка (15) є анальоґічна до крітерії Euler'a; вона висказує, що a є n-тим останком числа p. Символ, анальоґічний до Legendre'ового, є;

$$\left(\frac{s}{p}\right)_n = 1. \tag{16}$$

10. Примінення. 1) $n=2$; тоді є $p-1$ паристе, отже $d = (p-1, 2) = 1$. Крітерія Euler'a звучить, як знаємо: $s^{\frac{p-1}{2}} \equiv +1 \pmod{p}$;

[1]) Знаком (m, n) завначуємо *НСП* чисел m і n.

маємо по $\frac{p-1}{2}$ останків і не-останків. Первісні другі корінь з одиниці (mod. p) є: $+1$ і -1.

2) В разї $n=3$ маємо дві можливости: а) $p\equiv 1$ (mod. 6), б) $p\equiv -1$ (mod. 6); числа всїх инших форм не є перві.

а) Коли $p\equiv 1$ (mod. 6), то $d=3$, отже одинична конґруенція $z^3\equiv 1$ (mod. p) має три розвязки: 1, α, α^2, де $\alpha\equiv g^{\frac{p-1}{3}}$ Двочленна конґруенція (10) є рішима, коли $s^{\frac{p-1}{3}}\equiv 1$ (mod. p), нерішима, коли $s^{\frac{p-1}{3}}\equiv\alpha$ або α^2, отже коли один її корінь є r, то два другі є αr і $\alpha^2 r$. Єствує проте $\frac{p-1}{2}$ кубових останків, а $2.\frac{p-1}{3}$ не-останків; всї кляси чисел $GF[p]$ ділять ся на три громади так, що кожде число i тої громади є $\equiv\alpha^i$ (mod. p) ($i=0, 1, 2$). Кубовий характер числа s значимо так:

$$\left[\frac{s}{p}\right]\equiv s^{\frac{p-1}{3}}\ (\text{mod. } p). \qquad (17)$$

б) $p\equiv -1$ (mod. 6); тодї є $p-1=6m-2$, отже $d=(6m-2, 3)=1$, проте крітерія звучить $s^{p-1}\equiv 1$ (mod. p). В такім разї всї числа $GF[p]^*$ є кубовими останками, отже двочленна конґруенція (10) є завсїди рішима, зате одинична конґруенція має тільки одну розвязку, $x\equiv 1$.

3) $n=4$. Тут мусимо розріжнити рівно-ж дві можливости: а) $p\equiv -1$ (mod. 4), б) $p\equiv +1$ (mod. 4).

а) Коли p має форму $4m-1$, то $p-1=4m-2$, отже $d=2$; одинична конґруенція $x^4\equiv 1$ (mod. p) може мати очивидно тільки дві розвязки: $+1$ і -1. Крітерія для двоквадратного характеру числа s є проте ідентична з Euler'овою для квадратних останків; отже кождий квадратний $\left\{\begin{matrix}\text{останок}\\ \text{не-останок}\end{matrix}\right\}$ є в тім разї і двократним $\left\{\begin{matrix}\text{останком}\\ \text{не-останком}\end{matrix}\right\}$ того самого числа — і навпаки.

б) В разї $p\equiv 1$ (mod. 4) є $p-1=4m$, отже $d=4$. Одинична конґруенція має чотири розвязки; 1, α, α^2, α^3, де $\alpha\equiv g^{\frac{p-1}{4}}$ З огляду на те, що $\alpha^2\equiv g^{\frac{p-1}{2}}$, а g є первісним коренем, отже належить до виложника $p-1$, є $\alpha^2\equiv -1$, а дальше $\alpha^3\equiv -\alpha$, проте корінї згаданої конґруенції можна написати також так: 1, α, -1, $-\alpha$.

Крітерієм рішимости для $y^4\equiv s$ (mod. p) є тут $s^{\frac{p-1}{4}}\equiv 1$ (mod. p), а корінї тої конґруенції мають вартости r, $r\alpha$, $-r$, $-r\alpha$, де

$r^4 \equiv s \pmod{p}$. Величина $s^{\frac{p-1}{4}}$ може приймати (mod. p) такі чотири вартости: ± 1, $\pm \alpha$; супроти того всї числа $GF[p]^*$ розпадають ся на чотири кляси, відповідно до того, до котрого з первісних четвертих корінїв одиниці (mod. p) є пристайна його $\frac{p-1}{4}$-та степень.

Теорію двоквадратних останків перевів Gauss[1]), розширивши обсяг дїйсних чисел на числа форми $a + b\,i$, де i є коренем рівнаня $x^2 + 1 = 0$, а a і b належать до $GF[p]$; він дав тим чином початок теорії альґебраічних чисел. Подібно ужив Eisenstein[2]) коріня рівнаня $x^3 = 1$, т. є величини $\varrho = \frac{-1 + i\sqrt{3}}{3}$, до збудованя теорії кубових останків.

§. 3.

11. Займемо ся тепер дальше теорією поля Galois. Ми сказали, що скількість всїх функцій m-того степеня в $GF[p]$

$$f(x) = a_0 x^m + a_1 x^{m-1} + \quad + a_m \qquad (1)$$

є $p^m(p-1)$ заґл. p^m — відповідно тому, чи функції, що ріжнять ся постійним чинником, будемо вважати ріжним поміж собою, чи однаковими.

Нехай $F_n(x)$ буде якою небудь незведимою функцією в $GF[p]$ степеня n; тоді конґруенція

$$F_n(x) \equiv 0 \pmod{p} \qquad (2)$$

не має корінїв в $GF[p]$. Длятого дефінїюємо, подібно як в альґебрі або теорії альґебраічних чисел, її корінї як нові величини, необняті полем Galois степеня p. Отсї величини називають ся мнимими величинами Galois, бо він перший впровадив їх до теорії конґруенцій.[3]) — З огляду на те, що конґруенція n-того степеня не може мати більше як n корінїв (уст. 7), дефінїює нам кожда незведима конґруенція (2) точно n ріжних, мнимих чисел Galois. Проте можемо висказати таку теорему (I), анальоґічну до основної теореми альґебри:

[1]) Theoria residuorum biquadraticorum, Commentatio I. et II., Gottingae 1829/32. — Werke Bd. II. — Пор. рівно-ж Bachmann, Die Lehre von der Kreisteilung, Leipzig 1872, Vorlesung 13—16.

[2]) Crelle's Journ., Bd. 27, 28. Bachmann, op. cit.

[3]) Galois, Sur la théorie des nombres, Bulletin des sciences mathém. de Férussac, 1830. — Oeuvres, p. 17., éd. Liouville 1946. — Abhandlungen über die algebraische Auflösung von Gleichungen, von Abel und Galois, herausg. v. Maser, Berlin 1889, p. 100—107.

Кождa конґруенція n-того степеня з первочисельним модулом має рівно n корінів.

12. Утворім функцію (1) з незвісною x. Коли $m \geq n$, то при помочи конґруенції (2) можна зредукувати всї степенї незвісної, висші від $n-1$, так що зістане нам тільки

$$f(x) = a_0 x^{n-1} + a_1 x^{n-2} + \quad a_{n-1}, \tag{1a}$$

де сочинникови a_0 не накладаємо нїякого обмеженя.

Теорема II. Скількість функцій (1a) є p^n.

Доказ. Що скількість функцій $f(x)$ (степенїв 0, 1, 2, . ., $n-1$), не може бути більша як p^n, слїдує звідси, що кождий з n сочинників може приймати тільки p вартостий. Але вона не може бути менша від p^n, бо коли-б було $f(x) \equiv g(x) \pmod{p}$, то звідси слїдувало би

$$(a_0 - b_0) x^{n-1} + (a_1 - b_1) x^{n-2} + \ldots + (a_{n-1} - b_{n-1}) \equiv 0 \pmod{p},$$

де b_i є сочинниками функції $g(x)$. Тому x було би коренем конґруенції степеня низшого нїж n, т. зн. функція $F_n(x)$ мала би з функцією низшого степеня спільний чинник, отже не могла би бути незведима. Отже дві функції $f(x)$ є тільки тодї рівні згл. пристайні, коли їх дотичні сочинники належать (mod. p) до однакових кляс, а такі функції ми вважаємо ідентичними.

13. **Теорема III. Кождa функція $f(x)$ сповнює конґруенцію**

$$X^{p^n} \equiv X \pmod{p}. \tag{3}$$

Доказ. Напишім всї функції $f(x)$ з виїмком тої, якої всї сочинники належать до кляси K_0; їх буде $p^n - 1$:

$$f_1(x), f_2(x), \quad ., f_{p^n-1}(x). \tag{4}$$

Помножім ті всї величини якою небудь з поміж них, X:

$$Xf_1(x), Xf_2(x), \quad Xf_{p^n-1}(x). \tag{4a}$$

Оба ряди, (4) і (4a), складають ся з тих самих величин, тільки в иншім порядку, то-ж і добутки всїх величин кождого ряду є до себе (mod. p) пристайні:

$$f_1 f_2 \quad \cdot f_{p^n-1} \equiv f_1 f_2 \quad f_{p^n-1} X^{p^n-1} \pmod{p}$$

Обі сторони можна скоротити добутком $f_1 f_2 \quad \cdot f_{p^n-1}$, бо нї один його чинник не є пристайний до 0 (mod. p); длятого маємо

$$X^{p^n-1} \equiv 1 \pmod{p} \tag{3a}$$

або

$$X^{p^n} \equiv X \pmod{p}.$$

Отсей взорець є новим узагальненєм теореми Fermat'a.

Заключене. 1) Конґруенція (3a) має $p^n - 1$ коріннів, обнятих рядом (4). Проте можемо функцію X^{p^n-1} розложити на добуток

$$X^{p^n} - 1 \equiv \big(X - f_1(x)\big)\big(X - f_2(x)\big) \ldots \big(X - f_{p^n-1}(x)\big) \pmod{p}.$$

2) Порівнуючи обі сторони тої ідентичної конґруенції і означуючи через $\sigma_1, \sigma_2, \ldots \sigma_{p^n-1}$ основні симетричні функції величин $f_k(x)$, бачимо, що

$$\sigma_1 \equiv \sigma_2 \equiv \ldots \equiv \sigma_{p^n-2} \equiv 0, \ \sigma_{p^n-1} \equiv -1 \pmod{p}.$$

отже

$$\prod_{k=1}^{p^n-1} f_k(x) + 1 \equiv 0 \pmod{p}. \tag{5}$$

Отсе є узагальнене теорема Wilson'a.[1])

3) З окрема зазначимо, що $\sigma_1 \equiv 0 \pmod{p}$, т. зн.

$$\sum_{k=1}^{p^n-1} f_k(x) \equiv 0 \pmod{p}. \tag{6}$$

14. Теорема IV. Загал функцій (1a) або (4) творить поле Galois.

Доказ. Величини (4) репродукують ся через чотири основні операції. Що сума, ріжниця й добуток двох $f(x)$ мають опять ту саму форму, се очивидне; треба тільки ще до ряду (4) дібрати величину 0. Але і квот двох $f(x)$ належить рівно-ж до ряду (4). — Нехай буде дана реляція

$$f(x) \equiv g(x)\,h(x) \pmod{p};$$

тоді при даних $f(x)$ і $g(x)$ можна найти все одну і тільки одну таку функцію $h(x)$, яка сповнюватиме ту реляцію [виключивши $g(x) \equiv$ ідентично 0 (mod. p)]. Помножім обі її сторони через $\big[g(x)\big]^{p^n-1}$, то з огляду на (3a) буде

$$h(x) \equiv f(x)\big[g(x)\big]^{p^n-2} \pmod{p};$$

отсе оправдує уживати на означене квота символічного взірця

$$h(x) \equiv \frac{f(x)}{g(x)} \pmod{p}.$$

Проте можемо сказати так:

Загал многочленів в $GF[p]$ степеня $(n-1)$-ого[2]) творить поле Galois степеня p^n, коли за змінчиву x прий-

[1]) Теорема Wilson'a звучить: $(p-1)! + 1 \equiv 0 \pmod{p}$; вона є характеристична для первих чисел.

[2]) т. зн. всіх степенів, почавши від 0, до $(n-1)$-ого вкл.

мемо один з инших корінїв якоїсь незведимої конґруенції степеня n.

Поле Galois степеня p^n означуємо за Dickson'ом $GF[p^n]$[1]), а коли виключуємо з нього елемент 0, то зазначимо се, подібно, як попередно, $GF[p^n]^*$ і називаємо зредукованим полем Galois.

15. **Теорема V.** Коли в $f(x)$ заступимо x через x^p, то $f(x)$ перемінить ся в свою p-ту степень.

Доказ. Піднесїм $f(x)$ (1a) до степеня p; се дасть:

$$[f(x)]^p = a_0{}^p (x^p)^{n-1} + a_1{}^p (x^p)^{n-2} + \quad + a_{n-1}^p + g(x),$$

де $g(x)$ є сумою всїх прочих членів, отже членів з многочленними сочинниками (Binomialkoeffizienten), а вони всї є многократями числа p. Примінюючи теорему Fermat'a, $a^p \equiv a \pmod p$, маємо

$$[f(x)]^p \equiv a_0 (x^p)^{n-1} + a_1 (x^p)^{n-2} + \quad + a_{n-1} \pmod p,$$

отже

$$[f(x)]^p \equiv f(x^p) \pmod p. \qquad (7)$$

Тому, коли x заступити чéрез x^p, то $f(x)$ перейде в $[f(x)]^p$, т. є кожде X в X^p.

Замітка. Повторюючи сю операцію n разів, одержимо:

$$\left.\begin{aligned} f(x^p) &\equiv [f(x)]^p, \\ f(x^{p^2}) &\equiv [f(x)]^{p^2}, \\ &\cdots\cdots \\ f\left(x^{p^{n-1}}\right) &\equiv [f(x)]^{p^{n-1}}, \\ f\left(x^{p^n}\right) &\equiv [f(x)]^{p^n} \equiv f(x). \end{aligned}\right\} \pmod p,$$

17. Виконаймо отсю субституцію в даній конґруенції

$$F_n(x) \equiv 0 \pmod p; \qquad (2)$$

се дасть:

$$F_n(x^p) \equiv [F_n(x)]^p \equiv 0 \pmod p$$

отже коли x є коренем конґруенції (2), то x^p є її другим коренем. Так само є $F_n\left(x^{p^2}\right) \equiv 0$, $F_n\left(x^{p^3}\right) \equiv 0, \ldots, F_n\left(x^{p^{n-1}}\right) \equiv 0 \pmod p$, отже

Теорема VI. Коріні незведимої конґруенції (2) є

$$x,\ x^p,\ x^{p^2},\ \ldots\ x^{p^{n-1}},$$

де x означує який небудь з її корінїв.

[1]) Література про поле Galois: Schoenemann, Grundzüge einer allg. Theorie d. höh. Kongr. Crelle's Journal, Bd. 31 (1846) стр. 269—325. Dedekind, Abriss einer Theorie d. höh. Kongr. Crelle, Bd. 54 (1857) стр. 1—26. Dickson, Linear groups etc. стр. 1—71. Scarpis, Exposizione elementare della teoria del campo di Galois, Battaglini Annali, t. XLIV. (1907), p. 153—180.

Отсї величини, се власне мнимі числа, які ввів Galois.

Примір. Конґруенція

$$F_3(x) = x^3 - 3x + 1 = 0 \pmod 7$$

є в $GF[7]$ незвідима. Коли x є її коренем, то два другі корінї є x^7 і x^{49}; їх можна зредукувати до многочленів найвисше другого степеня при помочи даної конґруенції. Именно є $x^3 \equiv 3x - 1$, отже $x^7 = (x^3)^2 . x$, а що $(x^3)^2 \equiv 2x^2 + x + 1$, то $x^7 \equiv 2x^3 + x^2 + x \equiv 2(3x - 1) + x^2 + x \equiv x^2 - 2$; дальше є: $x^{49} = (x^7)^7 \equiv (x^2 - 2)^7 = (x^2 - 2)[(x^2 - 2)^3]^2$, а що $(x^2 - 2)^3 \equiv x^6 + x^4 - 2x^2 - 1$, то з огляду на $x^6 + x^4 \equiv -2x^2 + 1$, маємо $(x^2 - 2)^3 \equiv 3x^2$. Квадрат тої остатньої величини є $9x^4 \equiv -x^2 - 2x$, а помножений через $x^2 - 2$ дає $-x^4 - 2x^3 + 2x^2 - 3x \equiv x^2 - x + 2$, отже коли x є одним коренем даної конґруенції, то оба другі корінї є $x^7 \equiv x^2 - 2$, $x^{49} \equiv -x^2 - x + 2$. Легко провірити, що $x(x^2 - 2)(x^2 - x + 2) \equiv -1 \pmod 7$.

17. Напишім ряд степенів одної з величин в $GF[p^n]$:

$$1, X, X^2, X^3, \ldots;$$

отсей ряд не є безконечний, тільки повторюють ся в періодах що найвисше $(p^n - 1)$-членних, бо $X^{p^n - 1} \equiv 1 \pmod p$. Але можливе є й таке, що якась низша степень величини X, пр. s-та, буде пристайна до 1. Коли s є найменшим таким виложником, для якого є

$$X^s \equiv 1 \pmod p, \tag{8}$$

тоді кажемо, що X *належить* $\pmod p$ *до виложника* s.

Теорема VII. *Виложник* s, *до якого належить яка небудь з величин з* $GF[p^n]$, *є подільником числа* $p^n - 1$.

Доказ. Нехай s не буде подільником числа $p^n - 1$; тоді можемо написати так:

$$p^n - 1 = st + r, \quad 0 < r < s.$$

Підносячи (6) до степені t, маємо

$$X^{st} \equiv 1 \pmod p,$$

а що задля (3a)

$$X^{st + r} \equiv 1 \pmod p,$$

то мусїло би бути також $X^r \equiv 1 \pmod p$. Се неможливе, коли $0 < r < s$, бо s є найменшим виложником, для якого сповнюють ся вимога (8). Проте мусить бути $r = 0$, отже

$$s = \frac{p^n - 1}{t}.$$

18. Величину X, яка належить до виложника $p^n - 1$, називаємо *первісною величиною* в $GF[p^n]$, подібно як число g, яке $\pmod p$ належить до виложника $p - 1$, назвали ми первісним коренем модула p або первісною величиною в $GF[p]$ (уст. 9).

Теорема VIII. Цїле $GF[p^n]^*$ можна представити рядом степенів котроїсь небудь первісної величини X того поля.

Доказ. Коли X є первісною величиною в $GF[p^n]$, то ряд

$$1,\ X,\ X^2,\ \ldots,\ X^{p^n-2} \tag{9}$$

складаєть ся з $p^n - 1$ поміж собою ріжних величин того поля, бо реляція

$$X^k \equiv X^l \pmod{p}$$

можлива тільки тодї, коли $k \equiv l \pmod{p^n - 1}$; коли-ж k і l є $\leqq p^n - 2$, то се можливе тільки так, що $k = l$, отже два члени з ряду (9) з ріжними виложниками не можуть бути до себе пристайні (mod. p). — Супроти того, що кождe X^k є якоюсь величиною з $GF[p^n]$,

$$X^k \equiv f_k(x) \pmod{p},$$

є ряд (9) ідентичний з $GF[p^n]^*$.

§. 4.

19. Незведиму функцію n-того степеня в $GF[p]$, $F_n(x)$, при помочи якої ми конструювали $GF[p^n]$, називаємо **модуловою функцією** (Modularfunktion).

Нехай буде $\Phi(x)$ якоюнебудь функцією в $GF[p]$. Коли її степень r є менший від n, тодї $\Phi(x)$ належить вже прямо до $GF[p^n]$; коли-ж $r \geqq n$, тодї можемо написати її у видї

$$\Phi(x) = f(x) + \varphi(x) F_n(x) + p\,\psi(x), \tag{1}$$

де $f(x)$ є одною з величин в $GF[p^n]$, $\varphi(x)$ функцією степеня $r - n$, а $\psi(x)$ якоюнебудь функцією в $GF[p]$. В такім разї називаємо — розширюючи поняте пристайности — $\Phi(x)$ **пристайним** до $f(x)$ **з огляду на подвійний модул** p, $F_n(x)$ і пишемо

$$\Phi(x) \equiv f(x) \ [\text{modd. } p,\ F_n(x)]^1). \tag{1a}$$

Супроти того можемо всї цїлі функції з цїлочисельними сочинниками поділити на p^n кляс; кождy з тих кляс будемо характеризувати тою функцією $f(x)$ з $GF[p]$, до котроїсь вона пристайна [modd. p, $F_n(x)$]. Тих репрезентантів будемо називати, подібно, як в теорії цїлих чисел, **повною системою найменших останків подвійного модула** p, $F_n(x)$.

Нехай X означує якунебудь цїлу функцію з цїлочисельними сочинниками, отже

$$X = f(x) + \varphi(x) F_n(x) + p\,\psi(x);$$

підносїм се рівнанє чергою до степеней p, p^2, $\ldots$, p^n. Через се одержимо:

---

[1]) Означенє походить від Serret'a, Algèbre, t. II, стр. 165 (5 вид.).

$$X^p = \left[f(x)\right]^p + \left[\varphi(x)\right]\left[F_n(x)\right]^p + p\,\psi_1(x),$$
$$X^{p^2} = \left[f(x)\right]^{p^2} + \left[\varphi(x)\right]^{p^2}\left[F_2(x)\right]^{p^2} + p\,\psi_1(x),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$X^{p^n} = \left[f(x)\right]^{p^n} + \left[\varphi(x)\right]^{p^n}\left[F_n(x)\right]^{p^n} + p\,\psi_n(x),$$

де функції $\psi_1(x)$, $\psi_2(x)$., близше нас не обходять. Ті рівнання є рівнозначні з системою конґруенцій

$$\left.\begin{aligned} X^p &\equiv f(x^p), \\ X^{p^2} &\equiv f\left(x^{p^2}\right), \\ &\cdots\cdots \\ X^{p^n} &\equiv f\left(x^{p^n}\right), \end{aligned}\right\} \text{[modd. } p,\ F_n(x)\text{]},$$

а що $f\left(x^{p^n}\right) \equiv f(x) \pmod{p} \equiv X$ [modd. p, $F_n(x)$], то

$$X^{p^n} \equiv X \text{ [modd. } p,\ F_n(x)\text{]}. \qquad (2)$$

Теорема I. Кожда ціла функція з ціловисельними сочинниками сповнює реляцію (2), або иншими словами:

Функція $X^{p^n} - X$ є (mod. p) подільна через модулову функцію $F_n(x)$.

20. Взорець (2) можемо написати ще так:

$$X^{p^n} - X \equiv \varphi(x)\,F_n(x) \pmod{p},$$

а що вія є важний для кождої величини X в $GF[p^n]$, то можемо підставити також $X = x$, отже будемо мати

$$x^{p^n} - x \equiv \varphi(x)\,F_n(x) \pmod{p}, \qquad (3)$$

тому:

Теорема Ia. Функція $x^{p^n} - x$ є (mod. p) подільна через модулову функцію $F_n(x)$.

Теорема II. Функція $x^{p^m} - x$ є тільки тоді (mod. p) подільна через модулову функцію $F_n(x)$, коли m є многократю виложника n.

Доказ. Коли $m = kn$, то $x^{p^m} - x$ є подільне через $x^{p^m} - x$, отже теорема доказана. Коли-ж m не є многократю n, $m = kn + r$, $0 < r < n$, то з ділення $\left(x^{p^m}\right)$ $\left(x^{p^n}\right)$ випадає останок $x^{p^r} - x$. Отсей многочлен не є подільний через $F_n(x)$, бо $x^{p^n} - x$ і $x^{p^r} - x$ не мають крім x і $x - 1$ нїякого спільного чинника, проте неможлива реляція форми $x^{p^r} - x \equiv \chi(x)\,F_n(x) \pmod{p}$ для $0 < r < n$.

21. Отсї теореми дають нам змогу обчислити скількість незведимих (mod. p) в $GF[p]$ функцій n того степеня. Розложім іменно праву сторону конґруенції (3) на незведимі чинники:

$$x^{p^n} - x \equiv x\, F_n(x)\, G(x)\, H(x) \qquad K(x) \pmod{p}.$$

Поміж ними нема двох однакових, бо ліва сторона не має спільного чинника зі своєю похідною.

В ряді

$$x,\ F_n(x),\ G(x),\ H(x),\ \ldots,\ K(x)$$

містять ся всї незведимі функції n-того степеня, бо ми можемо кожду з них приймити за модулову функцію, а що модулова функція містить ся все в $x^{p^n} - x$, то в згаданім ряду мусять виступати всї такі функції, які можуть грати ролю модулових. — Крім них можуть містити ся в тім ряді незведимі функції тілько таких степенів, які є подїльні через n; слїдує се з теореми II

Проте, коли з $x^{p^n} - x$ видїлити добутки всїх незведимих функцій степенїв менших від n, то одержимо добуток всїх незведимих функцій n-того степеня.

Нехай n буде первим числом; тодї з $x^{p^n} - x$ треба усунути добуток всїх лїнійних чинників, проте добуток всїх незведимих (mod. p) функцій первого степеня n є

$$V = \frac{x^{p^n} - x}{x^p - x},$$

а його степень є $p^n - p$. Проте скількість незведимих (mod. p) функцій степеня n є

$$\lambda_n = \frac{1}{n}(p^n - p).$$

Коли n є зложеним числом,

$$n = a^\alpha b^\beta \qquad e^\varepsilon,$$

то з $x^{p^n} - x$ мусимо усунути добутки всїх незведимих чинників, яких степенї є подїльниками числа n. Вводячи скорочене

$$x^{p^\lambda} - x = [\lambda],$$

переконаємо ся легко, що бажаний добуток є

$$V = \frac{[n]\,\prod\left[\frac{n}{d_1\, d_2}\right]\prod\left[\frac{n}{d_1\, d_2\, d_3\, d_4}\right]\cdots}{\prod\left[\frac{n}{d}\right]\prod\left[\frac{n}{d_1\, d_3\, d_3}\right]},$$

де d, d_1, d_2, d_3, перебігають всї чинники числа n. Степень тої функції є

$$p^n - \sum p^{\frac{n}{d}} + \sum p^{\frac{n}{d_1 d_2}} - \sum p^{\frac{n}{d_1 d_2 d_3}} +$$

отже скількість всїх незведимих функцій n-того степеня є

$$\lambda_n = \frac{1}{n}\Big[p^n - \sum p^{\frac{n}{d}} + \sum p^{\frac{n}{d_1 d_2}} - \sum p^{\frac{n}{d_1 d_2 d_3}} + \quad \Big]. \quad (4)$$

22. Результати з уст. 16. можна узагальнити при помочи пристайности з подвійним модулом.

1) Кожда функція в $GF[p]$ належить [modd. p, $F_n(x)$] до якогось виложника, що є подільником числа $p^n - 1$; т. зн, коли s є найменшим виложником, для якого

$$X^s \equiv 1 \ [\text{modd. } p,\ F_n(x)], \quad (5)$$

то $p^n - 1$ є подільне через s.

2) Коли $s = p^n - 1$, то X називаєть ся первісною величиною в $GF[p^n]$ при подвійнім модулї p, $F_n(x)$. — При помочи степенїв первісної величини X можемо представити цїле $GF[p^n]$.

3) З (5) слїдує безпосередно, що $F_n(x)$ містить ся (mod. p) в $X^s - 1$, отже і в $x^s - 1$.

Дальше докажемо таку

Теорему III. До виложника s належить [modd. p, $F_n(x)$] $\varphi(s)$ ріжних величин з $GF[p^n]$.

Доказ. Коли X належить [modd. p, $F_n(x)$] до виложника s, то в ряді

$$1,\ X,\ X^2,\ \ldots\ X^{s-1}$$

є всї величини поміж собою ріжні, а s-та степень кождої з них є $\equiv 1$, бо для кождого $k < s$ є

$$(X^k)^s = (X^s)^k \equiv 1 \ [\text{modd. } p,\ F_n(x)].$$

Треба ще тільки найти виложник, до якого належить довільне X^k.

1) Нехай буде $(k, s) = 1$; тодї в ряді $k,\ 2k,\ \ldots,\ (s-1)k$ нема ні одної многократи числа s, отже ніяке X^{tk} не може бути $\equiv 1$, коли $t < k$, тому X^k належить до виложника s.

2) Коли $(k, s) = d < 1$, то $\left(X^k\right)^{\frac{s}{d}} = \left(X^{\frac{k}{d}}\right)^s \equiv 1$ [modd. $p, F_n(x)$] а що $\frac{k}{d}$ і s є супроти себе перві, то X^k належить до виложника $\frac{s}{d}$.

Назвім $\psi(d)$ скількість величин X, що належить до виложника d; з огляду на те, що кожде X належить до якогось чинника числа $p^n - 1$ як виложника, маємо

$$\sum_{d/p^n-1} \psi(d) = p^n - 1.$$

З другої сторони є $\Sigma\varphi(d) = p^n - 1$, отже

$$\sum_{d/p^n-1} \psi(d) = \sum_{d/p^n-1} \varphi(d),$$

т. зн. кожде $\psi(d) =$ або 0 або $\varphi(d)$. Перше є виключене, бо тоді було би $\Sigma\psi(d) = 0$, друге дає

$$\psi(d) = \varphi(d),$$

отже наша теорема доказана.

Заключене. В $GF[p^n]$ є $\varphi(p^n - 1)$ первісних величин [modd. p, $F_n(x)$], т. є таких, що належать до виложника $p^n - 1$.

23. Теорема IV. Коли X_1 і X_2 належать до виложників s_1 згл. s_2, то $X_1 X_2$ належить до виложника, який є найменшою спільною многократю чисел s_1 і s_2.

Доказ. Після заложеня є

$$X_1^{s_1} \equiv 1,\ X_2^{s_2} \equiv 1 \text{ [modd. } p\ F_n(x)].$$

Нехай буде v виложником, до якого належить $X_1 X_2$ т. зн. найменшим виложником, для якого є

$$(X_1 X_2)^v \equiv 1 \text{ [modd. } p,\ F_n(x)];$$

$НСП$ чисел s_1 і s_2 назвім d. Піднесім ту конґруенцію до степени $\frac{s_1}{d}$; се дасть

$$X_1^{\frac{v s_1}{d}} X_2^{\frac{v s_2}{d}} \equiv 1 \text{ [modd. } p,\ F_n(x)]$$

Тому, що $\left(\frac{s_1}{d}, s_2\right) = 1$, та конґруенція не може бути сповнена инакше, як тільки так, що і $X_1^{\frac{v s_1}{d}} \equiv 1$, і $X_2^{\frac{v s_1}{d}} \equiv 1$. Перша реляція вказує, що v мусить бути подїльне через d, друга, що $\frac{vs_1}{d}$ є многократю числа s_2. Так само побачимо, що $\frac{vs_2}{d}$ є многократю числа s_1, отже v многократю чисел s_1 і s_2; а що v має бути найменшим числом того рода, то наша теорема доказана.

Заключеня. 1) Коли величини X_1, X_2, X_k належать до виложників s_1, s_2, ., s_k, то виложник, до якого належить добуток $X_1 X_2 \quad X_k$, є найменшою спільною многократю тамтих виложників.

2) Коли $p^n - 1 = a^\alpha b^\beta$ (a, b, перві числа), а X_a, X_b, належать до виложників a^α, b^β, то добуток $X_a X_b$ є первісною величиною в $GF[p^n]$.

24. Функцію $X = f(x)$ в $GF[p]$ називаємо коренем конґруенції

$$\Phi(y) \equiv 0 \text{ [modd. } p,\ F_n(x)], \qquad (6)$$

коли X підставлене в нїй за y, зводить її до виду

$$\Phi(X) = \varphi(x)\ F_n(x) + p\,\psi(x).$$

Теорема V. Конґруенція (6) не може мати більше корінїв, як виносить її степень. Коли степень конґруенції m є рівний n або є подільником того числа, то конґруенція має точно m корінїв.

Доказ. Що конґруенція m-того степеня не може мати більше ріжних корінїв як m, слїдує з елементарної теореми I. в §. 2.

Нехай дальше буде m подільником числа n; тодї всї функції в $GF[p^n]$ є корінями конґруенції

$$X^{p^n} - X \equiv 0 \text{ [modd. } p, F_n(x)]. \tag{2}$$

З другої сторони є $X^{p^n} - X$ подїльне (mod. p) через кожду величину з $GF[p^n]$, отже і через $\Phi(x)$,

$$X^{p^n} - X \equiv \Phi(X)\,\Psi(X) \text{ (mod. } p),$$

отже

$$\Phi(X)\,\Psi(X) \equiv 0 \text{ [modd. } p, F_n(x)]$$

має тї самі корінї що (2). Через те розпадають ся всї величини з $GF[p^n]$ на корінї одної з двох конґруенцій

$$\left.\begin{aligned}\Phi(X) &\equiv 0,\\ \Psi(X) &\equiv 0\end{aligned}\right\} \text{[modd. } p \quad F_n(x)].$$

Перша з них є степеня m, друга степеня $p^n - m$; коли-б перша мала менше як m корінїв, то друга мусїла-б їх мати більше, ніж виносить її степень.

25. **Теорема VI.** Коли $\Phi(x)$ є функцією m-того степеня в $GF[p]$, то все можна найти таку незведиму (mod. p) функцію $F(x)$ в $GF[p]$, що конґруенція

$$\Phi(X) \equiv 0 \text{ [modd. } p, F(x)]$$

буде мати точно m корінїв.

Доказ. Розложім $\Phi(X)$ на незведимі (mod. p) чинники з $GF[p]$ степенїв $m_1, m_2, \ldots, m_\mu$:

$$\Phi(X) \equiv \Phi_1(X)\,\Phi_2(X) \ldots \Phi_\mu(X) \text{ (mod. } p);$$

кождий з них буде містити ся (mod. p) в одній з функцій

$$X^{p^{m_1}} - X,\ X^{p^{m_2}} - X, \ldots X^{p^{m_\mu}} - X,$$

а коли n є *нсм*[1]) чисел $m_1, m_2 \ldots m_\mu$, то всї ті функції містять ся знова в $X^{p^n} - X$.

Коли-ж тепер взяти якунебудь незведиму функцію в $GF[p]$ степеня n, то кожда з конґруенцій $\Phi_k(x) \equiv 0$ буде мати при тім самім подвійнім модулї p, $F(x)$ на основі теореми IV. m_k корінїв. Проте добуток тих функцій $\Phi_k(x)$ сповнює вимоги нашої теореми.

[1]) т. є. найменша спільна многократь.

26. **Теорема VII.** Коли X є корінем конґруенції (6), то прочі її корінь є X^p, X^{p^2} ., $X^{p^{n-1}}$.

Доказ. Подібно як в уст. 52 знаходимо, що

$$\left[\Phi(X)\right]^{p^k} \equiv \Phi\left(X^{p^k}\right) \equiv 0 \ [\text{modd. } p,\ F_n(x)]$$

для $k = 0,\ 1,$ $n-1$, та що дві ріжні степені з повищого ряду є поміж собою ріжні. Отже теорема доказана.

Заключене. Конґруенція $F_n(x) \equiv 0 \pmod{p}$ т. зн. $F_n(x) \equiv 0$ [modd. p, $F_n(x)$] має такі корінь: x, x^p, x^{p^2}, $x^{p^{n-1}}$

27. **Теорема VIII.** Поле Galois не залежить від модулової функції.

Доказ. В уст. 21 мали ми такий розклад:

$$x^{p^n} - x \equiv F_n(x)\, G_n(x) \ldots K_n(x)\, L(x) \ldots P(x) \pmod{p};$$

тут означують $F_n(x)$, $G_n(x)$ $K_n(x)$ незведимі функції степеня n, $L(x)$, ., $P(x)$ функції прочих допустимих степенів. Коли x є елементом з $GF[p^n]$, то

$$x^{p^n} - x \equiv 0 \pmod{p},$$

отже

$$F_n(x)\ G_n(x) \ldots K_n(x)\, S(x) \equiv 0 \pmod{p},$$

де в $S(x)$ звединені всї функції инших степенїв, — т. зн., що x може бути коренем одної, і тільки одної, з поміж незведимих конґруенцій

$$\left.\begin{aligned} F_n(x) &\equiv 0, \\ G_n(x) &\equiv 0, \\ &\ldots \\ K_n(x) &\equiv 0 \end{aligned}\right\} \pmod{p}.$$

Проте можемо за модулову функцію взяти котрунебудь з них, а поле Galois через те не зміниться.

Примір. В $GF[7]$ є незведимими функціями нпр. $x^3 - 2$ і $x^3 - 3$. Коли приймемо за модулову функцію першу з них, творимо $GF[7^3]$ як загал функцій

$$f(i) = a_0 i^2 + a_1 i + a_2 \pmod{7},$$

де i дане конґруенцією $i^3 \equiv 2 \pmod{7}$. Коли хочемо представити те саме поле Galois при помочи функції $x^3 - 3$, назвім j корінь конґруенції $j^3 \equiv 3 \pmod{7}$, тоді $GF[7^3]$ є дане функцією

$$g(j) = b_0 j^2 + b_1 j + b_2 \pmod{7},$$

Величини i і j можна виразити одну через другу. Именно одержуємо через помноженє обох дефінїційних конґруенцій

$$i^3 j^3 \equiv -1 \pmod{7},$$

отже $ij \equiv 3$ або 3α або $3\alpha^2$, де α дане реляцією $\alpha^2 + \alpha + 1 \equiv 0 \pmod{7}$, т. зн. $\alpha \equiv 2$. Проте є пр. $ij \equiv 3$. Помножім ту конґру-

енцію через j^2, то одержимо $i^3 j \equiv 3$, т. зн. $j \equiv -2i^2 \pmod 7$, а дальше $j^2 \equiv i$, т. зн.

$$g(j) \equiv -2b_1 i^2 + b_0 i + b_2 \pmod 7.$$

Напр. величина $g(j) = j^2 - 2j - 3$ відповідає величині $f(i) = 4i^2 + i - 3$, бо з $j \equiv -2i^2$ слїдує $j^2 \equiv 4i^4 \equiv 4i^3 . i \equiv i$.

28. **Теорема IX.** Степенем поля Galois може бути тільки степень первого числа.

Доказ. Ми бачили в уст. 4, що поле Galois найнизшого степеня складаєть ся з p елєментів, коли p є первим числом. Нехай x_1 буде одною з величин поля Galois степеня вищого ніж p; тоді формулка $c_1 x_1$, де c_1 належить до $GF[p]$, т. є ряд величин $0x_1$, $1x_1$, $2x_1$, $\ldots$ $(p-1)x_1$, не вичерпують ще цїлого поля. Проте мусить єствувати ще якась инша величина x_2, не обнята тамтим рядом. Утворім всї можливі суми

$$c_1 x_1 + c_2 x_2.$$

де c_1 і c_2 перебігають цїле $GF[p]$; скількість тих сум виносить p^2, бо тільки одна з них є 0, а однакових поміж ними нема. — Ті суми або вичерпують поле Galois, або ні. В першім разї маємо $GF[p^2]$, в другім разї єствує ще нова величина x_3, при помочи якої творимо дальші суми

$$c_1 x_1 + c_2 x_2 + c_3 x_3$$

і т. д. Таким чином бачимо, що степень поля Galois може бути тільки степению первого числа; отже можна дібрати таких n елементів $x_1, x_2, \ldots x_n$, що всї можливі комбінациї чисел з $GF[p]$ в сочинниках суми

$$X = c_1 x_1 + c_2 x_3 + \ldots + c_n x_n \pmod p \qquad (7)$$

вичерпують цїле $GF[p^n]$. — Таких n елєментів називаємо основою поля Galois.

Теорема X. Перших $n-1$ степенів кождої первісної величини з $GF[p^n]$, $1, x, x^2, \ldots, x^{n-1}$ творить основу поля Galois (пор. теорему VIII, уст. 18).

Теорема XI. Поміж величинами (7) є тільки одна ідентично пристайна (mod. p) до зера, або иншими словами: елєменти основи поля Galois є лїнійно незалежні.

Доказ. Кождий з елєментів основи $GF[p^n]$ є (mod. p) пристайний до одної з первісних величин x того поля (уст. 18), отже суму X можемо звести до виду

$$X \equiv c'_1 + c'_2 x + c'_3 x^2 + \ldots + c'_n x^{n-1} \pmod p.$$

Реляція $X \equiv 0$ можлива тільки так, що всї $c'_k \equiv 0 \pmod p$; коли-б так не було, то первісна величина $GF[p^n]$ сповнювала би конґру-

енцію степеня низшого як n, а се неможливе, бо x є корінем незведимої конґруенції степеня n. — Отже поміж елементами основи поля Galois не може вступати ніяка инша лінійна звязь, як тільки та, що всї сочинники є $\equiv 0 \pmod{p}$, т. зн. ті елементи є лінійно незалежні[1]).

§. 5.

29. Щоби знайти первісні корінї конґруенції

$$X^{p^n} - X \equiv 0 \ [\text{modd. } p,\ F_n(x)], \qquad (1)$$

маємо після уст. 23 (заключене 2) вишукати первісні корінї конґруенцій

$$\left.\begin{aligned} X^{a^\alpha} &\equiv 1, \\ X^{b^\beta} &\equiv 1, \end{aligned}\right\} \ [\text{modd } p,\ F_n(x)],$$

де $a^\alpha\ b^\beta \quad = p^n - 1$, і утворити їх добуток.

Коли модулова функція $F_n(x)$ належать (mod. p) до виложника $p^n - 1$, то всї її корінї є первісними величинами в $GF[p^n]$.

30. Коли знайдемо одну з незведимих (mod. p) функцій степеня n в $GF[p]$, $F_n(x)$, шукаємо при її помочи первісного коріня конґруенції (1). Тоді можемо розложити лїву сторону тої конґруенції на незведимі чинники.

Нехай X буде первісним корінем конґруенції (1); його k-та степень буде сповнювати якусь незведиму в $GF[p]$ конґруенцію

$$\Phi(x) \equiv 0 \ [\text{modd. } p,\ F_n(x)] \qquad (2)$$

степеня $m = n$ або $\frac{n}{d}$; корінї тої конґруенції будуть

$$X^k,\ X^{kp},\ X^{kp^2}, \qquad X^{kp^{m-1}},$$

отже будемо мати

$$\Phi(u) \equiv (u - X^k)(u - X^{kp}) \left(u \quad X^{kp^2}\right) \quad . \left(u \quad X^{kp^{m-1}}\right) \ [\text{modd. } p,\ F_n(x)],$$

Тому, що $X^{kp^m} \equiv X^k$, отже $X^{k(p^m-1)} \equiv 1 \ [\text{modd. } p,\ F_n(x)]$, мусить бути виложник $k(p^m - 1)$ многократю числа $p^n - 1$, отже m мусить бути таким найменшим числом, для якого $p^m - 1$ є подїльне через n; се висказуєть ся так, що X відповідає (passt) виложникови m.[2])

Коли X^k належить до виложника s, то ks є подїльне через $p^n - 1$, отже s є многократю числа n, а що отся конґруенція спов-

[1]) Пор. анальоґічну теорему в' теорії альгебраічних чисел. Гл. пр. Weber, Algebra, Bd. II (2 Aufl.), §. 161.

[2]) Encyklopädie der math. Wiss. Bd. I. 1, p. 575.

нюється для $n = s$, то X^k належить до виложника n. Але і $\Phi(X)$ належить до того самого виложника, як се легко провірити; проте коли хочемо найти всї незведимі конґруенції степеня n і всїх иншихъ допустимих степенїв, беремо за k якунебудь многократь числа m, перву супроти n.

31. Galois пояснює свою теорію на такім примірі: знайти незведиму конґруенцію, від якої залежать первісні корінї двочленної конґруенції

$$X^{7^3} \equiv X \pmod 7. \qquad (*)$$

Тут є $p = 7$, $n = 3$. Одною з незведимих (mod. 7) функцій третього степеня є $x^3 - 2$, отже творимо $GF[7^3]$ з функцій

$$f(x) = a_0 x^2 + a_1 x + a_2 \ [\text{modd. } 7,\ x^3 - 2].$$

Нашою задачею є, знайти таку величину $X = f(x)$, якої всї степени, від зерової до $(7^3 - 1)$-ої включно, мають вичерпати всї корінї конґруенції

$$X^{7^3-1} - 1 \equiv X^{2.3^2.19} - 1 \equiv 0 \pmod 7.$$

Після уст. 81. маємо помножити через себе первісні корінї таких трех конґруенцій

$$\left.\begin{aligned} X^2 &\equiv 1 \\ X^{3^2} &\equiv 1 \\ X^{19} &\equiv 1 \end{aligned}\right\} \pmod 7. \qquad (**)$$

Перша з них має первісний корінь -1, лїву сторону другої можна розложити на добуток $(X^3 - 1)(X^3 - 2)(X^3 + 3)$ (mod. 7), отже її первісні корінї містять ся в конґруенціях

$$X^3 - 2 \equiv 0 \text{ і } X^3 + 3 \equiv 0 \pmod 7.$$

Назвім корінь першої з них x, то x є первісним коренем середньої конґруенції в системи (**).

Врешті шукаємо первісного коріня третьої конґруенції. Galois робить се так, що пробує, чи функція $f(x) = ax + b$ її не сповнить, т. зн., як треба дібрати a і b, щоби було сповнене

$$(ax + b)^{19} \equiv 1 \pmod 7.$$

З двочленного розвинення слїдують такі вартости: $a \equiv 1$, $b \equiv -1$, отже $f(x) \equiv x - 1$ є тим первісним коренем. Помножім через себе ті три знайдені первісні корінї, то одержимо первісний корінь конґруенції (*):

$$X \equiv -1 \,.\, x \,.\, (x - 1) = -x^2 + x \pmod 7. \qquad (***)$$

Елїмінуючи x з (***) і $x^3 - 2 \equiv 0$ (mod. 7), одержимо конґруенцію, від якої залежить X:

$$X^3 - X + 2 \equiv 0 \pmod 7.$$

II. Конґруенції третього і четвертого степеня.

§. 6.

Конґруенції третього степеня.

32. Нехай буде дана конґруенція третього степеня в $GF[p]$

$$f(x) = a_0 x^3 + a_1 x^2 + a_2 x + a_3 \equiv 0 \pmod{p} \qquad (1)$$

Метода, яку примінює Cauchy, полягав на зведеню повної конґруенції до двочленної; є вона зовсім аналоґічна до методи Lagrange'a при рівнанях третього степеня. Cauchy розвязує в тій ціли одну двочленну конґруенцію третього степеня і дві квадратні.

33. Двочленні конґруенції. Спеціяльна (одинична) конґруенція

$$z^3 \equiv 1 \pmod{p} \qquad (2)$$

має завсїди один дїйсний корінь 1 і ще два инші, γ і γ^2, звязані реляцією

$$\gamma^2 + \gamma + 1 \equiv 0 \pmod{p};$$

ми назвали їх первісними третими корінями одиниці (mod. p). Розвязуючи ту квадратну конґруенцію, або примінюючи результати уст. 10, бачимо, що коли $p \equiv 1 \pmod{6}$, то γ і γ^2 є дійсні, а саме

$$\gamma \equiv g^{\frac{p-1}{3}} \pmod{p};$$

означимо їх через α і α^2. В разї $p \equiv -1 \pmod{6}$ належать вони до $GF[p^2]$; коли первісну величину того поля означимо через ε, одержимо

$$\gamma \equiv \varepsilon^{\frac{p-1}{2}} (1 - \varepsilon), \quad \gamma^2 \equiv \varepsilon^{\frac{p-1}{2}} (1 + \varepsilon), \quad \varepsilon^2 \equiv -3 \pmod{p}.$$

34. Загальна двочленна конґруенція

$$x^3 \equiv A \pmod{p} \qquad (3)$$

зводить ся до попередньої. Нехай r буде одним з її коріньв, тоді два инші корінї є, як знаємо, $r\gamma$ і $r\gamma^2$.

Крітерією рішимости для (3) в $GF[p]$ є

$$A^{\frac{p-1}{d}} \equiv 1 \pmod{p},$$

де $d = (p-1, 3)$, отже коли $p \equiv 1 \pmod{6}$, то $d = 3$, проте крітерія звучить

$$A^{\frac{p-1}{3}} \equiv 1 \pmod{p}. \qquad (4)$$

Коли вона сповнена, то конґруенція має три дійсні корінї:

$$r, \ \alpha r, \ \alpha^2 r.$$

В противнім разї назвім j одну з первісних величин в $GF[p^3]$; тоді три корінї є

$$j,\ \alpha j,\ \alpha^2 j.$$

Коли $p \equiv -1 \pmod 6$, то A є все третім степенним останком, отже конґруенція (3) має все один дійсний корінь r. Зате два инші корінї належать до $GF[p^2]$, отже (3) має такі три корінї

$$r,\ \frac{p-1}{2}(1 \quad \varepsilon)\ r,\ \frac{p-1}{2}(1+\varepsilon)\ r.$$

35. Повну конґруенцію третього степеня (1) множимо числом a_0', стовариш̌еним (mod. p) з числом a_0, і при помочи лїнїйного підставленя усуваємо член з квадратом незвісної; через те одержимо зредуковану конґруенцію

$$y^3 - 3Ay - 2B \equiv 0 \pmod p. \tag{4}$$

Назвім її корінї y_1, y_2, y_3 і утворім при їх помочи такі дві ресольвенти:

$$27\,v_1 = (3\,t_1)^3 \equiv (y_1 + \gamma y_2 + \gamma^2 y_3)^3,$$
$$27\,v_2 = (3\,t_2)^3 \equiv (y_1 + \gamma^2 y_2 + \gamma y_3)^3,$$

де $\gamma^2 + \gamma + 1 \equiv 0 \pmod p$. З огляду на те, що

$$27\,(v_1 + v_2) = 2\,\sigma_1{}^3 - 9\,\sigma_1\,\sigma_2 + 27\,\sigma_3,$$
$$27^2\,v_1\,v_2 = (\sigma_1{}^2 - 3\,\sigma_2)^3,$$

а у нас є $\sigma_1 = 0$, $\sigma_2 = -3A$, $\sigma_3 = 2B$ (основні симетричні функції корінів), маємо

$$v_1 + v_2 = 2B,\ v_1\,v_2 = A^3,$$

отже квадратна конґруенція для v_1 і v_2 є

$$v^2 - 2Bv + A^3 \equiv 0 \pmod p. \tag{5}$$

Вирiжник тої конґруенції, а заразом і конґруенції (3), є

$$D \equiv B^2 - A^3 \pmod p. \tag{6}$$

Нехай буде $D \equiv \beta^2$ (β може бути дійсне або належати до $GF[p^2]$), отже маємо

$$v \equiv B \pm \beta,$$

проте зістає ще до розвязки конґруенція

$$t^3 \equiv v. \tag{7}$$

Коли се стало ся і $t \equiv t_1$ є її розвязкою для $v \equiv v_1$, то для $v \equiv v_2$ одержимо $t \equiv t_2$, обмежуючи ся в виборі корінів конґруенції (7), подібно як при формулї Cardan'a, реляцією

$$t_1\,t_2 \equiv A \pmod p$$

(бо $v_1\,v_2 \equiv A^3$). Маємо тому:

$$y_1 + y_2 + y_3 \equiv 0,$$
$$y_1 + \gamma y_2 + \gamma^2 y_3 \equiv 3\,t_1,$$
$$y_1 + \gamma^2 y_2 + \gamma y_3 \equiv 3\,t_2,$$

а звідси:

$$\left.\begin{aligned} y_1 &\equiv t_1 + t_2, \\ y_2 &\equiv \gamma^2 t_1 + \gamma t_2, \\ y_3 &\equiv \gamma t_1 + \gamma^2 t_2, \end{aligned}\right\} \pmod p.$$

Бачимо отже, що розвязка даної конґруенції (4) зводить ся до трьох инших:

1) квадратної для v: $v^2 - 2Bv + A^3 \equiv 0$,

2) квадратної для γ: $\gamma^2 + \gamma + 1 \equiv 0$,

3) двочленної третього степеня $t^3 \equiv B + \beta \equiv C$, всї (mod. p).

36. **Дискусія розвязки.** 1) Конґруенція для v є зведима або ні, відповідно до того, чи

$$\left(\frac{D}{p}\right) = +1 \text{ чи } -1.$$

2) Конґруенція для γ є при $p = 6n+1$ зведима, при $p = 6n-1$ незведима.

3) Конґруенція $t^3 \equiv C$ є при $p = 6n+1$ зведима або ні, відповідно тому, чи

$$\left[\frac{C}{p}\right] = 1 \text{ чи } \neq 1;$$

при $p = 6n-1$ є вона все зведима.

Займемо ся перше дискусією виріжника D

I. $D \equiv 0 \pmod{p}$; тоді є $v_1 \equiv v_2 \equiv B$, отже $t_1 = t_2 = t$; t є дїйсне, бо тодї $t^2 \equiv A$, а що $A^3 \equiv B^2$, то $\left(\frac{A}{p}\right) = \left(\frac{A^3}{p}\right) = \left(\frac{B^2}{p}\right) = +1$. Тодї є $y_1 = 2t$, $y_2 = y_3 = (\gamma + \gamma^2)\, t \equiv -t$. Отже коли чисельна вартість виріжника є многократю модула, то конґруенція має одну двократну розвязку. — Щоби розвязка була трикратна, мусить ще бути $2t \equiv -t$, т. зн. $t \equiv 0 \pmod{p}$, отже і $A \equiv B \equiv 0 \pmod{p}$. Тодї трикратна розвязка є $y \equiv 0$, отже коли від y перейдемо до x через лінїйну субституцію, то трикратна розвязка буде $x \equiv c$, т. зн. дана конґруенція звучить: $(x-c)^3 \equiv 0 \pmod{p}$.

II. $\left(\frac{D}{p}\right) = +1$; в такім разї заложім $r^2 \equiv D$, отже буде r дїйсне, $v \equiv B \pm r \equiv C$ дїйсне. Тепер розвязуємо

$$t^3 \equiv C \pmod{p}. \tag{7a}$$

1) Коли $p \equiv 1 \pmod 6$, тодї є такі можливости:

$$\text{a) } \left[\frac{C}{p}\right] = 1, \quad \text{б) } \left[\frac{C}{p}\right] \neq 1.$$

а) Коли C є кубовим остатком, то t є дїйсне $= \tau$, а що і γ є дїйсне $= \alpha$, то маємо

$$\left.\begin{aligned} y_1 &\equiv \tau_1 + \tau_2, \\ y_2 &\equiv \alpha^2 \tau_1 + \alpha \tau_2, \\ y^3 &\equiv \alpha \tau_1 + \alpha^2 \tau_2, \\ \alpha^2 &+ \alpha + 1 \equiv 0 \end{aligned}\right\} \pmod{p}.$$

Всї три розвязки є дїйсні, ріжні поміж собою.

б) Коли C є не-останком, то t належить до $GF[p^3]$, отже $t = j$, і

$$\left.\begin{array}{l} y_1 \equiv j_1 + j_2, \\ y_2 \equiv \alpha^2 j_1 + \alpha j_2, \\ y_3 \equiv \alpha j_1 + \alpha^2 j_2, \\ j^3 \equiv C,\ j_1 j_2 \equiv A. \end{array}\right\} \pmod{p}.$$

Можемо ще одначе усунути один із елементів j, так що в розвязці буде приходити тільки одна j. Именно є $j_1^3 j_2 \equiv A j_1^2$; помножім $MC \equiv A$, то $j_2 \equiv M j_1^2$, отже коли напишемо j за j_1, а Mj^2 за j_2, то:

$$\left.\begin{array}{l} y_1 \equiv j\ (1 + Mj), \\ y_2 \equiv j\ (\alpha^2 + \alpha Mj), \\ y_3 \equiv j\ (\alpha + \alpha^2 Mj), \end{array}\right\} \pmod{p}.$$

В тім разї є всї три розвязки величинами в $GF[p^3]$, а наша розвязка лежала в тім, що ми виразили всї три y при помочи коріня можливо найпростїйшої модулової функції $j^3 - C \equiv 0 \pmod{p}$.

3) $p = 6n - 1$, тоді C є завсїди останком, а γ належить до $GF[p^2]$, отже маємо

$$\left.\begin{array}{l} y_1 \equiv \tau_1 + \tau_2 \\ y_2 \equiv \frac{p-1}{2}\left[(\tau_1 + \tau_2) + \varepsilon(\tau_1 - \tau_2)\right] \\ y_3 \equiv \frac{p-1}{2}\left[(\tau_1 + \tau_2) - \varepsilon(\tau_1 - \tau_2)\right] \\ \tau_1 \tau_2 \equiv A,\ \varepsilon^2 \equiv -3 \end{array}\right\} \pmod{p}.$$

В тім разї є y_1 дїйсне, а y_2 і y_3 є спряжені в $GF[p^2]$.

III $\left(\frac{D}{p}\right) = -1$. Тодї конґруенція $D \equiv \beta^2$ є незведима, отже β належить до $GF[p^2]$. Положім $\beta = i$, то се дасть $v \equiv B \pm i$, і

$$t^3 \equiv B + i.$$

Заложім

$$t_1 \equiv a + b\,i,$$

де a і b є величинами з $GF[p]$ або $GF[p^3]$, то злучена з t_1 величина t_2 має форму

$$t_2 \equiv a \quad b\,i.$$

Порівнанє сочинників при $t^3 \equiv B + i$ і ${t_1}^3 \equiv (a + b\,i)^3$ дає такі дві реляції:

$$a(a^2 + 3b^2 D) \equiv B,\ b(3a^2 + b^2 D) \equiv 1 \pmod{p}.$$

Коли дана конґруенція є рішима, то обі ті реляції є рівночасно рішимі в дїйсних числах, отже маємо

$$\left.\begin{array}{l} y_1 \equiv t_1 + t_2 \equiv 2a \\ y_2 \equiv \gamma^2(a + bi) + \gamma(a - bi) \equiv -a + (\gamma^2 - \gamma) b\,i \\ y_3 \equiv \gamma(a + b\,i) + \gamma^2(a - b\,i) \equiv -a - (\gamma^2 - \gamma) b\,i \end{array}\right\} \pmod{p}.$$

а) Коли $p = 6n + 1$, то $\gamma^2 - \gamma \equiv \alpha^2$ α є дійсне; положім ще $m \equiv b^2(\alpha^2 - \alpha)$, то $m^2 \equiv -3b^2$, отже

$$\left.\begin{array}{l} y_1 \equiv 2\alpha \\ y_2 \equiv -\alpha + mi \\ y_3 \equiv -\alpha - mi \\ m^2 \equiv -3b^2,\ i^2 \equiv D \end{array}\right\} \text{(mod. } p\text{)}.$$

Отже одна розвязка є дійсна, дві инші з $GF[p^2]$.

б) Коли $p = 6n - 1$, то $\gamma^2 - \gamma \equiv -1$; положім $\varepsilon i \equiv \omega$, то се є дійсне число, бо коли $\varepsilon^2 \equiv -3$, $i^2 \equiv D$, то $(\varepsilon i)^3 \equiv -3D$, а коли $\left(\frac{D}{p}\right) = -1$, то $\left(\frac{-3D}{p}\right) = +1$. Отже маємо

$$\left.\begin{array}{l} y_1 \equiv 2\alpha \\ y_2 \equiv -\alpha - b\omega \\ y_3 \equiv -\alpha + b\omega \\ \omega^2 \equiv -3D \end{array}\right\} \text{(mod. } p\text{)}$$

Проте в тім разї маємо три дійсні розвязки; тут маємо повну аналогію до casus irreducibilis рівнань третього степеня.

Примір

$$y^3 + 5y + 4 \equiv 0 \text{ (mod. 11)}.$$

Маємо тут $A \equiv 2$, $B \equiv -2$, отже $D \equiv -4$, а що $\left(\frac{-4}{11}\right) = \left(\frac{-1}{11}\right) = -1$, то можемо положити $i^2 \equiv -4$ (mod. 11), або коли за i вправадити величину $\vartheta = 5i$, т. зн. $\vartheta^2 \equiv -1$ (mod. 11) отже ϑ буде мати вартість звичайного Gauss-ового символа i. Супроти того квадратна ресольвента прийме вид

$$v^2 + 5v - 3 \equiv 0 \text{ (mod. 11)},$$

а її розвязка є $v \equiv -2 \pm 2\vartheta$ (mod. 11), отже

$$t^3 \equiv -2 + 2\vartheta.$$

Положім $t = a + b\vartheta$, то одержимо дві конґруенції

$$\left.\begin{array}{l} a^3 - 3ab^2 \equiv -2 \\ 3ab - b^3 \equiv 2 \end{array}\right\} \text{(mod. 11)}$$

яких розвязкою є $a \equiv 1$, $b \equiv 1$, отже $t_1 \equiv 1 + \vartheta$, $t_2 = 1 - \vartheta$. З $\varepsilon^2 \equiv -3$, $\vartheta^2 \equiv -1$ слїдує $(\varepsilon\vartheta)^2 \equiv 3$, т. зн. $\varepsilon\vartheta \equiv \omega \equiv 5$ (mod. 11), отже

$$\left.\begin{array}{l} y_1 \equiv 2 \\ y_2 \equiv -1 - 5 \equiv -6 \\ y_2 \equiv -1 + 5 \equiv 4 \end{array}\right\} \text{(mod. 11)}.$$

IV. Коли-ж дана конґруенція є незведима, то всї три розвязки належать до $GF[p^3]$, а модулова функція не дасть ся в тім разї звести до двочленної. Назвім один корінь даної конґруенції j, то два инші корінї є j^p і j^{p^2}

37. **Зіставлене.** Рішимість конґруенції залежить від того, чи циклїчний визначник Δ степеня $p-1$, утворений з її сочинників, є $\equiv 0 \pmod{p}$, чи ні.

I. $\Delta \equiv 0 \pmod{p}$; тоді маємо:

1) коли $\left(\frac{D}{p}\right) = +1$, а) для $p = 6n+1$ 3 корінї;

б) для $p = 6n-1$ 1 корінь;

2) коли $\left(\frac{D}{p}\right) = -1$, а) для $p = 6n+1$ 1 корінь;

б) для $p = 6n-1$ 3 корінї.

Щоби усунути ріжницю поміж обома формами числа p, положім за Мірімановим[1])

$$R \equiv -3D \pmod{p},$$

то $\left(\frac{R}{p}\right) = \left(\frac{-3}{p}\right)\left(\frac{D}{p}\right)$, а що $\left(\frac{-3}{p}\right) = \pm 1$ для $p = 6n \pm 1$, то маємо

1. а) $\left(\frac{D}{p}\right) = +1$, $\left(\frac{-3}{p}\right) = +1$, отже $\left(\frac{R}{p}\right) = +1$,

1. б) $\left(\frac{D}{p}\right) = +1$, $\left(\frac{-3}{p}\right) = -1$, отже $\left(\frac{R}{p}\right) = -1$;

2. а) $\left(\frac{D}{p}\right) = -1$, $\left(\frac{-3}{p}\right) = +1$, отже $\left(\frac{R}{p}\right) = -1$,

2. б) $\left(\frac{D}{p}\right) = -1$, $\left(\frac{-3}{p}\right) = -1$, отже $\left(\frac{R}{p}\right) = +1$.

Проте можемо сказати коротко: конґруенція має три дїйсні корінї, коли $\left(\frac{R}{p}\right) = +1$, один дїйсний корінь, коли $\left(\frac{R}{p}\right) = -1$.

II. Коли $\Delta \not\equiv 0 \pmod{p}$, то конґруенція є нерішима.

Конґруенції четвертого степеня.

38. **Двочленна одиничка конґруенція**

$$z^4 \equiv 1 \pmod{p} \qquad (8)$$

має все два дїйсні корінї $+1$ і -1; її первісні корінї залежать від

$$z^2 + 1 \equiv 0 \pmod{p}. \qquad (8a)$$

Коли $p \equiv 1 \pmod 4$, то $\left(\frac{-1}{p}\right) = +1$. отже (8a) має два дїйсні корінї $\alpha \equiv g^{\frac{p-1}{4}} \pmod{p}$ і $\alpha^3 \equiv -\alpha$, так що всї корінї конґруенції (8) є

[1]) D. Mirimanoff, Sur les congruences du troisième dégré, Enseignement mathématique, t. IX. (1907), p. 381—384.

$$1,\ \alpha,\ -1,\ -\alpha.$$

В разї $p \equiv -1 \pmod 4$ є $\left(\frac{-1}{p}\right) = -1$, отже оба корінї конґруенції (8а) є в $GF[p^2]$. Назвім одну з величин в $GF[p^2]$ γ, тодї маємо такі корінї конґруенції (8):

$$1,\ \gamma,\ -1,\ -\gamma.$$

39. **Для загальної двочленної конґруенції**

$$x^4 \equiv A \pmod p \tag{9}$$

є крітерією рішимости $A^{\frac{p-1}{4}} \equiv 1 \pmod p$; в разї $p \equiv 1 \pmod 4$ мусить отже бути A двоквадратним, в разї $p \equiv -1 \pmod 4$ квадратним останком. Проте в першім разї має конґруенція (9) 4 або 0 дїйсних корінїв,

$$r,\ \alpha r,\ -r,\ -\alpha r,$$

в другім разї 2 або 0 дійсних

$$r,\ \gamma r,\ -r,\ -\gamma r.$$

Коли крітерія рішимости несповнена, тодї дефінїює дана конґруенція $GF[p^4]$.

40. **Повну конґруенцію четвертого степеня**

$$F(x) = a_0 x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 \equiv 0 \pmod p \tag{10}$$

зводимо до зредукованої форми

$$f(y) = y^4 - 6 L y^2 - 4 M y - 3 N \equiv 0 \pmod p. \tag{11}$$

Нехай її корінї будуть y_1, y_2, y_3, y_4, то їх основні симетричні функції є $\sigma_1 \equiv 0$, $\sigma_2 \equiv -6 L$, $\sigma_3 \equiv 4 M$, $\sigma_4 \equiv -3 N$.

Утворім такі три ресольвенти:

$$\left.\begin{aligned} 4 v_1 &\equiv (y_1 + y_2 - y_3 - y_4)^2 - 16 L \\ 4 v_2 &\equiv (y_1 - y_2 + y_3 - y_4)^2 - 16 L \\ 4 v_3 &\equiv (y_1 - y_2 - y_3 + y_4)^2 - 16 L \end{aligned}\right\} \pmod p, \tag{12}$$

або коли положимо для скороченя

$$\begin{aligned} a &= (y_1 + y_2 - y_3 - y_4)^2, \\ b &= (y_1 - y_2 + y_3 - y_4)^2, \\ c &= (y_1 - y_2 - y_3 - y_4)^2, \end{aligned}$$

то будемо мати

$$\left.\begin{aligned} 4 v_1 &\equiv a - 16 L \\ 4 v_2 &\equiv b - 16 L \\ 4 v_3 &\equiv c - 16 L \end{aligned}\right\} \pmod p.$$

Щоби найти конґруенцію, від якої залежать v_1, v_2, v_3, творимо основні симетричні функції

$$\begin{aligned} 4 (v_1 + v_2 + v_3) &= \tau_1 - 48 L, \\ 16 (v_1 v_2 + v_2 v_3 + v_3 v_1) &= \tau_2 - 32 \tau_1 L + 3.16^2 L^2, \\ 64 v_1 v_2 v_3 &= \tau_3 - 16 \tau_2 L + 16^2 \tau_1 L^2 - 16^3 L^3, \end{aligned}$$

де $\tau_1 = a + b + c$, $\tau_2 = a\,b + b\,c + c\,a$, $\tau_3 = a\,b\,c$. Ті три остатні величини легко обчислити; вони є

$$\tau_1 = 3\,\sigma_1{}^2 - 8\,\sigma_2,$$
$$\tau^2 = (3\,\sigma_1{}^3 - 16\,\sigma_1\,\sigma_2 + 16\,\sigma_3)\,\sigma_1 + 16\,\sigma_2{}^2 - 64\,\sigma_4,$$
$$\tau_3 = (\sigma_1{}^3 - 4\,\sigma_1\,\sigma_2 + 8\,\sigma_3)^2,$$

а з огляду на вартости функцій σ маємо

$$\tau_1 = 48\,L,$$
$$\tau_2 = 16.12\,(3\,L^2 + N),$$
$$\tau_3 = 64.16\,M^2.$$

Звідси слїдує передовсїм

$$4\,(v_1 + v_2 + v_3) = \tau_1 - 48\,L \equiv 0,$$

а проте можемо обі прочі функції написати так:

$$16\,(v_1\,v_2 + v_2\,v_3 + v_3\,v_1) = \tau_2 - 16\,\tau_1\,L,$$
$$64\,v_1\,v_2\,v_2 = \tau^3 - 16\,\tau_2\,L + 2.16^3\,L^3,$$

отже врешті є

$$v_1\,v_1 + v_2\,v_3 + v_3\,v_1 = -\,12\,(L^2 - N),$$
$$v_1\,v_2\,v_3 = 16\,(M^2 - 3\,L\,N - L^2).$$

Проте конґруенція для v (ресольвента третього степеня) є

$$\varphi(v) = v_2 - 12\,(L^2 - N)\,v - 16\,(M^2 - 3\,L\,N - L^3) \equiv 0 \pmod{p}. \quad (13)$$

Знайшовши її три корінї, v_1, v_2, v_3, творимо

$$a \equiv 4\,v_1 + 16\,L,$$
$$b \equiv 4\,v_2 + 16\,L,$$
$$c \equiv 4\,v_3 + 16\,L$$

і розвязуємо три квадратні конґруенції

$$\left.\begin{aligned} 16\,X^2 &\equiv a \\ 16\,Y^2 &\equiv b \\ 16\,Z^2 &\equiv c \end{aligned}\right\} \pmod{p}. \quad (14)$$

Коли маємо їх корінї, находимо корінї даної конґруенції (11) з

$$\left.\begin{aligned} y_1 + y_2 + y_3 + y_4 &\equiv 0 \\ y_1 + y_2 - y_3 - y_4 &\equiv 4\,X \\ y_1 - y_2 + y_3 - y_4 &\equiv 4\,Y \\ y_1 - y_2 - y_3 + y_4 &\equiv 4\,Z \end{aligned}\right\} \pmod{p}.$$

Вони є

$$\left.\begin{aligned} y_1 &\equiv X + Y + Z \\ y_2 &\equiv X - Y - Z \\ y_3 &\equiv -X + Y - Z \\ y_4 &\equiv -X - Y + Z \end{aligned}\right\} \pmod{p}. \quad (15)$$

З конґруенцій (14) одержуємо по дві вартости на X, Y, Z; в розвязцї (15) треба їх так комбінувати, щоби було

$$4\,X\,Y\,Z \equiv M \pmod{p}, \quad (16)$$

отже, коли заложимо, що M в (mod. p) додатне, т. зн. $< \frac{p-1}{2}$, то скількість відємних (mod. p) величин, т. є X, Y, $Z > \frac{p-1}{2}$, буде 0 або 2. Можна також так поступити, що знайшовши дві з них, третю винаходимо з реляції (16).

41. **Дискусія.** Конґруенція (11) і її ресольвента (13)[1]) мають однаковий виріжник

$$D \equiv 64\,[(M^2 - 3LN - L^3)^2 - (L^2 - N)^3]. \qquad (17)$$

Від нього залежить якість розвязки.

I. Коли $D \equiv 0$ (mod. p), то $\varphi(v) \equiv 0$ має один многократний корінь, який може бути: 1) трикратний, 2) двократний.

1) Коли (13) має трикратний корінь $v_1 = v_2 = v_3$, то він є $\equiv 0$ (mod. p), проте ресольвента є

$$\varphi(v) = v^3 \equiv 0 \pmod{p}.$$

В такім разі є оба вищі сочинники в $\varphi(v)$ пристайні до зера:

$$L^2 - N \equiv 0,\ M^2 - 3LN - L^3 \equiv 0 \pmod{p},$$

тому панують поміж ними такі звязи:

$$N \equiv L^2,\ M^2 \equiv 4L^3 \pmod{p},$$

отже L мусить бути квадратним останком для p.

Звідси слїдує дальше: $a = b = c \equiv 16L$, проте $16X^2 \equiv 16L$ або

$$X^2 \equiv L \pmod{p},$$

а що $\left(\frac{L}{p}\right) = +1$, то ся конґруенція є рішима, отже X дїйсне. Назвім її корінь X, тоді є $Y \equiv Z \equiv X$, проте

$$z_1 \equiv 3X,\ y_2 \equiv y_3 \equiv y_4 \equiv -X.$$

Конґруенція четвертого степеня, якої ресольвента (13) має потрійний корінь, виглядає так:

$$f(y) = (y - 3X)(y + X)^3 \equiv 0 \pmod{p},$$

отже вона має один однократний, один трикратний корінь.

Замітка. Коли $X \equiv 0$, тоді $f(y)$ має чотирократний корінь; тоді є $L \equiv 0$, отже і $M \equiv 0$, $N \equiv 0$, а конґруенція звучить $f(y) = y^4 \equiv 0 \pmod{p}$.

2) Коли ресольвента має один двократний дїйсний корінь $v_2 = v_3$, то кладучи $v_1 \equiv 2z$, (z дїйсне) маємо $v_2 = v_3 \equiv -z$, отже

$$\varphi(v) = v^3 - 3z^2 v - 2z^3 \equiv 0 \pmod{p}.$$

---

[1]) Ресольвентами називаємо і функції, яких уживаємо до розвязки рівнання (чи конґруенції), і рівнанє (конґруенцію), від якого вона залежить. Непорозуміня нема тут чого побоювати ся.

Для визначеня z маємо реляцію $z^2 \equiv 4(L^2 - N)$; вона є завсїди рішима, бо з огляду $D \equiv 0$ є $(M^2 - 3LN - L^3)^2 \equiv (L^2 - N)^3$, отже $\left(\frac{L^2 - N}{p}\right) = +1$. Тодї є

$$\begin{aligned} a &\equiv 4(4L + 2z), \\ b = c &\equiv 4(4L \quad z). \end{aligned}$$

Дальше розвязуємо

$$\left.\begin{aligned} 16X^2 &\equiv 4(4L + 2z) \\ 16Y^2 = 16Z^2 &\equiv 4(4L \quad z) \end{aligned}\right\} \pmod{p} \qquad (18)$$

і маємо врештї

$$\left.\begin{aligned} y_1 &\equiv X + 2X \\ y_2 &\equiv X - 2Y \\ y_3 = y_4 &\equiv - X \end{aligned}\right\} \pmod{p},$$

отже один двократний корінь. Другий корінь є лише тодї двократний, коли $Y \equiv 0 \pmod{p}$.

а) $Y \not\equiv 0 \pmod{p}$. В такім разї (11) виглядає так:

$$f(y) = y^4 - 2(X^2 - 2Y^2)y^2 - 8XY^2 + X^2(X^2 - 4Y^2) \equiv 0 \pmod{p}. \quad (11a)$$

Чи X і Y можуть належати до иншого поля, як до $GF[p]$? Сочинники конґруенції (11a) мусять бути дїйсні; коли отже положимо $X = \alpha + \beta i$, $Y = \gamma + \delta i$, де i належить до $GF[p^2]$, то се доведе до таких реляцій:

$$\left.\begin{aligned} 2\gamma\delta &\equiv \alpha\beta \\ (2\alpha^2 + \gamma^2 + \delta^2 i^2)\beta &\equiv 0 \\ (\alpha\beta - 2\gamma\delta)(\alpha^2 + \beta^3 i^2) &\equiv 2\alpha\beta(\gamma^2 + \delta^2 i^2) \end{aligned}\right\} \pmod{p}.$$

Супротн першої реляції зводить ся третя до

$$(\gamma^2 + \delta^2 i^2)\alpha\beta \equiv 0,$$

а в злуцї з другою дає $\alpha^3\beta \equiv 0$. Звідси слїдує, що мусить бути $\alpha \equiv 0$ або $\beta \equiv 0$, а проте і одна з величин γ і δ рівно-ж $\equiv 0$.

Нехай буде перше $\alpha \not\equiv 0$, $\beta \equiv 0$; се не накладає на γ і δ нїякого иншого обмеженя, як тільки те, що одна з них є $\equiv 0$, т. зн. Y^2 є дїйсне. Коли-ж $\alpha \equiv 0$, $\beta \not\equiv 0$, тодї з другої реляції слїдує $\gamma \equiv \delta \equiv 0$; отже коли в X дїйсна часть є $\equiv 0$, тодї є або $X \equiv 0$, або $Y \equiv 0 \pmod{p}$. Проте всї сочинники конґруенції (11a) є дїйсні, і корінї або всї дїйсні, або двократний дїйсний, а два прочі належать до $GF[p^2]$.

б) $Y \equiv 0 \pmod{p}$ потягає за собою $z \equiv 4L$, т. зн. $3L^2 + N \equiv 0 \pmod{p}$. Се вимагає, щоби було $\left(\frac{-3N}{p}\right) = +1$ і дальше, з огляду на $D \equiv 0$, $M^2(M^2 + 16L^3) \equiv 0 \pmod{p}$. Тут мусить бути $M \equiv 0$, бо

$M^2 = -16L^3$ веде до $L \equiv 0$, отже рівно-ж і тоді було би $M \equiv 0$. Проте дана конґруенція виглядає так:

$$f(y) = (y^2 - X^2)^2 \equiv 0 \pmod{p},$$

а її корінї є $y_1 = y_2 \equiv X$, $y_3 = y_4 \equiv -X$.

42. Коли циклїчний визначник Δ, степеня $p-1$, утворений з сочинників ресольвенти $\varphi(v)$, є пристайний до 0 (mod. p), тоді $\varphi(v) \equiv 0$ має три або один дїйсний корінь, відповідно до квадратного характеру величини $R = -3D$.

II. $\left(\frac{R}{p}\right) = +1$; v_1, v_2, v_3 є дїйсні, ріжні поміж собою. Утворім a, b, c і означім характери символів $\left(\frac{a}{p}\right)$, $\left(\frac{b}{p}\right)$, $\left(\frac{c}{p}\right)$. З поміж усїх можливих їх комбінацій є допустимі такі:

α) один з поміж тих символів є $= 0$;

β) два або три символи є $= 0$;

γ) всї три символи мають вартість $+1$;

δ) один символ є $+1$, два -1.

Евентуальности, щоби один або три символи були -1, є недопустимі, бо abc є квадратом.

α) Коли одна з величин a, b, c є $\equiv 0$, тоді мусить бути одно $v \equiv -4L$; коли подїлимо $\varphi(v)$ через $v + 4L$, одержимо як вимогу подїльности $M \equiv 0$, отже ресольвента має такі корінї:

$$\begin{aligned} v_1 &\equiv -4L, \\ v_2 &\equiv 2L + 2T, \\ v_3 &\equiv 2L - 2T, \end{aligned}$$

де T залежить від $T^2 \equiv 3N$, а $X \equiv 0$. Проте корінї даної конґруенції є

$$\left.\begin{aligned} y_1 - y_2 &\equiv Y + Z \\ y_3 \equiv -y_3 &\equiv Y - Z \end{aligned}\right\} \pmod{p}.$$

α_1) Коли $\left(\frac{3N}{p}\right) = +1$, то v_2 і v_3 є дїйсні, а Y і Z дїйсні або мнимі, відповідно до характерів величин $6L \pm 2T$.

α_2) Коли $\left(\frac{3N}{p}\right) = -1$, то v_2 і v_3 належать до $GF[p^2]$, отже маємо

$$\left.\begin{aligned} 4Y^2 &\equiv 6L + 2i \\ 4Z^2 &\equiv 6L - 2i \\ i^2 &\equiv 3N \end{aligned}\right\} \pmod{p},$$

т. зн. Y і Z є спряжені в $GF[p^2]$. Положім $Y = \alpha + \beta i$, $Z = \alpha - \beta i$, то α і β находимо з

$$\left.\begin{array}{c} 4\,\alpha\,\beta \equiv 1 \\ 2\,(\alpha^2 + \beta^2\, i^2) \equiv 3\,L \end{array}\right\} \pmod{p}.$$

Еліміную̈чи з другої конґруенції $\beta \equiv \frac{1}{4\,\alpha}$, одержимо

$$16\,\alpha^4 + 24\,L\,\alpha^2 + 3\,N \equiv 0 \pmod{p}. \qquad (18)$$

При помочи α виразимо корінґ y так:

$$\left.\begin{array}{c} y_1 \equiv -\,y_2 \equiv 2\,\alpha \\ y_3 \equiv -\,y_4 \equiv 2\,\beta\,i \end{array}\right\} \pmod{p},$$

де $2\,\beta$ є (mod. p) товаришем величини $2\,\alpha$.

Конґруенція для α (18) є рівнозначна з

$$(4\,\alpha^2 + 3\,L)^2 \equiv 9\,L^2 - 3\,N \pmod{p}. \qquad (18a)$$

Займім ся ії правою стороною. Вона не може бути $\equiv 0$, бо тодї було би $N \equiv 3\,L^2$, т. зн. $4\,\alpha^2 \equiv -\,3\,L$, отже мусїло би бути $\left(\frac{9\,L^2}{p}\right) = -\,1$, а се недорічність. Отже можливе тільки таке, що $\left(\frac{9\,L^2 - 3\,N}{p}\right) = +\,1$ або $-\,1$.

В першім разї, $\left(\frac{9\,L^2 - 3\,N}{p}\right) = +\,1$, положім $9\,L^2 - 3\,N = U^2$; се дасть

$$4\,\alpha^2 \equiv -\,3\,L \pm U;$$

тут знова може бути $\left(\frac{-\,3\,L \pm U}{p}\right) = \pm\,1$. В разї $+\,1$ є α дїйсне, отже y_1 і y_2 дїйсні, а y_3 і y_4 належать до $GF[p^2]$; в разї $-\,1$ дїєть ся навпаки. Тому, коли $\left(\frac{9\,L^2 - 3\,N}{p}\right) = +\,1$, маємо два корінґ дїйсні, противних знаків, а два другі чисто мнимі спряжені в $GF[p^2]$.

Коли-ж врешті $\left(\frac{9\,L^2 - 3\,N}{p}\right) = -\,1$, то положім $9L^2 - 3\,N \equiv j^2$, де j належить до $GF[p^2]$, отже є

$$4\,\alpha^2 \equiv -\,3\,L \pm j.$$

Положім ще $\alpha = \mu + \nu\,j$, то се доведе до конґруенції

$$(8\,\mu^2 + 3\,L)^2 \equiv 3\,N \pmod{p},$$

яка є, з огляду на $\left(\frac{3N}{p}\right) = -\,1$, нерішима в $GF[p]$. Проте конґруенція (18) є нерішима в $GF[p^2]$, отже мусимо за α приймити якусь величину з $GF[p^4]$; тодї j дасть ся виразити через α:

$$j \equiv 4\,\alpha^2 + 3\,L,$$

отже шукана розвязка звучить:

$$\left.\begin{array}{c} y_1 \equiv -\,y_2 \equiv 2\,\alpha \\ y_3 \equiv -\,y_4 \equiv 2\,\beta\,(4\,\alpha^2 + 3\,L) \\ 4\,\alpha\,\beta \equiv 1 \end{array}\right\} \pmod{p}.$$

β) Коли ще другий з символів $\left(\frac{a}{p}\right), \left(\frac{b}{p}\right), \left(\frac{c}{p}\right)$ є 0, то через дальше ділене дійдемо до вимоги $3N \equiv 7L^2$, т. зн.

$$f(y) = y^4 - 6Ly^2 - 7L^2 \equiv 0 \pmod{p};$$

квадратами її корінів є

$$y^2 \equiv 7L \text{ і } -L.$$

Одержуємо проте дві пари корінів рівних, з противними знаками; вони можуть або бути дійсні, або належати до $GF[p^2]$.

Коли-ж всі три символі є $= 0$, то звідси слідує $L = 0$, отже маємо чотирократний корінь $y = 0$.

γ) Коли всі три символи, $\left(\frac{a}{p}\right), \left(\frac{b}{p}\right), \left(\frac{c}{p}\right)$, є $= +1$, то X, Y, Z є дійсні; дана конґруенція має чотири ріжні, дійсні розвязки.

δ) Нехай врешті буде $\left(\frac{b}{p}\right) = \left(\frac{c}{p}\right) = -1, \left(\frac{a}{p}\right) = +1$; тоді є X дійсне, Y і Z мнимі. Заложім $Y = \alpha + \beta i$, $Z = \gamma + \delta i$, тоді мусить бути $\gamma \equiv \pm \alpha$, $\delta \equiv \mp \beta \pmod{p}$, бо $4XYZ \equiv M$ є дійсне. Величини α і β визначуємо з конґруенцій

$$\left.\begin{aligned} X^2 + 2(\alpha^2 + \beta^2 i^2) &\equiv 3L \\ 4X(\alpha^2 - \beta^2 i^2) &\equiv M \end{aligned}\right\} \pmod{p},$$

а маючи їх, одержуємо такі корінї конґруенції (11):

$$\left.\begin{aligned} y_1 &\equiv X + 2\alpha \\ y_2 &\equiv X - 2\alpha \\ y_3 &\equiv -X + 2\beta i \\ y_4 &\equiv -X - 2\beta i \end{aligned}\right\} \pmod{p},$$

отже y_1, y_2 і y_3, y_4 творять дві пари розвязок: одну дійсну, другу спряжену в $GF[p^2]$.

43. В разї, коли III $\left(\frac{R}{p}\right) = -1$, ресольвента має один дійсний корінь, а два инші спряжені в $GF[p^2]$:

$$\left.\begin{aligned} v_1 &\equiv -2\alpha \\ v_2 &\equiv \alpha + \beta i \\ v_3 &\equiv \alpha - \beta i \end{aligned}\right\} \pmod{p},$$

отже ресольвента є

$$\varphi(v) = v^3 - (3\alpha^2 + \beta^2 i^2)v + 2\alpha(\alpha^2 - \beta^2 i^2) \equiv 0 \pmod{p},$$

а величини a, b, c мають рівно-ж форму $A + Bi$. В тім разї належать корінї y або до $GF[p^2]$, або до $GF[p^4]$, подібно як попередно.

IV. Коли ресольвента $\varphi(v) \equiv 0 \pmod{p}$ є незведима, то X, Y, Z, які залежать від її корінів, є величинами, спряженими

в $GF[p^3]$. Отже $X+Y+Z$ є дійсне, т. зн. y_1 є дійсне, а три прочі корінь належать до $GF[p^3]$.

44. Як виконувати операції на величинах поля Galois, покажемо на слідуючім примірі:

$$f(y) = y^4 - 5y^2 + 7y - 5 \equiv 0 \pmod{19}.$$

Тут є $L \equiv 4$, $M \equiv 3$, $N \equiv 8 \pmod{19}$, отже ресольвента звучить:

$$\varphi(v) = v^3 - v + 3 \equiv 0 \pmod{19}.$$

Її виріжник є $D \equiv -5$, а що $\left(\frac{-5}{19}\right) = -1$, то вона має один дійсний корінь -4 і два инші $2(1 \pm i)$, де i дане реляцією

$$i^2 \equiv 2 \pmod{19}. \qquad (*)$$

Тому є

$$\left.\begin{aligned} 16X^2 &\equiv a \equiv -9 \\ 16Y^2 &\equiv b \equiv -4+8i \\ 16Z^2 &\equiv c \equiv -4-8i \end{aligned}\right\} \pmod{19}.$$

Перша зводить ся до

$$X^2 \equiv 3 \pmod{19}, \qquad (**)$$

а що $\left(\frac{3}{19}\right) = -1$, то X належить до $GF[p^2]$; проте можемо його виразити через i. Робимо се так: множимо в собою (*) і (**), се дає $(Xi)^2 \equiv 6 \equiv 5^2$, $Xi \equiv \pm 5$, $Xi^2 \equiv 2X^2 \equiv \pm 5i$, отже

$$X \equiv \pm 7i;$$

нам вистарчить знати одну вартість, пр. $X \equiv 7i$.

Опісля находимо Y і Z, так що положимо

$$Y = \alpha + \beta i,\ Z = \alpha - \beta i;$$

се дає з огляду на $a+b+c \equiv 16(X^2+Y^2+Z^2) \equiv 2$

$$\left.\begin{aligned} \alpha^2 + 2\beta^2 &\equiv -5 \\ \alpha\beta &\equiv 5 \end{aligned}\right\} \pmod{19}.$$

Звідси еліминуємо β і одержуємо

$$\alpha^4 + 5\alpha^2 - 7 \equiv 0 \pmod{19} \qquad (***)$$

або

$$(\alpha^2 \quad 7)^2 \equiv -1 \pmod{19}.$$

-1 є знова не-останком для 19, отже треба корінь конґруенції $z^2 \equiv -1 \pmod{19}$ виразити через i; легко знайти, що $z \equiv 3i$, бо $z^2 \equiv 9i^2$. Отже є

$$\alpha^2 \equiv 7 + 3i \pmod{19}, \qquad (\dagger)$$

коли знова обмежимо ся до одного тільки знака.

Величина α, дана конґруенцією (***), дефініює $GF[p^4]$; при помочи реляції (†) можемо представити $GF[p^2]$, т. зн. i, через α:

$$i \equiv -5\alpha^2 + 4 \pmod{19}. \qquad (\dagger\dagger)$$

Остаточно треба ще виразити β згл. βi через α. $3\,\alpha\beta \equiv 5 \pmod{19}$ слїдує $\alpha^3 \beta i \equiv 5\,\alpha i$, т. зн.

$$(7 + 3i)\,\beta i \equiv 5\,\alpha i.$$

Розширюючи обі сторони спряженою величиною $7 - 3i$, одержимо з огляду на $(7 + 3i)(7 - 3i) = 49 - 9i^2 \equiv -8 + 1 \equiv 12$,

$$12\,\beta i \equiv 5\,\alpha i\,(7 - 3i) \equiv -3\,\alpha i + 4\,\alpha i^2,$$

отже дальше

$$12\,\beta i \equiv -\alpha(\alpha^2 - 7) + 8\,\alpha \equiv -\alpha^3 - 4\,\alpha,$$

т. зн.

$$\beta i \equiv -8\,\alpha^3 + 6\,\alpha.$$

Маємо отже

$$\left.\begin{aligned} X &\equiv -4\,\alpha^2 + 9 \\ Y &\equiv -8\,\alpha^3 + 7\,\alpha \\ Z &\equiv \quad 8\,\alpha^3 - 5\,\alpha \end{aligned}\right\} \pmod{19}.$$

Звідси слїдують корінї даної конґруенції, виражені при помочи коріньов простїйшої конґруенції (***):

$$\left.\begin{aligned} y_1 &\equiv -4\,\alpha^2 + 2\,\alpha + 9 \\ y_2 &\equiv -4\,\alpha^2 - 2\,\alpha + 9 \\ y_3 &\equiv \quad 3\,\alpha^3 + 4\,\alpha^2 - 7\,\alpha - 9 \\ y_4 &\equiv -3\,\alpha^3 + 4\,\alpha^2 + 7\,\alpha - 9 \end{aligned}\right\} \pmod{19}.$$

45. Як примір, в якім ресольвента 3. степеня є незвідима, отже приходить ся розвязувати квадратні конґруенції в $GF[p^3]$, розвяжемо таку конґруенцію:

$$f(y) = y^4 + y^2 - 2y + 3 \equiv 0 \pmod{7}.$$

Тут є: $L \equiv 1$, $M \equiv -3$, $N \equiv -1$, отже

$$\varphi(v) = v^3 - 3v + 1 \equiv 0 \pmod{7}.$$

Отся ресольвента є незведима; назвім один її корінь $v_1 \equiv j$, то два другі корінї є $v_2 \equiv j^2 - 2$, $v_3 \equiv -j^2 - j + 2$, (гл. уст. 16), отже

$$\left.\begin{aligned} a &\equiv -3j + 2 \\ b &\equiv -3j^2 + 1 \\ c &\equiv \quad 3j^2 + 3j + 3 \end{aligned}\right\} \pmod{7},$$

а квадратні конґруенції для X, Y, Y зводять ся до

$$\left.\begin{aligned} X^2 &\equiv \quad 2j + 1 \\ Y^2 &\equiv \quad 2j^2 - 3 \\ Z^2 &\equiv -2j^2 - 2j - 2 \end{aligned}\right\} \pmod{7}.$$

Першу з них розвяжемо так, що покладимо $X \equiv \alpha j^2 + \beta j + \gamma$, і визначуємо α, β, γ з

$$\left.\begin{aligned} 3\,\alpha^2 + 2\,\alpha\gamma + \beta^2 &\equiv 0 \\ \alpha^2 + \alpha\beta - 2\,\beta\gamma &\equiv -2 \\ \gamma^2 \quad 2\,\alpha\beta &\equiv 1 \end{aligned}\right\} \pmod{7};$$

се дає $\alpha \equiv 3$, $\beta \equiv 1$, $\gamma \equiv 0$, отже

$$X \equiv 3j^2 + j \pmod{7}.$$

Подібно знаходимо

$$Y \equiv -2j^2 - 3j + 3 \pmod{7},$$

а Z можемо обчислити зі звязи

$$4XYZ \equiv M \pmod{p},$$

т. є

$$XYZ \equiv 1 \pmod{7}.$$

Добуток XY є $\equiv \vartheta \equiv 2j^2 - 3j - 3$, отже

$$\vartheta Z \equiv 1 \pmod{7}.$$

Коли ϑ належить до виложника s, т. зн. $\vartheta^s \equiv 1 \pmod{7}$, то

$$Z \equiv \vartheta^{s-1} \pmod{7}.$$

Треба проте знайти виложник s; він мусить містити ся в $7^3 - 1 = 342 = 2 \cdot 3^2 \cdot 19$. Піднесїм ϑ до степеней 2, 3, 6, ., то найдемо $\vartheta^{57} \equiv 2$, отже

$$\vartheta^{57} Z \equiv 2Z \equiv \vartheta^{56} \pmod{7},$$

т. зн.

$$Z \equiv -3\vartheta^{56} \pmod{7},$$

а що $\vartheta^{56} \equiv 3j^2 + j - 3$, то

$$Z \equiv -2j^2 - 3j + 2 \pmod{7}.$$

Отже корінї даної конґруенції є

$$\left.\begin{array}{l} y_1 \equiv -j^2 + 2j - 2 \\ y_2 \equiv 2 \\ y_3 \equiv -3j^2 - j + 1 \\ y_4 \equiv -3j^2 - j - 1 \end{array}\right\} \pmod{7}.$$

Берлїн, май — червень 1913.

Résumé.

Gegenstand der vorliegenden Abhandlung bildet die Untersuchung der kubischen und der biquadratischen Kongruenzen mit Primzahlmodul im Galois'schen Felde. Dem eigentlichen Gegenstande geht ein Abriß der Theorie der Kongruenzen auf Grund der Eigenschaften des Galois'schen Feldes voran.

Mit den in Rede stehenden Kongruenzen hat sich schon Cauchy (1829) beschäftigt, ging aber über die Untersuchung der reduziblen Fälle nicht hinaus. Seine Methode ist der Lagrange'schen (für die kubischen bzw. biquadratischen Gleichungen) analog.

I. Die allgemeine kubische Kongruenz, auf die Form

$$f(y) = y^3 - 3Ay - 2B \equiv 0 \pmod{p}$$

reduziert, wird mit Hilfe der Resolventen gelöst:

$$\left.\begin{aligned} 27\,v_1 &= (3\,t_1)^3 \equiv (y_1 + \gamma y_2 + \gamma^2 y_3)^3 \\ 27\,v_2 &= (3\,t_2)^3 \equiv (y_1 + \gamma^2 y_2 + \gamma y_3)^3 \end{aligned}\right\} \pmod{p},$$

worin y_1, y_2, y_3 die Wurzeln von $f(y) \equiv 0$ sind, und γ durch

$$\gamma^2 + \gamma + 1 \equiv 0 \pmod{p}$$

gegeben wird; v_1 und v_2 hängen vor der Kongruenz ab

$$\varphi(v) = v^2 - 2Bv + A^2 \equiv 0 \pmod{p},$$

deren Diskriminante $D = B^2 - A^3$ zugleich Diskriminante von $f(y)$ ist.

Die Diskussion der Lösung führt zu folgenden Ergebnissen:

1) Ist $D \equiv 0 \pmod{p}$, so hat $f(y) \equiv 0$ eine doppelte, bzw. dreifache Wurzel; 2) ist $\left(\frac{-3D}{p}\right) = +1$, so hat die Kongruenz 3, ist 3) $\left(\frac{-D}{p}\right) = -1$, so hat sie nur eine reelle Wurzel, — vorausgesetzt, daß sie überhaupt lösbar ist. — Das Lösbarkeitskriterium lautet: es soll die zyklische aus den Koeffizienten der Kongruenz gebildete Determinante $(p-1)$ ter Ordnung $\equiv 0 \pmod{p}$ sein (König-Kronecker).

II. Die biquadratische Kongruenz reduziert man auf

$$f(y) = y^4 - 6Ly^2 - 4My - 3N \equiv 0 \pmod{p}$$

und führt als Resolventen ein

$$\left.\begin{aligned} 4\,v_1 &\equiv (y_1 + y_2 - y_3 - y_4)^2 - 16\,L \\ 4\,v_2 &\equiv (y_1 - y_2 + y_3 - y_4)^2 - 16\,L \\ 4\,v_2 &\equiv (y_1 - y_2 - y_3 + y_4)^2 - 16\,L \end{aligned}\right\} \pmod{p}$$

die von

$$\varphi((y) = v^3 - 12(L^2 - N)v - 16(M^2 - 3LN - L^3) \equiv 0 \pmod{p}$$

abhängen. Hat $\varphi(y) \equiv 0$ (die Resolventenkongruenz oder kurz: die Resolvente) eine Doppelwurzel, so hat auch die gegebene Kongruenz mehrfache Wurzeln, aber nur in diesem Falle.

Ist die Resolvente vollständig lösbar, also sind ihre Wurzeln v_1, v_2, v_3 reell,dann löst man die drei quadratischen Kongruenzen

$$\left.\begin{aligned}(y_1 + y_2 - y_3 - y_4)^2 &\equiv 4v_1 + 16L\\ (y_1 - y_2 + y_3 - y_4)^2 &\equiv 4v_2 + 16L\\ (y_1 - y_2 - y_3 + y_4)^2 &\equiv 4v_3 + 16L\end{aligned}\right\} \pmod{p};$$

nennt man ihre Lösungen $4X$, $4Y$, $4Z$, dann hat man:

$$\left.\begin{aligned}y_1 &\equiv X + Y + Z\\ y_2 &\equiv X - Y - Z\\ y_3 &\equiv -X + Y - Z\\ y^4 &\equiv -X - Y - Z\end{aligned}\right\} \pmod{p}.$$

Je nachdem die obigen quadratischen Kongruenzen alle lösbar sind oder nicht, bekommt man für die y entweder reelle Zahlen, oder Größen des Galois'schen Feldes der Ordnungen p^2 bzw. p^4.

Enthält die Resolvente einen irreduziblen quadratischen Faktor, so sind zwei von den v imaginär, d. h. konjugiert komplex im Galois'schen Felde der Ordnung p^2. Dann gehören die y dem Galois'schen Felde der Ordnungen p^2 oder p^4.

Ist schließlich die Resolvente irreduzibel, so hat die gegebene Kongruenz eine reelle Wurzel, und die drei übrigen gehören dem Galois'schen Felde der Ordnung p^3 an.

Дещо про теоретичне і методичне значінє сочинника температури скоростий процесів для хемічної кінетики.

НАПИСАВ

Др. Юлїян Гірняк.

Перед двома роками оголосив я в збірці кінетичних розвідок п. з. „Beiträge zur chemischen Kinetik. I.“, виданих Товариством ім. Шевченка у Львові, начерк поглядів, що випливають з експериментального материялу, зібраного мною в дослїдах над сочинником температури скоростий хемічних реакций. В сїм місци не можу, поки що, розвивати in extenso всїх думок там порушених, вже хочби з сеї причини, що й в згаданій публїкациї приходило ся менї з трудом упорядкувати річ в яку таку схему. Деяких, навіть дуже скомплїкованих квестий, вспів я діткнути ся ледви кількома словами, тому кілька важних, на мій погляд, моментів уважав я за відповідне висказати бодай в чисто афористичній формі (стор. 77, 88, 91, згаданої праці). Мушу також піднести, що деякі справи, там трактовані, уважаю тепер за передвчасно висунені так з огляду на методу представленя, як і з огляду на сучасну „констелляцию“ ріжнородних поглядів, що вибивають ся в літературі, а що найважнїйше — з огляду на призбираний, богатий експериментальний материял визначних дослїдників, на якім можна відразу оперти ся і деякі думки розвивати конкретно саме в ледви порушених, або й зовсїм тоді поминених фраґментах.

В сїм розуміню можна би зарезервувати на пізнїйшу пору увагу на значінє більшої або меншої симетрії реаґуючих молекулів (стор. 79 до 84). Тесаме сказав би я про думки, кинені на сторонах 85—86. За те цїлий натиск випадало би покласти передовсїм на сї моменти,

що ведуть до висуненя стеричних правильностий на перше місце цїлої хемічної кінетики. Отсю нотку присьвячу сій справі, щоби при тім ще й висказати, як і о скілько могли би сягнути консеквенциї згаданих думок в систему молекулярної хемії не лише в кінетичній, але й в її статичній области, коли би найголовнїйші зариси згаданих поглядів вдержали ся в будучности.

Річ однак в тім, щоби, після мого погляду, узгляднювати не так саму скорість хемічного процесу, як радше сочинник температури сеї скорости, увільняючи ся в експериментальних дослїдах, о скілько лише можна, від всяких каталїтичних впливів на самий процес (з виїмком перемін, в яких їх каталїчний перебіг є ґенетичною сутию цїлого механїзму реакциї, себто, коли першою фазою перемінн є переходова злука каталїзатора з реаґуючим молекулом).

Таке узгляднене сочинника температури можна би оперти і на кількох слїдуючих теоретичних арґументах.

Основною думкою всїх розумовань, опертих на другім законї термодинаміки, є в сути річи ідея ізотермічної рівноваги. Однак з умов одної одинокої температури не можна би а ргіогі нїчого вивести про якийнебудь материяльний уклад. Вистане вказати вже на славний цикль Карнота. А відтак всї методичні виводи, основані на другім родї неможливости perpetuum mobile, виходять, що найменше з двох температур, та комбінують характеристичну функцию $f(T, p, v)$ тїла в „макро-фізичнім“, розуміню з рівновагою енергії, зведеної до зера в замкненім циклї. Цїла отся аксіоматична термодинаміка, трактована чи то при помочи глибшої математичної аналїзи, чи без неї, не посунула би нас богато вперед поза те, що заміщує рівнане Clapeyron'a. Цїлий поступ і безперечний здобуток нових областий материяльної фізики і хемії — се лише примінене гіпотези Авоґадра до вище начеркненої ідеї. Чим однак не могла би ще бути цїла ся сьміла гіпотеза так в своїм заложеню як і в своїй доказовій арґументациї — як не унагляднением образом однакової вартости сочинника температури одної (чи радше двох) фізикальної прикмети всїх досконалих ґазів? В яких саме обсягах вартостий p і v тратить свою силу (в значіню нїм. Giltigkeit) характеристичне рівнане досконалих ґазів і розширене рівнане van der Waals'a, як — не там, де сочинники температури $\left(\frac{dp}{dt}\right)_v$, $\left(\frac{dv}{dt}\right)_p$ стають нерівнозвучні (nicht übereinstimmend) для поодиноких субстанций?

Абстрагуючи від непроглядного комплексу модерних молекулярних понять в цїлій области фізикальної хемії, комплексу спочиваючого на гіпотезї Авоґадра і безнастанних змаганях van der Waals'a та цїлої його школи, заакцентуймо лише факт, що цїла чисельна скаля абсолютної температури оперла ся о гіпотетичне зеро, виекстрапольоване з ідентичної вартости сочинника температури $\left(\frac{dv}{dt}\right)_p$ досконалих ґазів. Коли дальше перенесемо ся в область термічного супокою молекулярних системів ($T=0$) і поглянемо на форму нової гіпотези Nernst'a:

$$\left(\frac{dA}{dT}\right)_{T=0} = \left(\frac{dU}{dT}\right)_{T=0} = 0$$

зараз замітимо, що ся гіпотеза є пробою висказаня чогось конкретного про два дуже важні сочинники температури материяльних системів.

Досьвіди ствердять, о скілько ся гіпотеза окаже ся плідною в численних консеквенциях і відкритях, на які того рода тверджене повинно би напроваджувати. Поки що однак теорем Nernst'a заміщує лише чисто фізикальний зміст[1]) і не обіймає нїякого висказу про молекулярний механїзм материї. О скільки „хемічні сталі“ з него випроваджені приймуть в дїйсности усталені чисельні вартости, треба буде їх конечно механїстично в'інтерпретувати.

Наконець думаю, що злишно було би задержувати ся на універзальнім значіню функциї $p=f(Q, T)$ для якоїнебудь субстанциї в цїлій материяльній фізиці, фізикальній хемії, а навіть електрохемії. Вистане може загально натякнути, що до сеї функциї збігає всяка так чисто термодинамічна, як і чисто кінетична теория, що до неї стремлять не лише ширше закроєні ідеї небуденних дослїдників обох типів, але що в сїй функциї перехрещують ся дїйсно всякі звязи тепла і руху, вся дослїдна емпирия і здорова механїстична абстакция. Позволю собі висказати тут мій здогад, що кождий член сеї функциї (будьто поодиноко, будьто у відповідній частинній суммациї) є — що так висловлю — „дволичний“, т. зн. дасть ся раз термодинамічно, раз механїчно з'інтерпретувати. В статичній динаміці материї можна обі інтерпретациї зовсім довільно і без шкоди, т. зн. без наражуваня ся на суперечности, примінювати. Сьвідчать про се численні теоретичні проби Boltzmann'a, Voigt'a, G. Jäger'a і ин. при випроваджуваню функциї $p=f(Q, T)$ для насичених пар, в якій тепло парованя дало ся зіндентифікувати з молекулярною працею, при чім стала інтеґрациї дала ся звязати

[1]) Гл. Ph. Kohnstamm und Dr. L. S. Ornstein. Proc. of the section of sciences. v. XIV. 2 a part. 1912. Amsterdam.

безпосередно з ріжницею міжмолекулярних, вільних просторів раз в ґазовім, другий раз в плинним стані скупности. Можна би припускати[1]), що „хемічні сталі“ в рівнаню зближеним або й ідентичнім до рівнань Nernst'a дадуть ся вивести з того рода простірних вартостий, та що вони ґеометрично на них опруть ся. „Усталене“ їх піде найправдоподібнїйше по лїнїї узглядненя таких реляцій, особливо, коли загальна ассоцияційна теория ґазів і плинних тїл прибере конкретну форму.

Не входячи дальше в того рода рефлексиї, піднесїм один момент, що домінує, як очивидний аксіомат теоретичної думки в найголовнїйших питанях про явища материї. Ціла кінетика природи се лише рух молекулів та атомів (і електронів). Се, що ми називаємо температурою, се представляє лише інтензивність і зглядну скількість того руху, себ то напруженє, що його міримо емпіричним термометром. Коли ми прикладемо якенебудь функційне поняте або просто навіть першу лїпшу прикмету материї здовж температури, маємо тоді безперечно до діла з найповажнїйшою справою в матеріяльній фізиці або хемії. Тому все те, що ми називаємо сочинником температури, дотикає непроглядного комплексу функційних звязей всїх матеріяльних явищ. Навіть чиста термодинаміка не обійшла ся і не обійде ся без свого, собі питомого, „сочинника“. Вона однак нїколи не досягне механїзму справ, рівнаня $p = f(Q, T)$ дотикає ся лише з зовнїшної, граничної сторони, і що найвисше констатує, як ся функция є нечувано „вразлива“ на зміну температури. Взагалї отже треба піднести, що чим більшу вартість матиме функция $\frac{dD}{dT}$, в якій D означує якунебудь більше або менше скомплїковану дефінїцию, виведену з прикмет материї, тим ся функция глибше сягає в молекулярну суть механїзму матеріяльного явища, тим близше підходить вона до области чистої кінетики, і тим заразом більше віддалює вона нас від царини чистої термодинаміки, яка приймає тут постепенно ролю емпириї, передаючи теоретичний провід так в самій ідеї, як і методї чистій кінетиці.

Отсих кілька думок кидаю тут лише афористично, будучи тепер занятим сими питанями. В короткім часї, надїю ся, висловлю ся про се обширнїйше і в більше конкретній формі. Роблю се тому, щоби зазначити, що новий теорем Nernst'a вимагає як раз найбільше з того становиска докладнїйшого висьвітленя т. зн. в молекулярній области чистої хемії, а не із становиска „макрофізичних“ звязей поодиноких станів скупности.

[1]) Саме бажаю сю річ близше розслїдити кількома пробними рахунками.

Стерична динаміка концентрує ся до нинїшного дня виключно на дискусиї самої скорости хемічного процесу, отже явища на скрізь ізотермічного. На основі кількох повисших натяків уважаю сей напрям за зовсїм схиблений з теоретичного становиска, бо так не поступає навіть термодинамічна статика. Ся річ кидає ся тим більше в очи, що сочинник температури скорости хемічного процесу належить до найвисших, які лише знає стисла природнича наука. Що він є так високий, є зовсїм зрозуміле, коли зважимо, як далеко сягає того рода явище в атомістичну дрібноту своєї механїчної ґенези. Зінтерпретувати чисельну вартість сього сочинника — се на мій погляд — найвдячнїйша перспектива сьогочасної епохи, майже найдальша ціль всякої матеріяльної кінетики.

Коли я відважую ся висказати отсих кілька думок, то роблю се не для висуненя якогось субєктивного погляду, який не мав би значіня, але з огляду на методичні трудности, з якими боре ся і довго ще імовірно буде бороти ся математична аналїза кінетичної теориї, схоплена нинї під видом скомплїкованих, „найправдоподібнїйших“ констеляций всїляких молекулярних роїв материї. Я в переконаний, що аналїтичний рахунок дістане колись знамените „оперте“ в чисельній вартости кождого, доцїльно вибраного, „стеричного“ експерименту, однак під услівєм, що таких „даних“ назбирає ся більше, що з них виробить ся який такий „систем“.

До такого погляду осьміляє мене сконстатоване одної, про око може зовсїм незначної і припадкової появи, що дає ся замітити на сочиннику температури скорости кількох (зовсїм ріжних типів) амінових перемін.

Маємо до діла з трома парами хем. реакций, а то:

1.[1]) а) піридина + $C_2 H_5 J$
б) колїдина + $C_2 H_5 J$

2.[2]) а) пararозанїлїна + $Na O H$
б) кристальвіолет + $Na O H$

3.[3]) а) б-хльорбутильамін ⟶ пирролїдиновий хльорогидрат
б) гидрохльорбутальлїльметилькарбінамін ⟶ ⟶ $\alpha\alpha$, — двометильопирролїдиновий хльорогидрат.

В отсих трох парах хемічних перемін находять ся в безпосереднім сусїдстві атому N в припадках 1 а), 2 а), 3 а) два атоми H, нато-

[1]) I. Hirniak Beiträge zur chem. Kinetik. I. 1911. S. 67.
[2]) Hantzsch u. W. I Müller. Ber. d. deutsch. chem. Ges. 43, 2609—13.
[3]) H. Freundlich u A. Krestovnikoff. Zeitschr. f. phys. Chemie 76, 94
H Freundlich u. Marion B. Richards. „ „ „ „ 79, 695.

мість в припадках 1 б), 2 б), 3 б) оба місця атомів H є заступлені ґрупами CH_3. У всіх трох парах реакцій проявляє ся в однаковім змислї стеричний вплив CH_3 обменшенєм сочинника скорости переміни і підвисшенєм вартости сочинника температури сеї скорости. Тим самим був би сповнений загальний постулят стеричної кінетики на сих процесах і т. зв. правило антибазиї між обома згаданими хемічними характеристиками. З того погляду всї три пари перемін є інтересні і пригожі для сих постулятів, (нинї вони не рідко ще заводять), з другої однак сторони нїкому не може сьогодня прийти навіть на думку шукати якихнебудь правильностий в обменшуваню скорости перемін при зіставленях 1 а) — 1 б), 2 а) — 2 б), 3 а) — 3 б), бо тут маємо до дїла з перемінами, які належать до зовсїм ріжних типів і відбувають ся в зовсїм ріжних услівях. Тим однак інтереснїйшим повинен бути факт, що в сочинниках температури находимо майже ідентичні чисельні ріжниці, а то:

в) 1 б) і 1 а)	0·74
„ 2 б) і 2 а)	0·77
„ 3 б) і 3 а)	0·80

В моїй згаданій публїкациї я займив становиско, що стерична кінетика мусить оперти ся на сочиннику температури, а не на сочиннику скорости із богато инших, так теоретичних як і методичних причин. Саме сї мотиви повинні скріпити переконанє, що наведені тут цифри не мають припадкового значіня. Під хвилю я занятий зібранєм ще дальших двох-трох пар-амінових перемін, в яких будуть впроваджені по дві метилеві ґрупи (CH_3) в стеричну ґру, однак на основі того, що тут констатую, я очікую з гори ріжниць, що будуть хитати ся коло 0·77. Коли се ствердить ся, що є зовсїм імовірне, можна буде висказати в загальнїйшій формі погляд, що сочинник температури скоростий хемічних процесів стане першим методичним етапом квантитативної стеричної динаміки. Вже тепер пр. я відважу ся пояснити, чому с. т. (сочинник температури) переміни, обробленої Н. Меншуткином[1]), а то:

$$NH_3 + CH_3Br = (CH_3)NH_2 \cdot HBr$$

видав так малу вартість (1·32 між 50° — 100° C). На стор. 62. моєї публїкациї є поданий с. т. для двометильо-пара-толюїдини: 2·24. Стеричне значінє мають для с. т. лише оба метилї, злучені з атомом N. (Гл. подібні обставини l. c. при коллїдинї).

Гіпотетично можна заложити, що для монометильоанїлїни випаде с. т. менший о 0·35, для анїлїни (або пара-толюїдини) менший

[1]) Zeitschr. f. phys. Ch. 17, 193, 1895.

о дальшу вартість 0·35, або разом о 0·70, т. зн. він повинен би мати вартість 1·54. Коли тепер відтягнемо від сего числа дальших 2 до 3 десятні, припадаючі на стеричний вплив бензильової ґрупи C_6H_5, дістанемо дійсно незвичайно малий с. т. (дуже незначно висший від 1) для амоняку, згідно з тим, що експериментально ствердив l. c. Н. Меншуткин.

Хоч як ще далекі від стислости є того рода оцїнки, не можна би їм однак відказувати всякої вартости. Я зазначу лише, що на основі стеричних чисел для C_6H_5 (від 0·3 до 0·5) і для CH_3 (кругло 0·35) можна гіпотетично комбінувати, які вартости с. т. припадуть на неодні ще хемічні процеси, що належуть до ріжних типів.

В змислї повисших виводів насувала би ся для сьогочасної хемічної кінетики дуже важна задача, усталити стеричні числа для ріжних ґруп, більших від CH_3. Вони не конче і не все мають випасти висші від 0·35. Залежить се від способу, як вони ґеометрично розгалузують ся від хемічного центрум. Етиль (C_2H_5) виявив в моїм дослїді такий вплив, що так скорість процесу, як і її с. т. випали менші (в порівнаню з відповідними вартостями при метилю CH_3). На сім випадку бачимо, що хоч скорість процесу обменшує ся (немов під впливом ґеометрично більшого етилю), то однак вартість с. т., також менша була би виразом чогось противного і то аж до того степеня, що тут звихає ся релятивна антибазия між с. т. а с. р. (скоростию реакциї).

Сочинник температури мусить очивидно бути менше вразливий на фізикальні впливи того рода, як ассоциация молекулів, степень їх взаїмного, а свобідного сконфіґурованя в данім обємі, ротацийна рухливість і инші ще моменти так важні і рішаючі при вартости с. р. Нема сумнїву, що ціла їх низка становить отсе все, що ми могли би собі представити і унагляднити під видом „фізичних“ каталїзаторів. Сочинник температури має однак сю методичну висшість над с. р., що він є менше від них залежний, вже із свого понятя і дефініциї, а по друге тому, що йому припадає ширший екстраполяцийний обсяг реального проявленя ся і вдержаня ся в виді стеричних правильностий в тих пересічних умовах температури, з якими ми маємо до дїла. Проф. J. v. Braun зволив звернути мені увагу на се, що часто появляє ся менший стеричний опір при етилевих громадах, ніж при метилевих. Ся річ гармонізувала би з моїми повисшими спостереженями саме тодї, як опремо ся на змислї того, що висказує с. т. (анормальний з огляду на релятивну антибазию). Були би дуже інтересні дослїди над с. т. тих реакций, які мав на

думцї проф. Braun, о скілько іменно в них анормальна релятивна антибазия (в зіставленях „метилевих“ і „стилевих“) мала би місце. О скілько мої погляди є вірні, там антибазия випала би зовсім нормально, під услівєм, що всї експериментальні умови для порівнаня були би задержані.

Про око, скомпліковані дещо відношеня, дали би ся легко проглянути на ґрафічнім рисунку. Сорядна x нехай означає температуру, y скорість реакциї. Порівнувати з собою ізотермічні точки y_a, y_b, y_c . . . і т. д., значить наражувати ся на витяганє консеквенцій, які о кількадесять або лише о кільканайцять степенїв вище (або низше), залежно від полоєженя точки пересїчи кількох функций $y = f_a(x)$, $y = f_b(x)$, $y = f_c(x)$ і т. д., можуть давати зовсім противні висліди. Натомість ріжничкові квоти $\frac{dy_a}{dx}$, $\frac{dy_b}{dx}$, $\frac{dy_c}{dx}$ і т. д. викажуть в тих самих услівях, в своїх обсягах вартостий, далеко простїйший, і кваліт*а*тивно одноцїльнїйший образ стеричних відношень. Поодинокі стеричні громади (CH_3, C_2H_5, . . . C_nH_{2n+1}, і ин.) треба би тимсамим характеризувати відповідаючими їм квотами $\frac{dy}{dx}$, т. є. сочинниками температури. Практично тому, що в ріжничковій формі підлягали би вони теоремови додаваня (Гл. перехід: піридина, α-піколїна, коллїдина). Теоретично тому, що в ріжничковій формі представляють вони відвернений образ релятивних правдоподібностий або шанс поодиноких хемічних перемін (Гл. l. c. стор. 93). З такої теоретичної точки погляду стають нам зрозумілі незвичайно інтересні висліди праць проф. A. Skrabal'a, в яких він порівнує сочинники температури з кальоричними ефектами реакций[1]) і з повним успіхом інтерполює одні вартости при помочи других.

Отсе моє розуміня ролї кальоричного ефекту не колїдує з висказом на стор. 91 моєї згаданої праці. Однак сам ефект треба ще близше механїстично з'інтерпретувати, що однак вимагає більше місця і що задумую висьвітлити в найблизшій окремій публїкациї. Проти мого згаданого висказу застеріг ся до певної міри H. v. Halban (листовно). Однак його мотиви йдуть в иншім напрямі, а експериментальна праця, котру він відтак оголосив, не противорічить моїм виводам, що пізнїйше близше розгляну.

В звязи з повисшими поглядами стояло би також питанє, що відносить ся до ряду тавтомерних реакций. Питанє се має свою питоменну характеристику. До тепер не мало воно нїякого практичного значіня, замітна однак річ, що і для теоретичного погляду представляє ся воно, здає ся менї, навіть загалови кінетиків зовсім рівнодушне. Не є виключене, що такий стан справи спричинив по части висказ W. Ostwald'a, який определїлив се питанє в слїдуючий спосіб:

„Незалежно від того, чи тавтомерна реакция є intra- чи intermолекулярна (вийде на те саме: моно- чи полї-молекулярна), всї феноменні наслїдки лишуть ся в першім і другім випадку все одні і ті самі“.

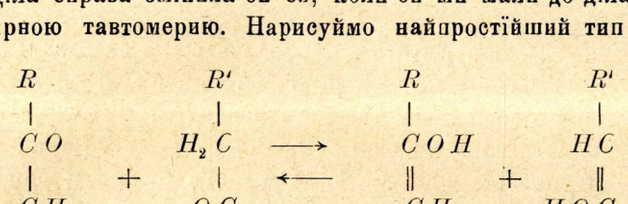
Супроти того, для практика се питанє стало би безпредметове, для теоретика неможливе до принціпіяльного рішеня, бо годї найти експериментальну критериєю для його порішеня. Тимсамим питанє се являє ся до сьогодня на скрізь ірраціональним чи трансцендентальним. Популярність поглядів W. Ostwald'a була так широка, що деякі з них розходили ся далеко навіть поза круги хеміків. Пр. славний американьский фільозоф W. James послужив ся в однім місци випадками тавтомерних перемін (в сїм власне осьвітленю, поданім W. Ostwald'ом) як одним з типових аргументів в своїм праґматичнім розумованю на обставину, що в природї стрічають ся ріжні механїзми появ, які в феноменних наслїдках лишають ся однакові.

Що правда, поки що лише в формі теоретичного здогаду, можна би тепер не так розуміти механїзм і феноменність тавтомерних перемін, як се тут зіставлено. На основі моїх поглядів дала би ся предвидїти дуже проста метода експериментального порішеня, як властиво стоїть справа з моно- чи полї-молекулярностю тавтомерних реакций в поодиноких випадках. Чисельна вартість сочинника температури має зовсїм инше жерело, коли ходить раз про дїйсно intra молекулярні, другий раз про вище молекулярні процеси. В припадках, що належуть до першого типу, жерелом є пересїчний статистичний момент атомових осциляций в нутрі молекулярної структури, представлений на вні в видї мексуелївского розкладу, момент, незвичайно вразливий на зміни температури (що стоїть в знаменнику експоненцияльної функциї). Можна би собі представити, що маючи до порівнаня кілька випадків тавтомериї, однак таких, що вони належали би до того самого хемічного типу, а ріжнили би ся лише кількома невтральними громадами в сусїдстві осцилюючого атому — що момент сеї осциляциї не богато змінить ся в переході від одного випадку до другого. Якнебудь могли би тут увійти в гру впливи сусїдних громад, на перший погляд тяжкі до схопленя, то однак проблєм був би сам про себе зовсім конкретний, хоч субтельний, а справа „власних осциляций“ атомів чи відокремлених громад

[1]) Гл. Monatshefte für Chemie pp. 1911 і 1912.

є нині в инших областях фізикальної хемії достаточно розвинена. Заложім (що найперше методично насуває ся), що дають ся подумати численні випадки, в котрих сей вплив не входив би в гру. Тодї однак вартість сочинника температури не змінила би ся від одного до другого порівнаного випадку, як що реакция буде дїйсно, в цїлім слово значіню мономолекулярна.

Цїла справа змінила би ся, коли би ми мали до дїла з між-молекулярною тавтомерию. Нарисуймо найпростїйший тип перемінн:



В зіставленю вількох випадків того самого типу можна собі подумати громади R і R' так постепенно вибрані, що їх стеричний вплив мусїв би бути щораз висший з огляду на їх положенє супроти хемічного центрум H, $O=$, або OH і H_2. Коли би однак в такім зіставленю оказав ся сочинник температури постепенно ріжний, в однозначнім змислї, в гармонїї з правилом антибазиї, тодї можна би з відповідною осторожностю проголосити процес як дїйсно бімолекулярний.

Тавтомерним перемінам треба би присьвятити увагу ще з иншого становиска. Треба іменно за H. v. Halban'ом сконстатувати, що вони одинокі не підходять під схему розумовань van't Hoff'a, в його загальнім розгляді вартости сочинника температури скоростий хемічних реакций (Vorlesungen I.). Ся обставина є також не маловажна, коли зважимо, що стремлїня модерних теорий про хемічну рівновагу, а навіть кінетику (гл. цїла теория M. Trautz'a) основують ся виключно на термодинамічних розумованях.

У відповідних місцях моєї згаданої працї я вказував на конечне узгляднене чисто кінетичних і стеричних представлень, що правда, поки що лише для хемічної кінетики, а не для рівноваги. Однак і ся послїдна область є безпосередно звязана з кінетикою. Дорога до сего не була би сьогодня непроглядна, тим більше, що хемічна статика повинна би й методично випливати з кінетики, а не противно. Відкладаючи сю річ до пізнїйшого розглянення, звер-

нім ся до кінетики тавтомерних перемін і даймо тут місце кільком влучним висказам H. v. Halban'ови (l. c. стор. 173):

„...Die Frage, wann die Arrheniussche und wann die Berthelotsche Formel voraussichtlich gelten wird, ist nie diskutiert worden. Berücksichtigt man, dass von zwei Gegenreaktionen, welche zu einem Gleichgewicht führen, die endotherme das grössere A haben muss, weil die Differenz der beiden A — Werte der Wärmetönung der Reaktion proportional ist, so kommt man zu dem Schluss, dass endotherme Reaktionen eher der Arrheniusschen Formel folgen werden, als exotherme, da ein etwa vorhandenes kleines B in der oben zitierten van't Hoffschen Gleichung neben einem grossen $\frac{A}{T^2}$ eher zu vernachlässigen sein wird als neben dem kleinern der exothermen Reaktion. Die Frage nach dem Einfluss der Temperatur auf umkehrbare Reaktionen ist aber noch wenig untersucht. van't Hoff (Vorlesungen I, 230) weist darauf hin, dass man B als den Ausdruck des rein kinetischen Temperatureinflusses ansehen könne, während das Glied $\frac{A}{T^2}$ mit der Gleichgewichtsverschiebung zusammenhängt.

Es könnte dies so geschehen, dass für die exotherme Reaktion $A = 0$ ist. Diese würde also der Formel von Berthelot folgen. Es lässt sich aber leicht zeigen, dass dann entweder die exotherme Reaktion eine abnorm kleine Temperaturabhängigkeit haben muss, oder die endotherme Gegenreaktion weder der Arrheniusschen, noch der Berthelotschen Formel innerhalb der Versuchsfehler folgen kann, sondern nur der vollständigen Formel von van't Hoff. Man erhält nämlich aus der van't Hoffschen Formel

$$\log \frac{K_{T+10}}{K_T} = \frac{10\,A}{T(T+10)} + 10\,B;$$

wäre nun für die exotherme Reaktion

$$A = 0, \text{ also } \log \frac{K_{T+10}}{K_T} = 10\,B.$$

Nehmen wir $T(T+10) = 10^5$, d. h. also t zwischen 40 und 50°, dann erhält man für die endotherme Reaktion

$$\log \frac{K_{T+10}}{K_T} = \frac{A}{10^4} + 10\,B.$$

Damit das mit der Arrheniusschen Formel innerhalb der Versuchsfehler zusammenfällt, muss $10^5 B$ neben A zu vernachlässigen sein. Die grössten bekannten Werte von A liegen aber unter 8.000, B müsste also neben 0·08 zu vernachlässigen sein. Für $K_{T+10}/K_T = 3$ ergibt sich aber bereits $B = 0{\cdot}03$.

Die grosse Zahl von Reaktionen, welche der Arrheniusschen Formel folgen, deren Gegenreaktionen also nicht der Berthelotschen Formel folgen können, macht es also unwahrscheinlich, das letztere häufig gilt, und weist darauf hin, dass B meist sehr klein ist.

Gegen die Verteilung der beiden Temperatureinflüsse, des gleichgewichtsverschiebenden und des kinetischen, auf die beiden Konstanten der van't Hoffschen Formel lassen sich indessen schwerwiegende Bedenken geltend machen. Es müsste nach dieser Ausschauung ein wesentlicher Unterschied in den Temperaturabhängigkeit zwischen solchen Reaktionen, welche mit beträchlicher Wärmetönung verlaufen[1]) (в замітці[1]): van't Hoff, Vorlesungen I, S. 228: „...und dass demnach das Temperaturgesetz sich voraussichtlich bei Reaktionen, die nicht von Wärmetönung begleitet sind, am einfachsten herausstellen wird, die gegenseitige Verwandlung optischer Isomeren, . . . wäre in dieser Beziehung ein Idealfall."), und solchen bestehen, bei welchen dies nicht der Fall ist. Die Erfahrung seigt jedoch das Gegenteil. Dimroth hat gezeigt, dass das Gleichgewicht der von ihm untersuchten tautomeren Verbindungen praktisch unabhängig von der Temperatur ist und doch folgen diese Reaktionen der Arrheniusschein Formel, und die Konstante A ist sehr gross. Die Konstante B, welche nach der oben erwähnten Anschauung den kinetischen Einfluss der Temperatur wiedergeben soll, ist also hier zu vernachlässigen, die Temperaturabhängigkeit selbst aber sehr gross, und da das Gleichgewicht von der Temperatur nicht beeinflusst wird, kann diese Temperaturabhängigkeit nur kinetischer Natur sein".

Передовсім мушу тут піднести, що H. v. Halban пораз перший і дуже влучно схарактеризував суперечність, яка скривала ся досі в поглядах на сю річ, сконструованих не меншим між дослідниками, як сам van't Hoff. Після мене, суперечність дає ся однак ухилити, при помочи дуже простої інтерпретації, поки що, на пів теоретичної, на пів емпіричної.

Теоретичну вартість має перший член рівнання:

$$\log k = -\frac{A}{T} + B\,T + C$$

Форма сего члена $\left(-\frac{A}{T}\right)$ випливає з теоретичних заложень H. Goldschmidt'a[1]) і F. Krüger'a[2]), основаних на фундаментальних рівнанях Boltzmann'a, Maxwell'a и. ин., відносно розкладу скоростий молекулів і атомів в газах.

[1]) Inaugural-Dissertation (Breslau) 1907.

[2]) „Zur kinetik.. usw.", Göttinger Nachrichten 1903.

Сї заложеня се незвичайно щаслива інновация для хемічної кінетики, абстрагуючи від того, в який спосіб оба згадані автори її перевели. Сї заложеня становлять, що правда, лише оден, а однак принціпіяльно важний фраґмент, що дотикає незвичайно скомплікованого механїзму хемічних перемін. Він розяснює відразу гіпотезу „активних" молекулів Arrhenius'a, антибазию між с. т. а скоростию процесу, обменшуване с. т. враз із підвищенем температури, але, що на мій погляд є особливо важне, що дає можність відвернути (злишну) увагу кінетиків від понятя кальоричного ефекту, вкорінену чи не за сильно в основи розуміня кінетичних явищ (без огляду на проби проф. A. Skrabal'a, що мають подекуди практичне значіне).

Коли тавтомерні реакциї будемо уважати за ваключно intra- або моно-молекулярні, тодї в формулї:

$$\log k = -\frac{A}{T} + B\,T + C$$

належить просто відвернути пояснене або інтерпретацию (подану van't Hoff'ом) членів $-\frac{A}{T}$ і $B\,T$. В сїм змислї, в якім я се роблю для всїх хемічних реакций (стор. 90 l. c.), член $-\frac{A}{T}$ є чисто „кінетичний", член $B\,T + C$ найправдоподібнїйше чисто „стеричний", а „термодинамічного" просто нема тут зовсїм.

О скілько тавтомерні переміни є на скрізь intra- молекулярні, цїла висока вартість їх сочинника температури має своє „кінетичне" жерело виключно в членї $-\frac{A}{T}$, стеричні впливи членів $B\,T + C$ не входили би тут зовсїм до гри. Тим самим формула Arrhenius'a була би вдержана, однак з тим, що в членї $-\frac{A}{T}$ треба би дошукувати ся не термодинамічних, а лише чисто кінетичних впливів. „Дволичність" інтерпретациї членів:

$$-\frac{A}{T} + B\,T + C$$

зводила би ся тимсамим, о скілько ходить о „чисту" хемічну кінетику[1]), до того, що цїла їх інтерпретация повинна би бути чисто кінетична, а не термодинамічна. Тодї однак і цїла суперечність, про яку так влучно говорить H. v. Halban, розвязала би ся сама від себе.

Наконець докину ще кілька слів до обставини, що праці проф. H. Freundlich'a (гл. висше l. c.) позвалають мені повести трохи

[1]) Гл. стор. 91 отсеї розвідки.

дальше клясифікацию хемічних процесів. Оба приміри, котрі він вичерпуючо трактує:

б- хльорбутильамін ⟶ пирролїдиновий хльорогидрат
гидрохльорбуталлїльметилькарбінамін ⟶
⟶ *a a*, — двометильопирролїдиновий хльорогидрат,

становлять припадково незвичайно щасливо вибрані появи, що реакция, після дотеперішних поглядів на скрізь моно- молекулярна, може і повинна бути представлена як бімолекулярна, з огляду на два хемічні центра, що злучують ся взаїмно з собою в осередку одного і того самого молекула. Є се дійсно незвичайно інтересні припадки, коли ходить про механїзм хемічних перемін. В них мусить іменно проявити ся стеричний вплив сусїдних громад (обох метилїв). Його досліди потверджують не лише кваліїтативно, але й квантитативно се, що я знайшов дотично приросту сочинника температури в переходї від піридини до коллїдини, що також квантитативно виявило ся на працях Hantzsch'a і Müller'a (l. c.) на молекулах високо зложених, а притім процесах, що належуть до зовсїм иншого типу. В виду того я можу мою клясифікацию хемічних процесів після хемічних центрів дальше розширити, і розвинути поняте перемін моно-, бі-, і полї- центральних, без огляду на се, чи реакциї є, відносно до кінетичних „ріжничкових рівнань" моно-, чи полї- молекулярні. Однак близше обговорене отсеї, для мене незвичайно пригожої обставини, мушу зі всїми застереженями відложити на пізнїйше, тим більше, що як раз тепер підняв я дальше оброблене сеї справи і з експериментального боку. Закінчу лише сим, що й інтерпретация т. зв. „реґули Halban¸a" стає для мене тимсамим подекуди лекшою до переведеня в деяких точках, які дотепер становили менї частинну трудність чи довільність в її поясненю.

Breslau, в падолистї 1913.

Причинки до ґеоґрафічної термінольоґії. I.

Написав *Др. Стефан Рудницький.*

Вступ.

Отсї стрічки суть першим доповненем мого „Начерку ґеоґрафічної термінольоґії“[1]). Се доповнене мабуть не останне, томуто й я сзначив його порядковим числом. Воно подиктоване подібно як і „Начерк“ чисто практичними потребами. При кінци першого десятьлїтя XX-го віку розширилась фізіоґрафічна система Уілема Морріса Девіса по всїй европейській ґеоґрафічній науці, так сильно і скоро, що прямо годї найти в цїлій історії нашої науки аналоґічно швидкого розросту якоїсь ідеї. Коли в 1908 році я вважав відповідним подати лиш деякі найважнїйші терміни з дуже гарної виразні ґенїяльного Американця, то нинї бачу необхідну конечність присвоїти всю термінольоґію Девіса українській мові. Я дуже далекий від безкритичного захвату над системою Девіса, однак вважаю єї дуже поважним кроком наперед у розвитку морфольоґії і признаю їй дуже визначну дидактичну вартість. Коли нинї найвизначнїйші представники ґеоґрафічної науки на найперших сьвітових катедрах займають ся докладним перероблюванем та інтерпретацією девісівської системи, то думаю не від річи буде дати й нашим адептам ґеоґрафії спромогу покористуватись сею системою і єї термінольоґією.

Нинїшні „Причинки“ обіймають отже передівсїм цїлу термінольоґію Девіса, т. б. о скілько вона не була узгляднена в „Начерку“. Крім сего помістив я ту деякі слова, що з ріжних причин були

[1]) Збірник математично-природописної секції Наукового Товариства ім. Шевченка, т. XII. ст. 1—151.

в „Начерку“ пропущені. І тепер я старав ся як найменче слів ковати, впрочім термінольоґія Девіса така легка і прозора, що кованнии майже не вимагала. „Причинки“ суть таксамо як „Начерк“ словарцем нїмецько-українським, лиш деякі питомі Девісу терміни подав я також в прямім переводї з анґлїйського.

На сїм мігбим і закінчити отсе моє передне слівце. Однак при термінольоґічній роботї насували ся менї від давна і з великою упертістю постійно насувають ся ріжні питаня, дотичні нашої наукової термінольоґії і мови в загалї. Хотївбим нинї їх бодай поставити, бож їх розвязанє не лежить в моїх руках. Некомпетентні до розвязки сих питань навіть українські язикослови, хибань що малиби рівночасно вповнї всесторонне, всї науки без виємку обіймаюче, образованє. А в наших часах така унїверсальність абсолютно неможлива. Справа нашої наукової мови й термінольоґії може рішитись тільки спільною працею загального зїзду українських ученых, який вибрав би постійну комісію, постанов котрої мусїв би придержуватись всякий Українець, що хотївби науково працювати в українській мові.

Чому я прийшов до таких радикальних висновків, поясню зараз, хоч тільки кількома словами. Зачну від термінольоґії. Завдяки матеріялам, зібраним дд. І. Верхратським, В. Левицьким, І. Горбачевським і иншими, маємо вже українську термінольоґію майже для всїх природних наук. Так щож з того? Термінольоґія ся є обмежена на невеличкий кружок наукових робітників, що гуртуєть ся довкола математично-природописної секції Наукового Товариства ім. Шевченка, крім сегож лиш на галицькі шкільні підручники (і то не на всї). Поза тим обсягом майже нїхто не узгляднює зібраних дотепер термінольоґічних матеріялів і то на жаль нетільки в популярно-наукових книжках але й в наукових виданях (пр. українського наукового Товариства в Київі). Натомість кождий автор, не жалуючи свого часу, сам творить собі термінольоґію, дуже часто навіть дивовижну, бо похопність до кованя нових слів у кождого пишучого Українця дуже велика. Щастє, що наша природописна наукова та популярно-наукова продукція ще така скупенька, а то невдовзї малиби ми безлїч термінольоґій. А одної лише потреба.

Такий стан для нашої молодої науки дуже а дуже непожаданий. Бо до безлїчи причин, що спинюють єї розвиток, прилучилаби ся отсим ще одна, дуже поважна.

А усунене термінольоґічного безголовя преціньтаки в наших, українських руках. Вище вказаний спосіб: загального зїзду вчених,

постійної комісії та виданих нею постанов у виді загального термінольоґічного словаря є одинокий. Бо на скільки знаю, видані дотепер термінольоґічні матеріяли, хоч нїгде з поважного місця не виказано їх безвартности, таки серед читаючої і пишучої публики не мають популярности й зустрічають ся з неприхильною критикою. По тім боцї кордону вважають їх „галичанщиною“ і тим одним словом престіж їх убитий на 9/10-их простору нашої країни, по сїм боцї кордону тамошний неприхильний осуд має теж богато значіня, крім сегож і в межах Австрії ще далеко не перевелись ті давні часи, колито кождий інтелїґентний Українець уважав себе компетентним в язикових справах. Такі обставини мусять спричинювати такий стан, який нинї маємо в термінольоґічнім питаню. Колижби термінольоґічні матеріяли були найповажнїйшим науковим збором передискутовані, справлені й усталені, тоді за прийнятою виразнею стоявби так сильний авторітет, що не хтобудь важивби ся проти него виступати і перемінювати працю термінольоґічних чорноробів у Сізифовий труд.

Вкінци ще дещо про нашу наукову мову в загалї. Ту справа стоїть без порівнаня лїпше, бо вся наша лїтературна мова опираєть ся на казочно богатій простонародній мові. На так широкій і богатій основі легко було побудувати систему нашої наукової мови. Але се зроблено дотепер лиш на поли історії та історії лїтератури, де маємо до дїла з категоріями предметів і відносин, які можна легко представити простим оповіданєм. Навіть аналїза на сих полях науки не спричинює нїяких трудностий у вислові чи стилїзації. Якже инакше стоїть справа в фільософії чи в природописних науках! Ту на кождім кроцї леґіонами повстають трудности, що хвиля виринає конечність так остро заказуваної нашими язикословами субординації речень, уживаня дїєприкметників ітд. ітд. В популярно-природописних статях можна ще сяк так обійти ся без тих заказаних овочів. Але в стисло науковій прозї се річ немислима. Замотані квестії стислих наук, представлені такою мовою, якої домагають ся тепер наші язикослови, стають ще більше замотаними, ба незрозумілими. Найлїпше се видно по переводах наукових чи навіть популярно-наукових творів на нашу мову. Вони майже без виїмку такі, що в богатьох випадках я мусїв дуже часто заглядати до оріґіналу, щоби зрозуміти перевід. А оріґінальні чистонаукові працї українських природописців мають як найгіршу славу: в них мовляв стиль страшний, мова неможлива, спосіб представленя темний і замотаний.

Чиж ту вина авторів та перекладачів? Зовсїм нї! Вина лежить в занадто одностороннім виробленю нашої наукової мови. Вона вже

вповні може вдоволити істориків чи фільольоґів — натомість природописці мусять страшно бідувати і рішучо домагати ся від язикословів, щоби помогли їм у всестороннім виробленю української наукової мови. Се справа першорядної ваги. На мій погляд стратилисьмо, головнож на россійській Україні, неоден десяток Українців природописців, що не бачучи змоги працювати науково в українській мові, пішли на службу чужій науці.

Сих кілька висловів я вважав потрібним подати на вступі сеї частини „Причинків". Може бути, що зможу в иншім місци розвести сї питаня. Се не критика наших фільольоґів, бож я не маю до сего нїяких квалїфікацій, се прямо кликанє помочи для цїлої так важної царини людського знаня, як є природописні науки.

A.

Abböschung	злагіднене (склону)
Ablenkung	відклоненє, відклін
Ablenkungsknie	колїно відклону
Abrasionsebene	абразійна рівня
Abrasionsterrasse	абразійна тераса
Abstumpfung	притупленє
Abtragungsebene	денудаційна, знесена рівня, пенеплєна
accident	перешкода, заколот
accordant jonction	рівнодонне устє
aggrade (to)	насипуванє
Altland	старосуша, материк
Amphitheater	амфітеатер, цирк, кар, ледняковий котел
Angliederungsinsel	прилученний острів
Antezedenz	антецеденція, упередність
Anzapfung	надточенє, надрізанє
arid	сухий, посушний, пустинний
attitude	лежба
Auflösung (des Flußsystems)	розвязанє
Aufpfropfung	нащіпленє
Aufschluß	вихідня, відкривка, відслоненє
Aufschüttungsterrasse	насипова тераса
auftauchen	вирінати
Aufwölbung	видвигненє, висклепленє
Ausgangsform	вихідна, основна форма
Ausgestaltung	виобразованє
Ausgleichung	вирівнанє
Aushöhlung	видовбанє
Auslieger	відшибок, (сьвідок)

B.

Bad-Lands	рипища
barrier beach	коса
baselevel of erosion	ерозійна основа
bay head	головище (заливу)
beach	бережина
beheaded	стятий, полонений
Becken arides	пустинна, посушна заглубина
Becken zerschnittenes	порізана, розтята заглубина
Beckenablagerung	заглубинне відложенє
Bergland unterjochtes	підяремна, підчинена верховина
Bergsporn	гірський причілок
Beschleunigung	прискоренє
bestimmt konsequent	визначно консеквентний
Binnenebene	внутрішна рівня
Blockdiagramm	блъоковий діяґрам
Boden gewachsener	вросла почва
Bodenbewegung	рух почви
Bolson	бользон
bowlder	пень, брус
branche	притока
Brandungshöhle	погійна нора
Brandungshohlkehle	погійний підрив, вруб
Brandungskehle	погійне горло
Brandungslinie	погійна лїнія
Brecher	бовван
Bruchlinienstufe	лімнолїнійний ступень, поріг
Bruchliniental	лімнолїнійна долина
Buckel	горб
Buhne	кашиця
butte	острощовб

C.

Caliche	калїче
capture	полонене
chasm	щілина

cliff	клїф, обрив, стрім
cliff-maker	стромотворець
coastal plain	побережна рівня
cove	погійний залив
creeping (of soil)	сповз
crest	гребінь, хребет
crooked	закручений, повигинаний
cuesta	куеста, поріг
cuesta-maker, Cuestabildner	пороготворець
Cuestabrücke	куестовий міст
cut off	меандровий пролім

D.

degrade to	зносити, обнижати
Delta rückläufiges	вспятна дельта
Deltaküste	дельтове побереже
Diffluenz	розплив
diffluierend	розпливний
dike	стїна
dismembered	розвязаний (про річну систему)
dissection	розрізане, роздолинене
divide	вододїл
domed mountains	щовбисті, копулисті гори
drainage	водяна сїть

E.

Ebene blossgelegte	обнажена рівня
Ebene fluviatile	річна рівня
Ebene zerschnittene	розтята рівня
eddy	вир, крутїж
Einbuchtung	вріз, вруб
Einebnung	вирівнане
Einebnungsfläche	вирівняна верхня
Einführung	введене (цикля)
Einschneiden	врізуване, поглублюване
Eiserosion	ледова ерозія
Eisfuß	ледова обнога
Eiskaskade	ледопад
Eiskliff	ледяний стрім
Eisstausee	ледовозапірне озеро

elbow of capture	колїно полонення
embayed	повирізуваний
Endform	наконечна форма
engrafted	нащіплений
enthauptet	стятий
Entwässerung zentripetale	доосередне відводнене
Entwickelungsstadium	стадія розвитку
Episode	епізод (в циклю)
Erosion normale	нормальна ерозія, правильне жолоблене
Erosion seitliche	бічна ерозія, бічне жолоблене
Erosionsbasis örtliche	місцева ерозійна основа
Erosionszyklus (arider, glazialer, mariner, normaler)	ерозійний цикль (посушний, ледняковий, морський, нормальний)
Ertrunken	затоплений (гори, долини ітд.)
Escarpment	верствовий ступень

F.

Facette	фацета, виглад
Falaise	фалєза, побережний стрім
Fallbildner	водопадотворець
Fall-linie, fall line	водопадна лїнія
fan (of waste)	сиповий вахляр
fastreif	майже спілий
fault	лім, скид
Felsebene	скельна рівня
Felsplattform	скельна платформа
Firnmulde	фірнова лотка
flat topped	рівномірно притуплений
flood plain	річна рівня
Fluß abgelenkter	відклонена ріка
Fluß alter	стара ріка
Fluß aufgepfropfter	нащіплена ріка
Fluß ausgeglichener	вирівнана ріка
Fluß beschleunigter	прискорена ріка
Fluß enthaupteter	стята, полонена ріка
Fluß epigenetischer	епігенетична, наложена ріка
Fluß insequenter	інсеквентна, ріжнопрямна ріка
Fluß intermittierender	інтермітивна, часова ріка
Fluß longitudinaler	повздовжна ріка
Fluß mäandernder	меандруюча ріка

Fluß neubelebter	новооживлена, відновлена ріка
Fluß normaler	нормальна, правильна ріка
Fluß peripherischer	періферична, окрайна ріка
Fluß reifer	спіла ріка
Fluß resequenter	ресеквентна, співпрямна ріка
Fluß subglazialer	субґляціяльна, підледникова ріка
Fluß überfähiger	надздібна ріка
Fluß unterfähiger	підздібна, менче здібна ріка
Fluß verjüngter	відмолодніла ріка
Fluß verlängerter	продовжена ріка
Flußablenkung	відклонене ріки
Flußablenkung bevorstehende	надходяче відклонене ріки
Flußablenkung lange vollzogene	давне відклонене ріки
Flußablenkung neue	новітне відклонене ріки
Flußablenkung voraussichtliche	майбутне відклонене ріки
Flußaufschüttungsebene	річна насипова рівня
Flußbelastung	обтяжене ріки
Flußentwicklung	розвиток ріки
Flußgefälle	спад ріки
Flußsystem aufgelöstes	розвязана річна система
Flußwindung	закрут, меандер
Flutdelta	приливна дельта
Folgeform	прямна, слїдна форма
Formlinie	формова лїнїя
Frane	франа
frühreif	вчасно спілий

G.

geköpft	стятий, полонений
Gekriech	сповз
Gesteinsbuckel	скельний горб
Gesteinsriegel	скельна перегорода
Gezeitendelta	временна дельта
Gezeitenmarsch	временна наплавина
Gezeitenöffnung	временна прірва
gleichsohlig	рівнодонний
Gleithang	сховзна збіч
Gletscherabzweigung	ледникове відгилене
Gletscherbach	ледниковий потік
Gletscherende	конець ледняка

Gletschersattel	леднякове сїдло
Gletschersystem	леднякова система
Gletschertrog	леднякове корито
Gletschertrogsee	леднякове озеро
Gletschertrübe	ледниковий каламут
gorge	звір, яруга, дебра, прірва
gorge de raccordement	злучна прірва
grade	вирівнане
gradient	спад
gravel	ситець, рінь
Greisenalter	старечий вік
gulley	рытвина

H.

Hangbildner	кручетворець
Hängetal, hanging valley	висяча долина
Härtling	твердяк, монаднок
Haupttrog	головне корито
headward (erosion)	вспятна (ерозія)
Hebungsform	форма двигненя
Hebungsküste	двигнене побереже
Hochgebirgsform	високогірська форма
hog-back	верствове ребро
Hohlkehle	підрив, горло
humid	вохкий

I. J.

ice sheet	ледище, ледовище
initial form	початкова форма, праформа
inlet	тоня
Insel verknüpfte	прилучений остров
insequent	інсеквентний, ріжнопрямний
integration	зроснене
interfluve	межиріче
Jagendstadium	молодеча стадія

K.

Kar divergierendes	розбіжний кар, котел
Kar convergierendes	збіжний кар, котел
Karboden	дно кару, кітла

Karwand	стіна кару, кітла
Kliffreihe	клїфовий, обривний ряд, стрім
Kliffrutschung	клїфовий сповз
Kliffsturz	клїфовий сув
Klippe aufgefrischte	відсьвіжена рипа
Klippe verschwindende	зникаюча рипа
Kluse	клюза, прірва
konsequent	консеквентний, прямний
Korrelation	корреляція
Kümmerfluß	збіднїла, злиденна ріка
Kuppelgebirge	копулисті гори
Küste heranreifende	доспіваюче побереже
Küste vereinfachte junge	упрощене молоде побереже
Küste zerrissene	роздерте побереже
Küstenart	рід побережа
Küstenform	форма побережа
Küstenebene lakustre	озїрна побережна рівня
Küstenebene untergetauchte	затоплена побережна рівня
Küstenebene verwickelte	замотана побережна рівня
Küstenebene zonar gegliederte	полосато розчленена побережна рівня
Küstenplattform	побережна платформа
Küstenstreifen	побережна смуга

L.

Landform	форма поземеля, терену
landslide	сув, сповз
landtied island	прилучений остров
Lavadecke	крига ляви
Lavaebene	лявова рівня
Lido	коса
load	синовий тягар
lobus	льоб, язик (меандра)
lofty mountains	високі, альпейські гори

M.

Mäander eingesenkter	поглублений меандер
Mäander freier	свобідний, мандрівний меандер
Mäanderdurchbruch	меандровий пролім
Marsch	марш, наплавина
meander belt	меандрова смуга

Meereshalde	морський насип
Mesa	меза, столище
migration of divides	переміщене вододїлів
misfit river	збіднїла, злиденна ріна
Mittelgebirgsform	середногірська форма
monadnock	монаднок, твердяк
mosor	мозор
Mündung gleichsohlige	рівнодонне усте
Mündung ungleichsohlige	нерівнодонне усте
Musterform	взірцева форма

N.

Nebenflußmündung	усте притоки
Nebengletscher	бічний ледняк
Nebentrog	бічне коригo
Nebenwasserscheide	побічний вододїл
neck	нек, чіп
Neubelebung	оживлене, віджите
Nische	нїша, вглублене, низок
nival	снїжний
normal	нормальний, правильний

O.

Obsequent	обсеквентний, протипрямний
Oberland	горіще, верховина
Öffnung	отвір, дїра, перерва
oldland	стара суша
outcrop	відкривка, вихідня
outlet	тоня, вихід
outlier	сьвідок, сьвідкова гора
oxbow lake	охаба

P.

Pfropfenberg	нек, чіп
piedmont	обніжна рівня
Piedmontebene fluviatile	річна обніжна рівня
Piedmontzone	обніжна полоса
piracy	надточене, полонене, стяте
Plateau zerbrochenes	поломане плоскозгіре
Prallhang	ударна збіч

R.

Randlich	окрайний
Randmoräne	окрайна морена
rapids	пороги, катаракти
ravine	звір, дебра, яруга, балка
reif	спілий, доспілий, дозрілий
reif zerschnitten	спіло розчленений, розтятий
Relief (mittleres, niedriges, starkes)	релєф, різьба (середня, низька, [сильна)
resequent	ресеквентний, співпрямний
Restberg	останкова, полишена гора
Resthügel	останковий, полишений горб
revived	відживший, ново оживлений
Riedel	клин, клинець (межирічний)
Riegel	перегорода, запір, засув
rivulet	потік
rückläufig	вспятний (пр. дельта)

S.

Salzablagerung	зложище соли
Salzschichte	сільна верства
Sandinsel	пісчаний острів
Sandriff	пісчана рипа
Saugloch	понор, хлань
Schichtflut	розлив
Schichtfluterosion	розливна ерозія
Schichtlinie	верствова лїнїя, ізогипса, верствиця
Schichtrippenlandschaft	верствореброва країна
Schichtstufe	верствовий ступень
Schlipf	сув
Schrägstellung	скісне уставлене
Schulter	плече
Schuttdecke	сипова крівля
Schuttebene	сипова рівня
Schuttfächer	сиповий вахляр
Schuttlast	сиповий тягар
Schuttlinie	сипова лїнїя
Schuttschnelle	сипова бистрина
Schutttransport	сиповий транспорт
Schuttzufuhr	довіз, достава сипу
sea cliff	надморський клїф, обрив, стрім

Seeebene	озїрна рівня
Seitencañon	бічний яр
Seitental hängendes	бічна висяча долина
Seitental ungleichsohliges	бічна висяча, нерівнодонна долина
Seitentrog	бічне корито
Senkungsküste	западове побереже
sequential	прямний, слїдний
sheet flood	розлив
shifting divides	переміщенє вододїлів
sink hole	вертеп
skerries	шєри
slope	круча
slope-maker	кручетворець
spätjung	немолодий, доспіваючий
spätreif	пізноспілий, переспілий
spit	гак
Spitzkuppe	острощовб
Sporn	виступ, причілок
Spornende	кінчик
Spornrest	останок причілка
spur	виступ, причілок
Stadium, stage	стадія, стан
Staubebene	пильна рівня
Stiel	черен
Stirn	чоло (ступеня)
Störung (des Zyklus)	перепона, перешкода
Strandebene	бережинна рівня
Strandrücken	бережинний хребет
Strandvorsprung	бережинний виступ
Strecke ausgeglichene	вирівнана просторонь
Streifen freigelegter	вільна смуга
Strichdüne	смугова надма
Stromstrecke	річна просторонь
strong relief	сильний релєф, різьба
Strudeltopf	вировий глек
Struktur (deformierte, einfache, gefaltete, geneigte, horizontale, verwickelte)	структура, будова (здеформована, проста, фалдова, наклонена, позема, замотана)
Strudelströmung	вирова течія
Stufe aufgefrischte	відсьвіжений ступень
Stufenbildner	сходотворець

Stufenlehne	сходова збіч
Stufenmündung	сходове усте
Stufensporn	ступенний виступ, причілок
Sturmdelta	бурна дельта
subdivide	побічний вододіл
subdued mountains	підяремна, підчинена верховина
subkonsequent	субконсеквентний
subsequent	субсеквентний, наслідний
surf	погій
swell	відгомінна филя

T.

Talaue	долинне болоне
Taldichte	густота долин, роздолиннене
Talentwickelung	розвиток долин
Talflur	долинне болоне
Talschluß	головище долини
talus	завале, насип
Talvereinigung	злука долин
Talvertiefung	долинне вглубленє
Talwindung	закрут долини
Terrasse geschützte	захищена тераса
Terrassenstufe	терасовий ступень
Terrassenspitze	терасовий кінчик
Textur, texture	текстура, розчленене, роздолиннє
texture (of waste)	грубість (ріни, сипу)
tidal marshes	временні наплави
Tief	тоня
tilting	скісне уставленє
Treppenstufe	сходовий ступень
Trogbett	(коритове) ложбище
Trogschluß	головище корита
Trogtal	коритова долина
Trogwand	стіна корита

U.

überfähig	надздібний
Überfließgletscher	переливний ледняк
Überhöhung	перевершенє
Übertiefung	переглубленє

Überweitung	переширенє
Uferlinie	бережна лінія
Uferstreifen	бережна смуга
ultimate form	наконечна форма
Umkehrung, Umkehr (des Reliefs)	відвернене
Umlaufberg	обіжна гора
unbestimmt konsequent	неозначено, неточно консеквентний
undercut slope	ударна збіч
Unterbrechung (des Zyklus)	перерване (циклю)
unterfähig	піддібний, ледви здібний
Untertauchung	занурене
upland	горіще, верховина
uplift	двигненє, двиг
Urabdachung	прасклін
Urbach	прапотік
Urbecken	праночва
Urentwässerungsgebiet	прасточище
Urfluß	праріка
Urflußsystem	прарічна система
Urform	праформа
Urküste	прапобереже
Urküstenlinie	прапобережна лінія
Urmulde	пралоть, пралотка
Urmuldenlinie	пралоткова лінія
Uroberfläche	праповерхня
Ursee	праозеро
Ursenke	празападина
Urtiefland	праниз
Urwanne	праванна
Urwasserscheide	праводіл

V.

valleuse	валєза, висяча побережна долина
Vereinfachung	виправленє, упрощенє
Vereinigung gleichsohlige	рівнодонна злука
verjüngt	відмолоджений, відмолодніли
Verknüpfung	сполученє, прилученє (островів)
Verlängerung	продовженє
Verschleppung	перетащенє
Verwachsen	зрастанє
Verwilderung	здичінє

Verzögerung	припізнене
vollreif	повноспілий, доспілий
Vordüne	передна надма
Vorgang	процес, хід
Vorlandvergletscherung	чолове зледеніне
Vorstrand	чолова бережина
Vulkankern	черен вулькану

W.

warping	погнуте
waste	сип, груз
watergap	пролім, проломова долина
weathering	вітріне
Wellenbasis	основа филь
wet weather rill	дощева ритвина
wiederbelebt	віджившний, воскресший
Windmulde	вітрова лотка
Wüstenbecken	пустинна ночва
Wüstenebene	пустинна рівня

Z.

Zerschneidung	розрізане, розтяте, розчленене
Zertalung	роздолинене
Zeugenberg	свідкова гора
zonar gegliedert	полосато розчленений
Zungenbecken	язикова ночва
Zurückschneiden	взадне зарізуване
Zurückweichen	пячене, відступане
Zweigtrog	побічне корито
Zweikanter	двограняк
Zweizyklisch	двоциклевий

Бібліографія.

V, 9. Bachmann P., Über Gauß' zahlentheoretische Arbeiten. (Materialien für eine wissenschaftliche Biographie von Gauß, gesammelt von F. Klein und M. Brendel, I). Nachrichten der kgl. Ges. d. Wiss. zu Göttingen, math.-phys. Klasse 1911, p. 455–508.

Ґетінґенське наукове товариство, що займаєть ся виданем творів свого незабутнього члена Карла Фрідріха Ґавсса, має дати в X. томі сего видання повну научну біоґрафію того найвизначнійшого нїмецького математика XIX ст. Хто бодай поверховно займав ся творами того ґенїя, сей буде знати, що перед усїми иншими його працями треба поставити твори з теорії чисел; вони-ж дали підвалину до нинїшнього величавого розвитку сеї галузи математики. Вже сам Gauß сказав, що як математика є королевою наук, так аритметика (теорія чисел) є королевою математики. З тої саме причини як перший випуск матеріялів до біоґрафії Gauß'a появила ся праця проф. Bachmann'a про його роботи з теорії чисел; сюди належать такі твори:

Disquisitiones arithmeticae, епохальний твір Gauß'a, виданий 1801 р. в Липску, передрукований опісля як I. том його творів (вид. заходом ґетінґського наук. тов. у Teubner'a 1870 р.);

кільканацять розвідок з ріжних часів по 1801 р., друкованих в записках того-ж тов-а і виданих як II. том творів (1876), а також дещо з його спадщини.

Всї ті твори писані в латинській мові; нїмецький їх переклад зладив H. Maser, Berlin (Springer) 1890; видав п. з. „Arithmetische Untersuchungen von C. F. Gauß".

До научної біографії Gauß'а взята як субстрат його цїла письменницька спадщина, в якій містить ся богато начерків пізнїйших публїкацій, а головно записник Gauß'а, провадженый точно від р. 1796 до 1814. (Сей записник передрукований в записках ґетінґенського тов-а з 1901 р. і в 57 т. „Mathematische Annalen“).

Disquisitiones появили ся лїтом 1801 р.; тим проблємом займав ся Gauß від 1795 р. Одначе можна здогадувати ся, що він вже давнїйше нераз ломив собі голову над деякими трудними питанями теорії чисел. Найдавнїйшим його занятем (від 15. року житя) було укладане числових таблиць, які служили йому опісля емпіричним матеріялом для дедукованя загальних законів. Деякі з тих законів попали йому — що так скажемо — припадково під руку.

В перших роках твореня Disq. Gauß не був зовсїм обізнаний з творами своїх попередників на полї теорії чисел; але вже 1796 р. знав добре працї Euler'а, Lagrange'а і Legendre'а і переконав ся, що його висліди обнимають дослїди тамтих математиків, а крім того в численних точках виходять значно дальше поза них. Слїди студіованя тих творів є в цитатах, поміщених в Disq.

З записок Gauß'а виходить дальше, що він по кілька разів переробляв поодинокі роздїли своїх Disq., а крім того мусїв останнїй (VIII) роздїл відлучити з готової вже майже книжки, раз що не хотїв занадто збільшати її обєму, а друге — мабуть не вважав її розультатів ще вповнї зрілими до друку. Сей роздїл зістав невикінчений; фраґменти з нього оголошені в розвідцї „Analysis residuorum“, а решта лишила ся невидрукована і оголошена вже по смерти як спадщина.

Чотири перші роздїли Disq. є посвячені тій дісціплїнї, яка нинї має назву „множної теорії чисел“ (multiplikative Zahlentheorie), отже обіймають теорію цїлих чисел, розкладане чисел на чинники, перві числа, останки і т. д. Се не все є оріґінальний доробок Gauß'а; є там богато старого, а заслуга Gauß'а лежить в научнім уґрупованю матеріялу і систематичнім переведеню його. Вже на самім вступі вводить поняте пристайности і конґруенції[1]) і веде теорію конґруенцій, починаючи від першого степеня і переходячи до висших. Се з природи річи потягає за собою теорію степенних останків; найінтереснійші є ті розслїди, що відносять ся до первих чисел, і їм посвячений цїлий III. роздїл.

[1]) На думку Bachmann'а є добір знака пристайности ($\equiv$) дуже щасливий, бо пригадує на велику анальоґію поміж конґруенціями а рівнаннями (стр. 460); тимчасом значна більшість математиків є противного погляду, бо-ж пристайність слабше вяже числа з собою вїж рівність. Все-ж таки сей знак закорінив ся так глибоко в цїлій матем. лїтературі, що нїкому навіть не приходить на думку пропонувати зміну.

Четвертий роздїл займаєть ся квадратними останками; тут рішені такі два питаня: 1) які числа є квадратними останками даного модула m, і 2) для яких первочисельних модулів p є дане число a останком? Се провадить до означеня квадратного характеру чисел — 1, 2 і довільного первого q для даного модула p; сюди належить також „закон відворотности“ в теорії квадратних останків, якого перший вдоволяючий доказ повів ся Gauß'ови.

Дальші роздїли (V і VI) займають ся теорією квадратних останків; початки тої теорії виводять ся від тої части „додавничої“ теорії чисел, де говорить ся про представлюване чисел як суми двох квадратів зґл. в формі $x^2 + m y^2$. Богато з висліїдів того рода знали вже Fermat і Euler; були се одначе самі тільки поодинокі епізоди — що так скажемо — з того поля, які що йно Gauß уняв в одноцїльну теорію.

У нього виступають квадратні форми в виді

$$f(x, y) = a x^2 + 2 b x y + c y^2,$$

але що тут не так ходить о змінні x, y, як о постійні сочинники, значить він форму так: $f = (a, b, c)$; її сочинники є цїлі числа, а понад те ще середнїй сочинник $2b$ є паристий.

Теорія Gauß'а полягає на двох основних прикметах квадратних форм; одна з них містить ся в ідентичности

$$f(x, y) \cdot f(x' y') = [(a x + b y) x' + (b x + c y) y']^2 - D.(x y' - x' y)^2,$$

де $D = b^2 - a c$ є виріжником (у Gauß'а: determinans) форми f. Звідси слїдує сейчас, що коли якесь число n має бути „представлене“ тою формою, то виріжник форми D мусить бути його квадратним останком, т. зн. мусить бути рішима конґруенція $z^2 \equiv D \pmod{n}$. Се такий важний факт, що говоримо про представлене, яке „належить“ до даного коріня конґруенції.

Друга прикмета лежить в трансформації форм при помочи лїнійних субституцій

$$x = \alpha x' + \beta y',\ y = \gamma x' + \delta y';$$

коли нова форма $\varphi = a' x'^2 + 2 b' x' y' + c' y'^2$ має визначник D, то мусить бути $D' = D \cdot (\alpha\delta - \beta\gamma)^2$. Щоби обі форми містили взаїмно одна другу, мусить бути $D' = D$, отже $\alpha\delta - \beta\gamma = \pm 1$. Дві форми, що переходять в себе при помочи такої „одномодулової“ субституції, називають ся рівноважні (äquivalent). Через те зводить ся проблєма представлюваня чисел до шуканя найпростійших форм, рівноважних з даною (се т. зв. редукція форм). З редукції форм слїдує т. зв. рівнанє Pell'а

$$t^2 - Du^2 = 1,$$

яке конечно треба розвязати, щоби знати всї бажані форми. Відповідно тому, чи визначник є додатний чи відємний (зером анї повним квадратом він не може бути, бо тоді форма розпадаєть ся на два лїнїйні чинники), треба до розвязки рівнаня Pell'a примінити відповідну методу. Відємні визначники ставлять нас перед значно лекшу задачу, нїж додатні.

Дальші здобутки в теорії квадратних форм є власностю Gauß'a. Сюди належить: роздїл форм з даним визначником на кляси, роздїл кляс на порядки, на роди (genera) і т. д. Потім іде складане форм, яке дає перший в історії математики примір Абелевих ґруп, обчислюване скількости кляс, скількости родів, а врештї екскурс в теорію трійкових форм

$$f = a x^2 + a' x'^2 + a'' x''^2 + 2 b x' x'' + 2 b' x'' x + 2 b'' x x',$$

з якої переведена тільки елементарна частина; висшу часть перевели що йно пізнїйші математики.

Те все є змістом епохального пятого роздїлу; шестий роздїл подає тільки деякі примінення тої теорії. Зате семий роздїл порушує зовсїм нову до того часу в математицї матерію, теорію поділу кола. Вийшовши з найпростїйшого ґеометричного проблему, поділити обвід кола на n рівних частий, доходить Gauß до альґебраічного сформулованя тої задачі: розвязки рівнаня $x^n = 1$. Він мабуть не сподївав ся, яке значінє буде мати його теорія для цїлої пізнїйшої математики та які горизонти вона отворить! Люди ждали звиж 2000 лїт, щоби посунути вперед питанє про поділ кола; стало ся се 1796 р., коли Gauß подав конструкцію правильного 17-кутника, і то на чисто альґебраічній дорозї.

Bachmann здогадуєть ся, що до тої теорії дійшов Gauß з альґебраічних розслїдів, займаючи ся рівнанем $x^n = 1$, яке стоїть в очивидній звязи з поділом кола. Як в теорії конґруенцій, так і тут грають перві числа особлившу ролю, отже Gauß обмежуєть ся до первостепенних рівнань того рода. Він виказує, що рівнанє $(p-1)$-ого степеня

$$X = \frac{x^p - 1}{x - 1} = 0$$

є незведиме та що його всї корінї є r, r^2, r^3, . . ., r^{p-1}, де $r = \cos\frac{2\pi}{p} + i \sin\frac{2\pi}{p}$. Коли через g означимо первісний корінь (mod. p), то всї ті корінї r можна виразити таким рядом:

$$r,\ r^g,\ r^{g^2},\ \ldots,\ r^{g^{p-2}}.$$

На такім уставленю в ряд і розкладаню того ряду на „f-членні періоди“ в числї e ($e \cdot f = p - 1$) полягає розвязка того рівнаня. Коли розложимо $p - 1$ на перві чинники, $p - 1 = a^\alpha b^\beta c^\gamma \ldots$, то маємо до розвязки α рівнань a-того степеня, β рівнань b-того степеня і т. д. В разї коли $p = 2^{2^k} - 1$, є всї помічні рівнаня другого степеня, отже конструкція того p-кутника дасть ся перевести при помочи лїнїї і циркля; сюди належить згадана вже конструкція 17-кутника.

На тім роздїлї кінчать ся „Disquisitiones“; осьмий роздїл, про який є згадка навіть в передмові, відпав. Його змістом є, як згадано, теорія двочленних конґруенцій з первочисельним модулом:

$$x^n \equiv 1 \pmod{p}.$$

Вона поміщена в части в „Analysis residuorum“. Тут є передовсїм доказ, що n мусить містити ся в $p - 1$ та коли $\varphi(n) = a^\alpha b^\beta \ldots$ то — подібно як при рівнанях поділу кола — маємо розвязати α конґруенцій a-того степеня, β b-того степеня і т. д. І тут стрічаємо ся з розкладом на періоди.

В дальшій части маємо загальний розслїд конґруенцій висших степенів $F(x) \equiv 0 \pmod{p}$, які мають богато спільних точок з теорією рівнань. Врештї є згадка про розклад функцій на чинники, коли модулом є зложене число.

Дальшими розвідками з того поля є: „Theorematis arithmetici demonstratio nova“ (1808), „Summatio quarundarun serierum singularium“ (1811) і „Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae“ (1818). В них містять ся чотири нові докази основної теореми квадратних останків; головну трудність робило в однім з тих доказів визначенє знака $\pm$ приєднім квадратнім корени. На се стратив Ґавсс цїлих 4 роки! — Замітна тут є ще т. зв. „лемма Gauß'a“: коли (q, p) означує скількість чисел

$$q,\ 2q,\ 3q,\ \ldots,\ \frac{p-1}{p} q,$$

яких абсолютно найменші останки (mod. p) є відємні, то

$$q^{\frac{p-1}{2}} \equiv (-1)^{(q,\,p)} \pmod{p}.$$

Загалом дав Gauß 8 доказів основної теореми.

Так вичерпали ми всї працї Gauß'a, що вяжуть ся з теорією квадратних останків; остає ще сказати дещо про теорію двоквадратних останків, опубліковану в двох розвідках: „Theoria residuorum biquadraticorum, commentatio prima (1828)“ і „commentatio secunda

(1832)“. Тут є бесїда тільки про перші числа типу $4n+1$, бо тип $4n+3$ зводить ся до квадратних останків. Всї ті числа розпадають ся на чотири кляси після того, яка є вартість

$$z^{\frac{p-1}{4}} \equiv 1, f, f^2, f^3 \pmod{p},$$

де $f^2 \equiv -1 \pmod{p}$; перша й третя кляса дають квадратні останки, а друга й четверта не-останки.

В Comm. prima подає Ґавсс ще двоквадратні характери чисел -1 і 2 і розклад первих чисел $p+4n+1$ на a^2+b^2; в Comm. secunda знаходить через індукцію характери кількох инших чисел і вказує на неможливість переведеня тої теорії, коли обмежимо ся на цїлих дійсних числах. Повну теорію будемо мати, коли возьмемо під увагу звичайні злучені числа $a+bi$. Gauß подає передовсїм арифметику тих чисел і висловлює дуже точно -- одначе без доказу — закон відворотности для двоквадратних останків.

Третя обіцяна розвідка не появила ся. — Зате в кількох уривках (друкованих і в спадщинї) знаходять ся натяки на те, як будувати теорію кубових останків; до тої цїли треба розширити дійсні цїлі числа на числа форми

$$a+b\varrho+c\varrho^2, \text{ де } \varrho = \frac{-1+i\sqrt{3}}{2}, \text{ отже } \varrho^3 = 1.$$

Для повности треба згадати, що Gauß займав ся також студіями над числом π і дав доказ на невимірність стичних вимірних дуг.

Поза тим не друкував Gauß нїчого більше з теорії чисел, хоча в його спадщинї лишило ся богато матеріялів, які дають доказ, що він займав ся ще й иншими питанями, а саме т. зв. „аналїтичними методами теорії чисел“, які розвинув щойно Dirichlet; належать сюди головно деякі „асимптотні закони теорії чисел“.

Як бачимо з того короткого начерку, є становиско Gauß'a в теорії чисел перворядне; він дав їй основу, дав зміст і вказав нові дороги, якими пішов дальший розвиток тої науки. Теорія квадратних форм, теорія подїлу кола й двоквадратних останків вказали пізнїйшим наслїдникам прямо невичерпані скарби, яких ще доси вони не використали вповнї.

Праця проф. Bachmann'a, знаменитого знатока лїтератури з того поля, а головно творів Gauß'a, є дуже цїнним причинком до історії математики XIX ст., яка щойно творить ся. Ми ще занадто стоїмо під впливом минувшого віку, щоби могти дати об'єктивний огляд тих теорій і дисциплїн, що в нїм зродили ся й зросли. — Реферована тут праця повинна причинити ся у великій мірі до глибшого зрозуміня й пізнаня Gauß'ового ґенїя. *M. Ч.*

A2aa, c, D6a. Mertens F., Über die Zerfällung einer ganzen Funktion einer Veränderlichen in zwei Faktoren. Sitzungsberichte, Wien, CXX. Band, Abt. II a, 1911, p. 1485—1502.

Щоби перевести розклад функції n-того степеня $f(x) = \Sigma c_i x^i$ на добуток двох иншиx функцій степенїв m і $n-m$, $f(x) = \Sigma a_i x^i$ і $h(x) = \Sigma b_i x^i$, вводить автор такі неозначені величини: $x_1, x_2, \ldots, x_n$. Основні симетричні функції тих n величин називає $\sigma_1, \sigma_2, \ldots, \sigma_n$, основні симетричні функції перших m неозначених $\omega_1, \omega_2, \ldots, \omega_m$, а симетричні функції прочих $n-m$ означених $\vartheta_1, \vartheta_2, \ldots, \vartheta_{n-m}$. При помочи иншиx m змінних $u_1, u_2, \ldots, u_m$ творить лїнїйну функцію

$$\omega = u_1\omega_1 + u_2\omega_2 + \ldots + u_m\omega_m,$$

яка є з огляду на x $v = \binom{n}{m}$ - вартісна, отже сповнює рівнанє

$$F(z;\ \sigma;\ u) = \Pi(z-\omega) = 0.$$

Рівнанє $F(\omega) = 0$ є ідентичне в $\omega_1, \ldots \omega_m$ і $\vartheta_1, \vartheta_2, \ldots \vartheta_{n-m}$, тому можна в нїм величини ω_i і ϑ_k заступити сочинниками функцій $g(x)$ і $h(x)$, а проте величини σ_j сочинниками функції $f(x)$, отже

$$F(a_1u_1 + \ldots + a_mu_m;\ c;\ u) = 0$$

є знова ідентичне в u. Длятого всї u можна заступити довільними числами $g_1, g_2, \ldots, g_m$. Коли напишемо

$$F(z;\ c;\ g) = G(z)$$

і положимо $g_1a_1 + g_2a_2 + \ldots + g_ma_m = A$, то одержимо

$$G(A) = 0.$$

По тім приготованю ставить собі автор питанє, чи знаючи один корінь рівнаня $G(z) = 0$ можна при відповіднім доборі чисел g спричинити бажаний розклад. Ріжничкуючи $F(\omega)$ після всїх змінних u і кладучи $\frac{\partial F(z)}{\partial u_i} = -F_i(z)$, одержуємо

$$g_0(x) = \prod_{i=1}^{m}(x+x_i) = x^m + \frac{F_1(\omega)}{F(\omega)}x^{m-1} + \ldots + \frac{F_m(\omega)}{F'(\omega)}.$$

Звідси доходимо до такої ідентичности:

$$F'(z)^{n-m+1} f_0(x) = Q[F'(z)x^m + F_1(z)x^{m-1} + \ldots + F_m(z)] + RF,$$

де $f_0(x) = \prod_{i=1}^{n}(x+x_i)$, а Q і R є цїлими функціями змінних

x; z; σ; u. Тут можна покласти замість σ і u: c і g, а через се перейде та ідентичність в

$$G'(z)^{n-m+1} f(x) = Q_0(x,z)[G'(z)x^m + G_1(z)x^{m-1} + \ldots + G_m(z)] + R_0 G(z).$$

Коли вдасть ся числа g так дібрати, щоби рівнанє $G(z) = 0$ не мало многократних корінів, то кождий його корінь w дає розклад:

$$f(x) = \left(x^m + \frac{G_1(w)}{G'(w)} x^{m-1} + \ldots + \frac{G_m(w)}{G'(w)}\right) \frac{Q_0(x, w)}{G'(w)^{n-m}}.$$

Такий добір чисел можливий завсїди, коли виріжник Δ функції f не є зером; се слїдує з одної давнїйшої теореми автора (Sitzungsberichte, 1892). Проте бажаний розклад довершений.

Отсей розклад дає безпосередно другий доказ Gauss'a для основної теореми альґебри.

В дальшім уступі подав автор конечну й достаточну вимогу, щоби функція $f(x)$ мала чинник $g(x)$ приписаного степеня m; ся вимога лежить в тім, щоби рівнанє $G(z) = 0$ мало один вимірний корінь.

Примінене тих вислїдів до загальних альґебраічних тїл веде перше до питаня, коли рівнанє

$$G(x, \alpha) = x^\nu + \psi_1(\alpha) x^{\nu-1} + \ldots + \psi^\nu(\alpha) = 0,$$

де α належить до даного альґебраічного тїла R, має в тім тїлї R вимірний корінь. Коли $\psi(\alpha)$ є коренем того рівнаня, то він має форму $\psi(\alpha) = a_0 + a_1 \alpha + \ldots + a_{\nu-1} \alpha^{\nu-1}$, де ν є степенем рівнаня $\chi(z) = 0$, яке дефінїює величину α; з істнованя того коріня слїдує, що добуток

$$\Psi(x, z) = \Pi G\left(x, \frac{\chi_1(z, \alpha)}{\chi'(\alpha_1)}, \alpha\right)$$

в якім $G(x, y, z) = y^\nu G\left(\frac{x}{y}, z\right)$, а добуток розтягаєть ся на всї α, — має чинник $T(x, z)$ з вимірними сочинниками типу

$$x^{\nu-1}(x - \psi(z)) + M X(z),$$

де $M(x)$ не переступає в x степеня $r - 1$.

Врештї доказує автор, що цїла функція $F(x, t)$, яка має для кождої цїлої вартости t лїнїйний чинник $x - g$, мусить мати лїнїйний чинник $x - T$, де T є цїлою функцією змінної t. *М. Ч.*

A. 3 c. Jeřábek A., O vyhledávání resolvent methodou neurčitých součinitelův. Časopis pro pěstování mathematiky a fysiky, ročník XLII, стр. 65—97, v Praze 1912.

Дорога до твореня ресольвенти загального альґебраічного рівнаня n-того степеня складаєть ся з двох кроків:

а) При помочи неозначеного сочинника α творить ся вимірну функцію перших $n - 1$ корінів даного рівнаня

$$f(x_0, x_1, \ldots x_{n-2})$$

так, щоби вона мала тільки $n - 2$ вартостий: $f_0, f_1, \ldots, f_{n-2}$. Опісля добираючи позісталий корінь і другий неозначений сочинник β, кладемо

$$y_k = f_k + \beta x_{n-1}$$
$$(x = 0, 1, \ldots, n - 2),$$

а через те одержимо помічні функції y_k всїх корінів. Їх визначуємо методою неозначених сочинників так, щоби добуток $n - 1$ величин $y_0, y_1, \ldots, y_{n-2}$ був симетричною функцією всїх корінів x. Потім творимо помічне рівнанє степеня $n - 1$, якого корінї є $y_0, y_1, \ldots, y_{n-2}$; його сочинники R_i будуть містити в собі і x_{n-1}.

б) З того помічного рівнаня одержимо шукану ресольвенту, вводячи в нїм нову незвісну, т. зв. „розвязуючу функцію“

$$\eta = \varphi(y),$$

і вибираючи φ так, щоби всї сочинники нового рівнаня були вимірними функціями всїх R, але x_{n-1} в нїй вже не приходить.

Автор переводить свою теорію на рівнанях 3. і 4. степеня і виказує, що при загальнім рівнаню степеня вишого над 4-ий крок а) не дасть ся перевести, бо веде до суперечности. *М. Ч.*

B. 16. Moritz R. E., On the Cubes of Determinants of the Second, Third and Higher Orders. Bull. of the American Math. Society, vol. XVIII (1911/12), p. 182—189).

Коли квадрат визначника є визначником того самого порядку, то в разї куба звісне доси се явище тільки в двох виїмкових випадках: 1) $\Delta_4^3 \equiv \Delta_4'$, де Δ_4 є визначником четвертого порядку, а Δ_4' є відворотним визначником супроти Δ_4 (т. є утворений з його міноpів), і 2) визначник з першим рядком $x^n, x^{n-1}y, x^{n-2}y^2, \ldots, xy^{n-1}, y^n$, а всї прочі його рядки можна утворити символїчно так: $x'\frac{d}{dx} + y'\frac{d}{dy}$, $\frac{1}{1.2}\left(x'\frac{d}{dx} + y'\frac{d}{dy}\right)^{(2)}, \ldots, \frac{1}{n!}\left(x'\frac{d}{dx} + y'\frac{d}{dy}\right)^{(n)}$. — Маючи визначник другого ряду,

$$\Delta_2 \equiv \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}$$

одержує автор як його куб

$$\Delta_2^3 \equiv - \begin{vmatrix} a_1^2 & a_2^2 & (a_1 + a_2)^2 \\ a_1 b_1 & a_2 b_2 & (a_1 + a_2)(b_1 + b_2) \\ b_1^2 & b_2^2 & (b_1 + b_2)^2 \end{vmatrix};$$

для третього ряду

$$\Delta_3 \equiv \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}$$

$$\Delta_3{}^3 \equiv \frac{-1}{c_1\, c_2\, c_3} \begin{vmatrix} A_1{}^2 & A_2{}^2 & A_3{}^3 \\ A_1 B_1 & A_2 B_2 & A_3 B_3 \\ B_1{}^2 & B_2{}^2 & B_3{}^2 \end{vmatrix},$$

$$A_i = \frac{\text{minor } a_i}{c_{i+1}\, c_{i+2}},\quad B_i = \frac{\text{minor } b_i}{c_{i+1}\, c_{i+2}} \text{ (index mod. 3).}$$

На основі двох помічних теорем знаходить автор загально:

$$\Delta_n{}^3 \equiv \frac{-1}{(c_1\, d_4 \ldots n_n)\,(c_2\, d_4 \ldots n_n)\,(c_3\, d_4 \ldots n_n)} \begin{vmatrix} A_1{}^2 & A_2{}^2 & A_3{}^2 \\ A_1 B_1 & A_2 B_2 & A_3 B_3 \\ B_1{}^2 & B_2{}^2 & B_3{}^2 \end{vmatrix},$$

а A_i і B_i є мінорами дотичних елементів в Δ_n. Порядок куба визначника Δ_n є $3n$. *М. Ч.*

J. 4. d. Fite W. B., Irreducible Homogeneous Linear Groups of Order p^m and Degree p or p^2. Ibid., Vol. XVIII, (1911/12) p. 117—121.

До ґруп, що не можуть бути одностепенно-ізоморфні з незведимими ґрупами ріжних степенів, належать ґрупи порядку p^m першої, другої та третої кляси. В отсій розвідці розбирає автор питане, які ґрупи порядку p^m можуть бути одностепенно-ізоморфні з незведимими ґрупами ріжних степенів, і рішає його в кількох спеціяльних випадках. Висліди, до яких доходить, є: 1) Незведима ґрупа порядку p^m і степеня p не може бути ізоморфна з незведимою ґрупою иншого степеня, бо вона містить в собі Абелеву підґрупу о показчику p, а ґрупа порядку p^m, що має Абелеву підґрупу о показчику p^δ, не може бути ізоморфна з незведимою ґрупою степеня $> p^\delta$. 2) Незведима ґрупа порядку p^m і степеня p^2 не може бути ізоморфна з незведимою ґрупою якого иншого степеня; коли ґрупа степеня p^m належить до k-тої кляси ($k > 2$) і є ізоморфна з незведимою ґрупою степеня p^2, то вона містить Абелеву підґрупу о показчику $< p^k$. Коли $k = 2$, то показчик тої підґрупи є p^2. *М. Ч.*

J. 4. d. Miller G. A., Note on the Maximal Cyclic Subgroups of a Group of Order p^m. Ibid., Vol. XVIII (1911/12), p. 189—191.

Коли H є не-визначною підґрупою ґрупи G порядку p^m, то H трансформує ся в саму себе через всі спряжені з нею підґрупи в G, отже через всі оператори поза H. Коли H є циклїчною ґрупою і не містить ся в ніякій висшій циклїчній підґрупі ґрупи G, то називає ся вона **найбільшою циклїчною підґрупою в G**. До неї відносить ся така теорема: Конечною й достаточною умовою, щоби кожда найбільша циклїчна підґрупа порядку p^α в ґрупі G порядку p^m ($m > 3$) була трансформована в саму себе тільки $p^{\alpha+1}$ операторами ґрупи G, є те, щоби G містило в собі одну і тільки одну циклїчну підґрупу порядку p^{m-1}. *М. Ч.*

J. 4 d. Miller G. A., A few Theorems Relating to Sylow Subgroups. Ibid., Vol. XIX (1912/13), p. 63—66.

Доказані такі теореми: 1) Коли ґрупа G, що має підґрупи Sylow'a порядку p^m, містить визначну підґрупу H, яка зі своєї черги має підґрупи Sylow'a порядку p^β, то число підґруп порядку p^β в H є дільником числа підґруп порядку p^m в G. Коли перше число є більше ніж друге, то G трансформує свої підґрупи порядку p^m після одної неперехідної ґрупи. 2) Число підґруп Sylow'a порядку 2^m в симетричній ґрупі степеня $n > 5$ є таке саме, як число тих підґруп порядку 2^{n-1} в альтернуючій ґрупі того самого степеня. *М. Ч.*

J. 4 d. Miller G. A., The Product of Two ar More Groups. Ibid., Vol. XIX (1912/13), p. 303—310.

Щоби добуток двох ґруп H_1 і H_2 був зі своєї черги ґрупою, є конечною і достаточною вимогою те, щоби було $H_1 \cdot H_2 = H_2 \cdot H_1$, отже щоби сей добуток містив в собі відворотність кождого оператора. Коли $H_0 = \{H_1,\ H_2\}$ [1]), а h_1, h_2, h_0 є порядками дотичних ґруп, то $H_1 \cdot H_2$ містить в собі $\frac{h_1 h_2}{h_0}$ ріжних операторів. Теорія добутків двох ґруп є елементарна, зате як в добуток виходить кілька чинників, то теорія є доволї скомпліковання.

Автор доказує перше, що коли добуток $H_1 \cdot H_2 \ldots H_\gamma$ містить в собі циклїчну ґрупу тих чинників, то мусить містити рівно-ж і „двостінну ґрупу“ (Diedergruppe) тих всїх чинників. Дальше займає ся субституціями, що трансформують добуток ґруп в себе самого і доказує, що ті субституції творять ґрупу, а доказ переводить на трех ґрупах порядків 3, 4, 5. Врешті займає ся ґрупами, які є добутками підґруп Sylow'a і показує, що коли G є ґрупою

[1]) Се означене ввів Netto (Gruppentheorie, Samml. Schubert LV, p. 35) для перекрою обох ґруп, т. є ґрупи операторів, спільних обом ґрупам H_1 і H_2.

порядку $p^\alpha q^\beta r^\gamma$, де p, q, r є первими числами, а G_1, G_2, G_3 є підґрупами Sylow'a порядків p^α, q^β, r^γ, то число ріжних операторів в $G_1 \cdot G_2 \cdot G_3$ має форму $p^\alpha q^\beta r^\gamma - k p^\alpha r^\gamma$; щоби було $G = G_1 G_2 G_3$, мусить бути $k = 0$. Кожда рішима ґрупа є добутком не-спряжених (non-conjugate) підґруп Sylow'a, а порядок тих чинників в тім добутку є довільний. — Ті результати дають приступ до розвязки таких двох нерішених доси питань: 1) чи істнує проста (незложена) ґрупа зложеного порядку, яка є добутком всїх можливих рядів не-злучених підґруп Sylow'a? 2) Чи істнує ґрупа, яка не є таким добутком? *М. Ч.*

J. 4 d. Miss Cummings L. D., Note on the Groups for Triple-Systems. Ibid., Vol. XIX, (1912/13). p. 355—356.

Авторка конструує трійкову систему (Trippelsystem) з 15 елементів і доказує, що дві непристайні трійкові системи можуть мати ту саму ґрупу. *М. Ч.*

A. 4 d. Miller G. A., A Third Generalization of the Groups of the Regular Polyhedrons. Annals of Math., II ser. Vol. 13 (1912), p. 103—113.

Під назвою ґруп Hamilton'a розуміємо ґрупи, здефінїовані рівнанями

$$s_1^2 = s_3^3 = (s_1 s_2)^r = 1 \quad (r = 3, 4, 5);$$

се ґрупи оборотів правильних многостїнників. Їх узагальнив Dyck так, що три реляції Hamilton'a заступив одною. Другим узагальненєм є одна давнїйша розвідка автора, в якій $(s_1 s_2)^r$ заступлене реляцією $(s_1 s_2)^r = (s_2 s_1)^r$. Третє узагальнене, яке є предметом нинїшньої розвідки, є

$$s_1^2 = s_2^3 = (s_1 s_2)^r \quad (r = 3, 4, 5);$$

тут ходить о доказ, що для кождого r істнує minimum дві, а maximum чотири ґрупи. Крім того розбирає автор ще кілька инших, подібних реляцій.

Виславід є такий: для $r = 3$ маємо узагальнене ґрупи чотиростїнника $s_1^2 = s_2^3 = (s_1 s_2)^3$, яке дає чотири ґрупи: 1) ґрупу чотиростїнника, 2) не-дванацяткову ґрупу порядку 24, 3) і 4) ґрупу, одержану через потрійний ізоморфїзм одної з тих ґруп і циклїчної ґрупи порядку 9. Коли s_1 і s_2 є перемінні, то творять циклїчну ґрупу порядку 9 або ґрупу порядку 3.

Реляція $s_1^3 = s_2^3 = (s_1 s_2)^2$ дефінїює: коли оператори неперемінні, або чотиростїнну ґрупу або не-дванацяткову ґрупу порядку 24. Коли $s_1 s_2 = s_2 s_1$, то ґрупа є порядку 3.

Неперемінні оператори, що сповнюють рівнанє $s_1^3 = s_2^4 = (s_1 s_2)^2$, творять або ґрупу осьмистїнника, або ґрупу порядку 48, яку автор вже давнїйше назвав G_{52}. Перемінні оператори того рода творять ґрупу порядку 2.

З $s_1^4 = s_2^2 = (s_1 s_2)^3$ слїдує: в разї неперемінности операторів з чотирох ґруп: осьмистїнна, або G_{52}, або прямий добуток одної з них і ґрупи порядку 5. Перемінні оператори дають ґрупи порядків 2 або 5, або циклїчну ґрупу порядку 10.

В разї $s_1^2 = s_2^3 (s_1 s_2)^4$ маємо: з неперемінних операторів 1) ґрупу осьмистїнника, 2) ґрупу G_{52}, 3) і 4) прямий добуток одної з них з ґрупою порядку 7; з перемінних: ґрупи порядків 2 і 7 або циклїчну порядку 14.

В разї $s_1^3 = s_2^5 = (s_1 s_2)^2$ маємо або ґрупу або 20-стїнника, або ґрупу порядку 120, звісну як G_{120}.

Коли дефінїюючим рівнанєм є $s_1^2 = s_2^5 = (s_1 s_2)^3$, то маємо: 1) ґрупу 20-стїнника, 2) G_{120}, 3) і 4) прямий добуток одної з них і ґрупи порядку 11. Коли $s_1 s_2 = s_2 s_1$, маємо ґрупу порядку 11.

Врешгї $s_1^2 = s_2^3 = (s_1 s_2)^5$ дає ті дві ґрупи, що висше або їх добутки з ґрупою порядку 19. Перемінні оператори творять ґрупу порядку 19. *М. Ч.*

J. 4 d. B. 2 c. ß. Miller G. A.. Groups which Contain an Abelian Subgroup of Prime Index. Ibid. Vol. 14 (1913), p. 95—100.

Поданий доказ, що показчик підґрупи, утвореної із спільних операторів двох спряжених підґруп, супроти одної з тих підґруп, є завсїди менший, нїж показчик одної з тих підґруп супроти даної ґрупи. Звідси слїдує, що спільні оператори двох визначних підґруп того самого показчика p творять визначну підґрупу показчика p супроти кождої з тих визначних підґруп. Автор уживає тих теорем, щоби випровадити умови, серед яких неподїльна не-абелева ґрупа містить в собі не-визначну, а серед яких визначну абелеву підґрупу о первочисельнім показчику. *М. Ч.*

J. 4 a, d. V 2. Bortolotti E., Un teorema di Paolo Ruffini sulla „Teoria delle sostituzioni“. Atti della R. Accademia dei Lincei, Serie V. Vol. XXII. 1 sem. 1913, p. 679—683.

В згаданім творі доказує Ruffini таку теорему: „Коли ґрупа підставлень поміж 5 елементами 1, 2, 3, 4, 5 обіймає разом з яким небудь підставленєм t всї трансформовані з нього при помочи циклю $S_5 = (1\ 2\ 3\ 4\ 5)$, то вона містить в собі рівно-ж і сей цикль“. На

однім з примірників тої книжки дописав Ruffini власноручно таку замітку: „Отсю теорему можна розширити на перве число елементів; коли число елементів є зложене, теорема не має примінення“, відсилаючи за доказом до своїх манускриптів, там його одначе не найдено.

Тому автор подає доказ тої теореми, і опирає його на двох леммах: I. субституція

$$T=\begin{pmatrix}1 & 2 & \dots & p\\ \alpha_1 & \alpha_2 & \dots & \alpha_p\end{pmatrix},$$

що переставлює не більше як p елементів, тільки тоді може бути переміна з циклем

$$S_p=(1,\ 2,\ \dots,\ p),$$

коли є степенню того циклю“, і II. „ріжні субституції, трансформовані при помочи S_p з якоїнебудь субституції T поміж елементами 1, 2, . . ., p, непереміннної з S_p, творять перехідну ґрупу G“. Порядок тої ґрупи є p або многократь числа p. Звідси легко слїдує теорема Ruffini'я і представлене субституції T_p о p елементах в формі

$$T_p=S_p^{\alpha_p}\,S_{p-1}^{\alpha_{p-1}}\,S_{p-2}^{\alpha_{p-2}}\dots S_3^{\alpha_3}\,S_2^{\alpha_2},$$

де $S=(1\ 2\ 3\ \dots\ n)$, $n=1,\ 2,\ \dots,\ p$ (се анальоґія до розкладу цїлого числа на перві чинники), а врештї і друге представлене в формі:

$$T_p=S_p^{\alpha}\,T_{p-1},$$

де T_{p-1} є субституцією поміж $p-1$ першими елементами, а α якимнебудь числом поміж 1 і p. *М. Ч.*

I. a. b a, 19 b. Meissner W., Über die Teilbarkeit von 2^p-2 durch das Quadrat der Primzahl $p=1093$. Sitzungsberichte, Berlin, 1913, p. 663—667.

Коли три числа $x,\ y,\ z$ сповнюють реляцію Fermat'a $x^p+y^p+z^p=0$, то мусить бути, як вказав Wieferich,

$$2^{p-1}\equiv 1\ (\mathrm{mod.}\ p^2);$$

се стоїть в звязи з теоремою Furtwängler'a, що для таких трех чисел $x,\ y,\ z$ без спільного чинника мусить бути

$$r^{p-1}\equiv 1\ (\mathrm{mod.}\ p^2)$$

для кождого чинника r числа x, коли $x\not\equiv 0\ (\mathrm{mod.}\ p)$ і для кождого чинника r числа x^2-y^2, коли ся ріжниця $\not\equiv 0\ (\mathrm{mod.}\ p)$.

Для $r>2$ знайшов Jacobi такі числа, які сповнюють конґруенцію Furtwängler'a, зате конґруенція Wieferich'a не була доси провірена на жїякім конкретнім примірі. Робить се автор, вказуючи, що в перших двох тисячках є число $p=1093$ одиноке того рода, що сповнює ту конґруенцію. Врештї обчисляє вартости величин $\lambda\equiv\dfrac{2^t-1}{p}$ і $\tau=\dfrac{p-1}{t}$, де t є виложником, до якого належить 2 (mod. p), для всїх $p<200$. *М. Ч.*

J. 19 b. Bernstein F., Über den letzten Fermat'schen Satz. Nachr. d. kgl. Ges. d. Wiss. zu Göttingen, math.-phys. Kl., 1910, p. 382—488. — Über den zweiten Fall des letzten Fermat'schen Satzes. Ibid., p. 507—516.

Перша розвідка подає доказ, що: 1) коли другий чинник $h_2=l^\mu h_2'$ числа кляс $h=h_1h_2$ тїла $k(\xi)$ l-тих корінїв з одиниці є що найменше раз дїлимий через l ($\mu>0$, h_2' перве супроти l), і 2) в частиннім тїлї кляс степеня l^μ, що належить до чинника l^μ величини h_2, всї ідеали тїла $k(\zeta)$, яких l-ті степені є головними ідеалами, є вже самі головними ідеалами, — рівнане Fermat'a $a^l+b^l+c^l=0$ неможливе до сповненя в числах ріжних від 0 і первих супроти l. — Ся теорема, як також і друга, поміщена в другій розвідцї, обіймають як спеціяльні випадки результати, одержані Kummer'ом, так що ті дві працї становлять упрощене і узагальнене остатньої розвідки Kummer'a.

В другій розвідцї, згаданій в заголовку, містить ся доказ, що рівнане Fermat'a для l первого супроти тільки двох чисел a і b є неможливе, коли число кляс тїла $k(Z)$ l^2-тих корінїв з одиниці є дїлиме тільки через першу степень числа l, — і що воно неможливе також тодї, коли те тїло $k(Z)$ не містить в собі кляси, що належить до виложника l^2, а число кляс h_2 тїла $k(J+J^{-1})$ є супроти l перве. *М. Ч.*

I. 19 b. Carmichael R. D., Note on Fermat's Last Theorem. Bulletin of the American Math. Society, Vol. XIX (1912/13), p. 233—236. — Second Note on Fermat's Last Theorem. Ibid., 402—403.

В першій нотї доказує автор, що коли p є перве, а рівнане

$$x^p+y^p+z^p=0$$

має цїлочисельну розвязку $(x,\ y,\ z)$, а всї ті числа перві супроти p і поміж собою, тодї істнує таке цїле число $s<\frac{1}{2}(p-1)$, що

$$(s+1)^{p^2}\equiv s^{p^2}+1\ (\mathrm{mod.}\ p^3).$$

В другій нотї заступає отсю вимогу простїйшою, а саме:

$$(s+1)^p\equiv s^p+1\ (\mathrm{mod.}\ p^3).$$

Оба докази є елементарні. *М. Ч.*

I. 19. b. Plemelj J., Die Unlösbarkeit von $x^5+y^5+z^5=0$ im Körper $k(\sqrt{5})$. Monatshefte f. Math. u. Phys. XIII. (1912), p. 305–308.

Автор подає елементарний доказ теореми Ферматa для $n=5$. В тілї $k(\sqrt{5})$ дасть ся се рівнанє представити в видї

$$x^5 - y^5 = (\sqrt{5})^5 + \mu \,.\, z^5, \qquad (1)$$

де $(x, y, z)=1$, а всї ті числа неділимі через $\sqrt{5}$. Розкладаючи лїву сторону на два чинника, з тих один лінїйний, знаходимо, що $x \equiv y \pmod 5$, отже можна дїйти до того, що коли $x \equiv 1$, то буде і $y \equiv 1 \pmod 5$. Нелїнїйний чинник многочлена $x^5 - y^5$, скороченний через 5, розпадаєть ся знова на два чинники

$$x y + \frac{\sqrt{5} \pm 1}{2\sqrt{5}}(x-y)^2; \qquad (2)$$

вони оба мусять бути добутками якихось пятих степенїй і якихось одиниць, одначе ті остатнї можна пропустити. Тому одержимо:

$$x - y = (\sqrt{5})^3 + \mu \,.\, \zeta^5$$

а звідси:

$$\zeta^5 - \eta^5 = (\sqrt{5})^{5+2\mu} \,.\, \zeta^{10}, \qquad (3)$$

до ξ і η в обома чинниками (2), а $\xi\,\eta\,\zeta = z$. Отсе рівнанє (3) має ту саму форму, що (1), але о стїльки простїйше, що тут ζ має менше первих чинників, як z, бо ξ і η не в рівночасно одиницями. Повторенє того самого процесу на рівнаню (3) веде до суперечности, отже неможливість розвязки $x^5+y^5+z^5=0$ з $k(\sqrt{5})$ доказана. *М. Ч.*

I. 18 c., Hilbert D., Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen. (Waringsches Problem). Dem Andenken Hermann Minkowskis gewidmet. Nachrichten der kgl. Ges. J. Wiss. zu Göttingen, math.-phys. Klasse, 1909, p. 17–26.

Анґлїйському математикови Waring'ови приписують загально висказ такої теореми: „Кожде додатне цїле число дасть ся представити як сума n-тих степенїв додатнїх цїлих чисел так, що їх скількість лежить низше границї, залежної тільки від виложника n, а незалежної від представлюваного числа“. — Доси вдав ся був сей доказ тільки в кількох спеціяльних випадках, а саме для $n=2\ldots10$ з виїмком 9. Автор подає загальний доказ при помочи „нового примінення аналїзи до теорії чисел“, яке полягає в тім, що — відворотно, як се звичайно дїєть ся — автор виходить з одної інтеґральної формулки і одержує з неї чисто аритметичну реляцію.

Згаданий взорець висказує таку теорему, дану Hurwitz'ом: „При довільнім цїлім числї m є ідентично в 5 змінних $x_1, \ldots x_5$:

$$(x_1^2+x_2^2+\ldots+x_5^2)^m = C\int_{(T)}\!\!\ldots\!\int (t_{11}x_1+\ldots+t_{15}x_5)^{2m}\, dt_{11}\, dt_{21}\ldots dt_{22}\, dt_{23}\ldots dt_{45}\, dt_{55}$$

де C означує довільну постійну додатну величину, дану числом m, а 25-кратний інтеґрал простягаєть ся на царину T, положену зовсім в скінченость, а визначену так, що віддалене кождої точки t_{kh} від точки o_{kh} 10-вимірного простору Ω, даного 15 реляціями прямокутности (ортоґональности)

$$o_{k_1}^2 + \ldots + o_{k_5}^2 = 1$$
$$o_{k_1}\, o_{h_1} + \ldots + o_{k_5}\, o_{h_5} = 0 \quad (k \neq h)$$
$$(k, h = 1, 2, \ldots, 5)$$

є

$$\sum_{k,\,h} (t_{kh} - o_{kh})^2 \leqq 1.$$

З тої теореми переходить автор до другої ідентичности:

$$(x_1^2 + x_2^2 \ldots + x_5^2)^m = \sum_{h=1,\ldots,M} r_h\,(a_{1h}\,x_1 + \ldots + a_{5h}\,x_5)^{2m},$$

де

$$M = \binom{2m+4}{4},$$

$r_1, \ldots, r_M$ означують додатнї вимірні числа, залежні від m, а $a_{1h}, \ldots, a_{5h}$ цїлі числа, рівно-ж залежні тільки від m. Доказ тої ідентичности переводить ся через заступленє інтеґрала скінченою сумою.

Звідси слїдує доказ головної теореми за посередництвом таких заключень:

1) До кождого m належить якась скількість N додатнїх чисел $r_1, r_2, \ldots, r_N$ і два цїлі числа a, A, що мають таку прикмету: коли x і G є довільними цїлими числами, а Γ довільним додатнім числом, X цїлим додатнім числом, що сповнює нерівність $X < \Gamma^2 x^2$; тоді можна до тих чисел x, G, Γ, X дібрати таких N чисел $\left(\gtreqless 0\right) X_1\ X_2, \ldots, X_N$, які сповнюють нерівности $|X_h| < A\,\Gamma x$ $(h=1, \ldots, N)$, що

$$(G^2x^2 + X)^m = \sum_{h=1,\ldots,N} r_h\,(a\,G\,x + X_h)^{2m}.$$

2) Серед тих самих преміс істнує N таких цїлих чисел $X_1, \ldots, X_N$, як попередно, що

$$x\,(G^2x^2 + H)^m = \frac{1}{G}\sum_{h=1,\ldots,N} r_h\,(a\,G\,x + X_h)^{2m+1}.$$

3) До кождого виложника m належить якась скількість N додатніх чисел $r_1, r_2, \ldots, r_N$, дальше дійсна функція $\varphi(k)$ дійсної змінної k, зовсім додатна, врешті функція $F(K, k)$ (де K є цілим числом), яка при постійнім k разом з K зростає в безконечність; ті належні до m величини r_h, φ, F мають такі прикмети: коли x є довільним додатнім цілим числом, а $K > 16$, дальше дійсна змінна k сповнює нерівність $1 \leqq k < \frac{1}{2}\sqrt{K} - 1$; коли $k' = \varphi(k)$, $K' = F(K, k)$ і коли Y є довільним цілим числом $\left(\gtreqless 0\right)$, для якого $|Y| < k\sqrt{K}\,x^2$, то до величин x, K, k, Y можна завсїди дібрати N цілих чисел $Y_1, \ldots, Y_N$ $\left(\gtreqless 0\right)$, для яких $|Y_h| < k'\sqrt{K'}.x$, що

$$(Kx^2 + Y)^m = \sum_{h=1,\ldots,N} r_h (K'x + Y_h)^{2m}.$$

4) Серед тих самих преміс істнує реляція

$$x(Kx^2 + Y)^m = \frac{1}{K'} \sum_{h=1,\ldots,N} r_h (K'x + Y_h)^{2m}.$$

5) До кождого виложника n належать два цілі числа p, q такі, що $0 \leqq p < q$ і $n = p + q$, дальше додатне число K і якась скількість N додатніх вимірних чисел $k_1, k_2, \ldots, k_N$ того рода, що коли x є довільним цілим числом > 0, Y яким небудь цілим числом $\left(\gtreqless 0\right)$, для якого $|Y| < \sqrt{K}\,x^q$, то істнує завсїди N^* таких додатніх цілих чисел $P_1, P_2, \ldots, P_{N^*}$, що

$$x^p(Kx^q + Y) = \sum_{h=1,\ldots,N} k_h P_p^n.$$

З остатнього заключення виводить ся легко теорема Waring'a.

М. Ч.

B 2 a, I 3 a, b. Sanderson M., Generalizations in the Theory of Numbers and Theory of Linear Groups. Annals of Mathematics. II. ser. Vol. 13. (1912) p. 36—39.

Автор розважує конґруенції з подвійним модулом і дефінїює відворотну функцію $f_1(y)$ до функції $f(y)$ як таку, що

$$f(y) \cdot f_1(y) \equiv 1 \text{ [modd. } m, P(y)].$$

На тій основі доказує, що до кождої функції (степеня иншого, як степень модулової функції $P(y)$), якої всї сочинники мають НСП первий супроти m, істнує відворотна функція [modd. m, $P(y)$], опісля означує скількість кляс останків, що мають відворотности, формулою: $\varphi_r(m) = m^r \prod_p \left(1 - \frac{1}{p_1^r}\right)$, де $m = \prod p$, і узагальнює теореми: Фермата: $[f(y)]\,\varphi_r^{(m)} \equiv 1$ [modd. m, $P(y)$] і Wilson'a: добуток всїх функцій, що мають відворотности, є $\equiv \mp 1$ [modd. m, $P(y)$]; перший знак тоді, коли $m = p^v$ або $2p^v$ або $m = 4$, $r = 1$, другий знак в кождім иншім разї. Врешті узагальнює лїнїйні субституції, даючи їм подвійний модул; в такім разї мусить їх визначник мати відворотність [modd. m, $P(y)$].

М. Ч.

I 15 c *α.* Frobenius G., Über die Markoffschen Zahlen. Sitzungsberichte, Berlin, 1913, p. 458—487.

Числами Маркова називає автор кожду трійку чисел, що сповнює т. зв. рівнанє Маркова

$$a^2 + b^2 + c^2 = 3abc.$$

Отсе рівнанє найшов Марков з звязи з розслїдами з теорії двійкових неозначених квадратних форм; сим рівнанєм займав ся доси один Hurwitz.

В отсїй розвідці подав автор повну теорію тих чисел, опираючи ся на своїй редукції неозначених квадратних форм і розвиваю на тяглі дроби.

Передовсїм доказує автор, що в загальнїйшім рівнаню $a^2 + b^2 + c^2 = kabc$ може k мати вартість 1 або 3; підставлюючи в першім разї за a, b, c нові змінні, подільні через 3, приходимо до $k = 3$, отже рівнанє Маркова є одиноко можливе того рода. Кожда трійка чисел Маркова не має спільної міри; кожде з тих чисел p є форми $4n + 1$ або $2.(4n + 1)$, а дальше: кождий непаристий первий чинник одного з тих чисел p та чисел $3p \pm 2$ є рівно-ж форми $4n + 1$.

Найменшими розвязками того рівнаня є: (1, 1, 1) і (2, 1, 1); їх називає автор одиничними (singulär). Всї инші розвязки містять в собі трійки ріжних чисел. Коли дві розвязки ріжнять ся тільки одним числом, то вони є сусїдні; кожда трійка має три ріжні сусїдні, тільки перша одинична трійка має одну, друга дві. З кождої трійки можна одержати цілий ряд нових, коли одно число задержимо постійним, а два другі будемо зміняти і добирати до трійок сусїдні. Дїєть ся се так, що розвязуємо рівнанє $f(x) = x^2 + b^2 + c^2 - 3bcx = 0$, яке має два корінї a і a', звязані реляціями: $a + a' = 3bc$, $aa' = b^2 + c^2$. Через те одержуємо дві сусїдні трійки: (a, b, c) і (a', b, c); коли в кождій з них одно число зробимо постійним, одержимо ряд нових розвязок, який автор називає ланцухом, належним до того постійного числа. Таким чи-

ном можна одержати, кладучи за те постійне число чергою 1, 2 3, . . ., всї трійки чисел Маркова.

Щоби p було числом Маркова, є конечне і достаточне, щоби його можна представити формою φ, рівноважною з $-\varphi$, о виріжнику $9p^2-4$. Такою формою є м. и. $\varphi = px^2+(3p-2q)xy+(r-3q)y^2$; найменшим числом, яке вона представляє, є p.

Врештї розвиває автор числа Маркова на ланцухові дроби і вводить знак $p_{\alpha\beta}$ для числа, яке відповідає дробови $\varrho = \frac{\alpha}{\beta}$, именно є $p_{10}=1$, $p_{01}=2$, $p_{11}=5$, і дальше

$$p_{\alpha\alpha'} = 3p_{\beta\beta'}p_{\gamma\gamma'} - p_{\delta\delta'},$$

де $\alpha=\beta+\gamma$, $\alpha'=\beta'+\gamma'$, $\delta=|\beta-\gamma|$, $\delta'=|\beta'-\gamma'|$. Поміж такими числами панує звязь

$$p_{\alpha\alpha'}{}^2 + p_{\beta\beta'}{}^2 + p_{\gamma\gamma'}{}^2 = 3p_{\alpha\alpha'}p_{\beta\beta'}p_{\gamma\gamma'}$$

отже рівнанє Маркова. Число Маркова $p_{\varkappa\lambda}$ є тодї і тільки тодї паристе, коли $\varkappa$ є подїльне через 3.

На закінченє подає примінене виведених теорем до теореми Маркова про квадратні форми. *М. Ч.*

I. 15 a. Bieberbach L., Über die Minkowskische Reduktion der positiven quadratischen Formen und die endlichen Gruppen linearer ganzzahliger Substitutionen. Nachrichten der kgl. Gesellschaft der Wiss. zu Göttingen. Math.-phys. Klasse. 1912, p. 207—216.

Теорія редукції квадратних форм, дана Мінковским, представляє в порівнаню з давнїйшими теоріями дуже богато користий. Та можна її оперти на зовсїм иншій основі, що тїснїйше вяжеть ся з сутю річи поодиноких тверджень. Отся розвідка подає примінене теорії Мінковського в тій новій інтерпретації до доказу такої теореми: побіч одномодулових цїлочисельних трансформацій істнує тільки скінчене число ґруп цїлочисельних однородних лїнійних субституцій. Звідси дедукують Jordan і Мінковскі істнованє тільки скінченого числа одномодулових цїлочисельних субституцій, що переводять редуковані форми в инші редуковані форми. З огляду на її важність подає автор безпосередний, елементарний доказ тої другої теореми. *М. Ч.*

I. 22 a. d. Jacobsthal E., Zur Theorie der Funktionale. Crelle's Journal f. reine u. angew. Mathematik, Bd. 140, 1911, p. 266—276.

Отся розвідка подає нове уґрунтованє теорії альґебраічних чисел на основі т. зв. „Функціоналів“ Weber'a; вона замітна тим,

що на неї покликуєть ся Weber в найновійшім, скороченім виданю своєї альґебри (Braunschweig 1912, Vieweg u. Sohn. Цїна 14 м.).

Функціоналом називаємо, як звісно, квот $\omega = \frac{\varphi}{\psi}$ двох цїлих вимірних функцій яких небудь змінних з сочинниками з якого небудь альґебраічного тїла n-того степеня. Загал всїх функціоналів творить функціональне тїло, в якім містить ся те альґебраічне тїло як дїльник. Функціонал з вимірними сочинниками називаєть ся вимірним. — Заступаючи в данім функціоналї сочинники їх спряженими вартостями, одержимо n спряжених функціоналів; їх добуток є їх нормою.

Коли функціонал є вимірний, то можна його представити в формі $R = r\cdot\frac{P_1}{P_2}$, де r є вимірним, додатнїм числом, а P_1 і P_2 первісними функціями (т. є з цїлими сочинниками і без спільних чинників); r називаєть ся абсолютною вартістю функціонала: $r=|R|$.

Абсолютна вартість норми довільного функціонала називаєть ся абсолютною нормою.

Вимірний функціонал називаємо цїлим, коли його абсолютна вартість є цїлим числом. — Довільний функціонал називаєть ся цїлим, коли є коренем рівнаня, якого найвисший сочинник є 1, а прочі сочинники цїлими вимірними функціоналами.

Коли ε і $\frac{1}{\varepsilon}$ є рівночасно цїлими функціоналами, то ε називаєть ся одиницею, отже кожда первісна функція є в тім значінню одиницею.

Головна цїль тої розвідки є, виснувати з кількох теорем головне творджене цїлої теорії про однозначність розкладу цїлих функціоналів на перві функціонали, вже відворотно, як се робить Weber (Algebra, II, 1. вид. p. 590 sqq). Автор доходить до своєї цїли такими головними теоремами:

I. Функціонал $A_0 t^m + A_1 t^{m-1} + \ldots + A_m$, якого сочинники є цїлими функціоналами без спільної міри, а t змінного, що не приходить в них, є одиницею.

II. Коли ϑ є який небудь функціонал, в якім не приходить змінна u, то $\frac{1}{\vartheta+u}$ є цїлий функціонал.

III. Коли цїла функція $G(u)$ з цїлими сочинниками функціоналами, в яких не приходить змінна u, є подїльна через цїлу функцію

$g(u)$ з якими небудь сочинниками-функціоналами (рівно-ж без змінної u), то ціла функція $G(u):g(u)$ має цілі сочинники. Сю остатню теорему доказали вже перше Kronecker, Dedekind і Hurwitz, одначе не опирали ся на II. твердженю, яке в отсій розвідці грає головну ролю. *M. Ч.*

I. 4 a, 8 c, 13 b α. v. Schrutka L., Ein Beweis für die Zerlegbarkeit der Primzahlen von der Form $6n+1$ in einfaches und ein dreifaches Quadrat. Ibid., Bd. 140, 1911, p. 252—265.

Уживаючи т. зв. „сум n-того рода", введених Jacobsthal'ем (Crelle, т. 132)

$$S_n = \sum \left(\frac{f(i)}{p}\right),$$

де i є цілою функцією з цілими сочинниками n-того степеня в i, а $\left(\frac{x}{p}\right)$ означує символ Legendre'a для квадратних останків, доказує автор звісну теорему, що кожде перве число форми $6n+1$ можна розложити на суму a^2+3b^2. Опісля означує основу (Basis) того розкладу і примінює свої висліди до означеня скількости наслїдств (Sequenzen) квадратних останків і неостанків в природнім ряді чисел. *M. Ч.*

I. 4 a. v. Schrutka L., Theorie der quadratischen Kongruenzen. Monatshefte für Mathematik u. Physik, Bd. XXIII (1912), p. 92—105.

Навязуючи до попередної своєї статї в тій часописи (т. XVI, „Theorie der Polygonalreste"), автор переводить теорію квадратних конґруенцій на основі прінціпу, який називає „відбитем (Abbildung) відповідно дібраних вимірних чисел, що творять аритметичні ряди, на ряд цілих чисел". Коли в конґруенції

$$Ax^2+Bx \equiv -C \pmod{m}$$

положимо $2A=T$, $B-A=U$, де T і U є цілими, впрочім довільними, числами, то її ліву сторону переведемо в

$$T\cdot\frac{x^2+x}{2}+Ux.$$

Кождому цілому числови a приписуємо число (неконечно ціле)

$$\alpha = F(a) = \frac{4a-T-2U}{2T};$$

перехід від a до α називаємо трансформацією F. Вона відповідає

розтягненю (Streckung) чисельної лїнії від точки $\frac{T+2U}{4-2T}$ у відношеню $1:\frac{2}{T}$; лише для $T=2$ маємо пересунене о $\frac{1+U}{2}$, а для $U=1$ є $F(a)=a$.

Функція, відворотна до F є

$$a=\Phi(\alpha)=\frac{2T\alpha+T+2U}{4}.$$

Автор вводить ще такі означеня:

$$\iota=F(0),\ \varepsilon=F(1),\ \eta=F(2),\ \varrho=F(3),$$
$$f=\frac{(T+2U)(T+2U-4)}{8T};$$

вони під деяким зглядом грають ролю зера й одиниць. На їх основі дефініює такі анальоґії додаваня, множеня й степенованя:

$$\alpha(+)\beta=F(a+b)=\alpha+\beta-\iota,$$
$$\alpha(\cdot)\beta=F(ab)=\frac{T}{2}\alpha\beta+\frac{T+2U}{4}(\alpha+\beta)+f,$$
$$\overset{(n)}{\alpha}=\overset{1}{\alpha}(\cdot)\overset{2}{\alpha}(\cdot)\ldots(\cdot)\overset{n}{\alpha};$$

до них відносять ся закони перемінности, злучности і роздїльности; врештї є

$$\alpha(+)\iota=\alpha,\ \alpha(\cdot)\varepsilon=\alpha,\ \alpha(\cdot)\iota=\iota.$$

Ті операції дають ся відвернути; виключене ε дїлене через ι. З комбінацій тих рівнань слїдує твердженє, що виконане всїх операцій є завсїди можливе, коли по знаку (:) не стоїть ι, отже коли k означає результат операцій на числах $a, b, c, \ldots$, то істнує завсїди $\varkappa$, результат подібних операцій $\alpha, \beta, \gamma, \ldots$, так що $\varkappa=F(k)$.

Дальше вводить автор поняте дїлимости, первих чисел, і лїнійних конґруенцій $\alpha(\cdot)\xi\equiv\beta \pmod{p}$, які є рішимі, коли α і μ є перві супроти себе. Теорема Fermat'a звучить так:

$$\alpha^{(\varphi(\mu))}\equiv\varepsilon \pmod{p}.$$

Дальше істнує тут анальоґія до символів Legendre'a:

$$\left(\frac{\delta}{\pi}\right)\equiv\delta^{\left(\frac{\varphi(\pi)}{2}\right)};$$

ті символї мають такі самі прикмети, як звісні нам з теорії квадратних останків.

Переходячи до квадратних конґруенцій, називає автор кожде перве число p при данім F неправильним (irregulär) або правильним (regulär) в міру того, чи воно містить ся в T, чи ні; 2 є правильне

лише тоді, коли $T \equiv 2 \pmod 4$. Модул називає правильним тоді, коли він має виключно правильні перві чинники.

Коли модул правильний, то дріб $\frac{2}{T}$ є все (mod. m) пристайний до цїлого числа m, первого супроти модула; так само $F(a) \equiv s$, де s рівно-ж цїле число, врешті й f. Тодї конґруенція $\alpha \equiv \beta$ для модула m є ідентична з конґруенцією для модула μ.

Конґруенцію другого степеня зводить до виду

$$\xi^{(2)} \equiv \gamma + f \pmod{\mu},$$

де $\xi \equiv x \pmod m$, $\gamma \equiv -C \pmod m$, отже вона рішима, коли $\gamma + f$ є квадратним останком модула m.

Коли-ж модул $M = q^n q'^{n'} \ldots m$ є який небудь, а q, q', ... його неправильні чинники, то що до рішимости даної квадратної конґруенції оба модули, M і m, заховують ся однаково; доказ роздїлений на дві части, відповідно до того, чи ті перві q чинники є перві, чи $= 2$. *М. Ч.*

I 13 b *α*. v. Schrutka L., Drei Parallelsätze zum Fermat'schen Satz über die Zerlegung der Primzahlen von der Form $4n+1$ in zwei Quadrate, Ibid. Bd. XXIII (1912) p. 267–273.

Уживаючи тих самих означень, що в попередній статї, зводить автор питане можливости розкладу

$$p = a^2 + b^2,$$

де p є первим числом форми $4n+1$, до рішимости неозначеного рівнаня

$$T\frac{x^2+x}{2} + Ux + T\frac{y^2+y}{2} + Uy = k.$$

Переводячи тут трансформацію F і визначуючи вартість вираженя $x^2 + y^2 \pmod m$, доходить до таких трех теорем:

1) Коли перве число $p \equiv 5 \pmod{12}$, то $\frac{p-2}{3}$ дасть ся розложити в один, і тільки один спосіб, на суму двох „осьмикутників“ (т. є чисел форми $3x^2 - 2x$).

2) Коли $p \equiv 13 \pmod{20}$, $\frac{p-8}{5}$ дасть ся розложити в один і тільки в один спосіб на суму двох „дванацятикутників“ $(= 5x^2 - 4x)$.

3) Коли $p \equiv 10 \pmod{20}$, то $\frac{p-2}{5}$ дасть ся розложити в один і тільки один спосіб на суму двох чисел форми $5n^2 - 2n$. *М. Ч.*

D. 2 b. Petr K., O sčitání řad numerickych. Časopis, ročník XLII. p. 353–369, 465–493. V Praze 1913.

В елєментарній статї, призначеній для студентів, розбирає автор такі питаня з теорії чисельних рядів: трансформація слабо збіжного ряду в сильнїйше збіжний, розвиване останка ряду в тяглий дріб, формулка Wallis'a для π, ряд $\sum \frac{a^k}{k}$, ряд для $\frac{\pi}{\sin \pi \xi}$, ряд $\sum_{n=0}^{\infty} \frac{1}{n^2 + u^{(1)} n + u^{(2)}}$, гіпергеометричний ряд Gauß'a, а врешті ряд $\sum_{n=0}^{\infty} \frac{8}{(2n+1)^3 - D(2n+1).}$. Статейка містить в собі богато цїкавих річий, з яких не всї подибують ся в звичайних підручниках аналїзи. *М. Ч.*

B. I c. e, D 2 d. a. Rice L. H., Continuant Expressions for $\sqrt{a^2+b}$ and $(\sqrt{a^2+b}+a)^n$. Annals of Math. II. ser., vol. 14 (1913), p. 139–142.

Автор розвиває $\sqrt{a^2+b}$ і $(\sqrt{a^2+b}+a)$ в визначники і тяглі дроби, опираючи ся на теоремі Ramus'a:

$$\begin{vmatrix} 1 & b & & & \\ -1 & a & b & & \\ & -1 & a & b & \\ & & \ldots & & \end{vmatrix}_{n-1} = \frac{1}{\sqrt{a^2+4b}} \left[\left(\frac{a+\sqrt{a^2+4b}}{2} \right)^n - \left(\frac{a-\sqrt{a^2+4b}}{2} \right)^n \right]$$

Се дає:

$$(\sqrt{a^2+b}+a)^n = \begin{vmatrix} 1 & \sqrt{a^2+b} & & & \\ -1 & a & b & & \\ & -1 & 2a & b & \\ & & -1 & 2a & b \ldots \\ & & & \ldots & \end{vmatrix}_{n+1}$$

і

$$\sqrt{a^2+b} = |a| + \frac{b}{2|a| + \frac{b}{2|a| + \ldots}} \qquad M.\ Ч.$$

H. 11 h. Levi-Civita T., Sulle funzioni che ammettono una formula d'addizione del tipo $f(x+y) = \sum_{i=1}^{n} X_i(x)\, Y_i(y)$ Atti della R. Accademia dei Lincei, Vol. XXII, 2 dem. 1913, p. 181–183.

Примірами таких функцій є $e^{\omega x}$, $\sin \omega x$, $\cos \omega (x)$ (де ω є довільною постійною величиною) і многочлени $P(x)$. Щоби в загальнім разї функція $f(x)$ сповнювала ту умову, мусить бути $n = \infty$; тому автор питаєть ся, яким умовам мусить відповідати $f(x)$ для скінченого n, щоби було сповнене згадане рівнанє, і відповідає, що всї функції типу $P(x)\, e^{\omega x}$ (ω дїйсне або спряжене). Приймаючи, що всї X_i і Y_i є лїнїйно незалежні, приходить автор до заключеня, що всї X_i мусять бути розвязкоми системи рівнань

$$X_i' = \sum_{j=1}^{n} a_{ij} X_j$$

з постійними сочинниками; Y_i рівно-ж. Звідси знаходимо f як лїнїйну комбінацію сочинників функції x. *М. Ч.*

H. 12 b. E. 5. Brodén T., Einige Anwendungen diskontinuierlicher Integrale auf Fragen der Differenzenrechnung. Lunds Universitets Årsskrift. N. F. Afd. 2. Bd. 8. 1912. Nr. 8. pag. 1—17.

Автор навязує до розвідки Guichard'a з 1887 р. в „Annales de l'école normale supérieure", який ужив до розвязки функційного рівнаня

$$f(z+1) - f(z) = \varphi(z),$$

де φ звісне, f незвісне, нетяглих інтеґралів. Після його припису творить ся функцію $L(u)$ помічної змінної u, яка є аналїтичною, однозначною функцією о періоді 1 і в точках $u \equiv 0 \pmod 1$ має поодинокий бігун з останком (residuum) $= \frac{1}{2\pi i}$, впрочім є правильна. Потім треба утворити інтеґрал

$$H(z) = \int_{ih}^{ik} \varphi(u)\, L(u-z)\, du,$$

$h < k$ (оба дїйсні, довільні), інтеґрал здовж прямої лїнії від ih до ik. При помочи того інтеґрала одержуємо врешті розвязку:

$$f(z) = H(z) + \Sigma m\, \varphi(z-n).$$

Подібною методою розслїджує автор два функційні рівнаня,

$$f(z+1) - f(z) = \varphi(z)$$
$$f(z+i) - f(z) = \psi(z),$$

де φ і ψ є однозначними, аналїтичними функціями, а треба найти функцію $f(z)$; тут стоять 1, i замість звичайно уживаних період ω, ω'. — Коли отся система має бути рішима, і то однозначно, то поміж φ і ψ мусить істнувати звязь

$$\varphi(z+i) - \varphi(z) = \psi(z+1) - \psi(z).$$

Коли $F(z)$ є розвязкою другого рівнаня, то розвязка системи має форму $F(z) + P(z)$, де $P(z)$ є довільна однозначна функція з періодою i, отже для її визначеня маємо рівнаня:

$$P(z+1) - P(z) = \varphi(z) + F(z) - F(z+1),$$
$$P(z+i) - P(z) = 0.$$

Тому розвязка даної системи редукуєть ся до випадку, де $\varphi(z) \equiv 0$:

$$f(z+1) - f(z) = \varphi(z) \qquad [\varphi(z+i) = \varphi(z)].$$
$$f(z+i) - f(z) = 0$$

Її легко розвязати, кладучи

$$S(z) = \varphi(z-1) + \varphi(z-2) + \ldots$$

або

$$T(z) = -\varphi(z) - \varphi(z+1) - \varphi(z+2) - \ldots,$$

коли тільки знаємо, що оба ті ряди є рівномірно збіжні; але се тільки виїмковий випадок. — Можемо також приймити, що $\varphi(z)$ дасть ся в прямовіснім поясї о ширині > 1 розвинути в ряд

$$\varphi(z) = \varphi_0(z) + \varphi_1(z) + \varphi_2(z) + \ldots,$$

де функції φ_n мають рівно-ж періоду i, а притім рівнаня

$$f_n(z+1) - f_n(z) = \varphi_n(z)$$

є легко рішимі і то так, що також f_n має періоду i. Коли ряд

$$\sum_{0}^{\infty} f_n(z)$$

є збіжний в згаданім обсягу, то се є бажана розвязка.

Дальше займаєть ся автор приміненем нетяглих інтеґралів і вводить функцію $L(u)$, двоперіодну другого порядку, з періодами 1, i і бігунами $u = 0$, $u = \frac{1}{2}$. При її помочи творить інтеґрал

$$H(z) = \int_{0}^{ik} \varphi(u)\, L(u-z)\, du,$$

де $0 < k < \frac{1}{2}$, а дорогою інтеґрованя є пряма лїнїя. Тоді одержуємо як розвязку

$$f(z) = H(z) + \Sigma m\, \varphi(z-n) + \Sigma m,\ \varphi(z+\tfrac{1}{2}-n)$$
$$(m, n, m_1, n_1 = 0, \pm 1, \pm 2, \ldots).$$

Врешті дискутує автор прикмети функції $f(z)$ і подає ріжні модіфікації своєї методи, які мають примінене в поодиноких випадках. *М. Ч.*

I. 8 a. Plemelj J., Die Siebenteilung des Kreises. Monatshefte für Math. u. Phys. Bd. XXIII (1912), p. 309—311.

Поділ кола на 7 частий залежить від рівнаня $\frac{x^7-1}{x-1}=0$. Назвім один з його корінів $\zeta=-e^{\frac{\pi i}{7}}$; тоді величини $\zeta^\lambda+\zeta^{-\lambda}$ $(\lambda=1, 2, 4)$ сповнюють рівнанє

$$y^3+y^2-2y-1=0, \qquad (1)$$

а бік семикутника є $s_7=i(\zeta^{-1}-\zeta)$. Через субституцію $y=2-s^2$ переходить рівнанє (1) в добуток двох чинників

$$s^3\pm\sqrt{7}(s^2-1)=0; \qquad (2)$$

Карданська розвязка того рівнаня дає $s_7=r\frac{\sqrt{3}}{2}:\cos\frac{\alpha}{2}$, де $\alpha=\frac{1}{3\sqrt{3}}$. Через се осягає автор таку точність, що блуд в s_7 виносить $r.\,0{\cdot}000038<r.\frac{1}{2.10^5}$. *М. Ч.*

O¹ 2 e, q. Ernst P., Die allgemeine Mannheimsche Kurve. Ibid. Bd. XXIII (1912), p. 289–286.

Кривою Mannheim'a називаєть ся — як звісно — геом. місце осередків кривини точок стичности кривої Γ, що котить ся по прямій; як її узагальненє приймив автор і H. Wieleitner, що крива Γ котить ся по колї[1]). В отсій розвідцї йде ще дальше узагальненє, а саме, що за „криволїнійну вісь", по якій котить ся крива Γ, приймає автор довільну криву K. *М. Ч.*

O¹ 2 q. Braude L., Über die Kurven, unter deren Zwischenevoluten sich Kreise befinden. Ibid. Bd. XXIII, (1912). p. 283—288.

Криву, що ділить кождий луч кривини даної кривої K в постійнім відношеню $1:\lambda$, назвав автор в своїй діссертації „посередною еволютою" (Zwischenevolute) кривої K. В обговорюваній тут розвідцї займаєть ся він такими кривими, які поміж своїми „посередними еволютами" мають кола. Показуєть ся, що крім кола кривими K можуть бути епі- і гіпоцикльоіди $\lambda^2 s^2+R^2=a^2\left(\frac{\lambda^2-1}{\lambda}\right)^2$, після того, яке є λ. Як спеціяльні випадки є обговорені $\lambda=\pm 1$ і $a=\infty$, т. зн., що поміж „посередними еволютами" приходить пряма лїнїя. *М. Ч.*

[1]) Monatshefte XVIII, (1907), p. 315/6.

K¹ 6 a. Láska V., O nomografii. Časopis pro pěstování mathematiky a fysiky, ročnik XLII, стр. 209—217, v Praze 1912.

В тій статейцї пояснює автор суть номоґрафії; вона грає в приміненій математицї ту саму ролю, що н. пр. ґрафічна статика в будівництві. З огляду на се, що деякі номоґрами є дуже елємментарні, радить автор ужити їх до ожившленя науки в середнїх школах. — По вступі переводить як приміри: номоґрами квадратних функцій $x^2\pm ax\pm b=0$ і функції $\frac{1}{a}+\frac{1}{b}=\frac{\sqrt{2}}{c}$, яка грає ролю в оптицї. Врештї згадує про номоґрафічне визначенє ріжничкового квота $\frac{da}{db}$. *М. Ч.*

L¹. 16 a. Jeřábek V., Geometricke důkazy parametrické vlastnosti kuželoseček. Ibid. ročník XLII, (1912) p. 217—226.

Автор доказує ґеометрично таку теорему: В стіжковім перекрою (M) о осях $AB=2a$, $CD=2b$, прямі MN і MP, нормальні до тятив AM і BM, визначують на оси AB відтинок $PN=2p=2\frac{a^2}{b}$. *М. Ч.*

K¹ 7. Kounovský J., Základové projektivni geometrie. Ibid. ročník XLII, (1912), p. 230—236, 369—377.

Тут подані основи метової ґеометрії для учеників середнїх шкіл; є згадка про ряд точок, подвійний поділ, перспективні ряди, вязки лучів, метове повстанє кола, конструкцію стіжкових перекроїв, а врештї теореми Pascal'a і Brianchon'a. *М. Ч.*

L¹ 16 a. Pleskot A., O jistè vlastnosti kuželoseček. Ibid., ročník LXII, (1912) p. 494—497.

Навязуючи до ноти Єржабка (гл. вище), узагальнює автор його теорему так: Нарисуймо два стіжкові перекрої, що стикають ся з собою в кінцевих точках головної оси CD, виберім на одній з тих кривих довільну точку A, получім її з кінцями спільної оси і продовжім ті прямі до точок пересїчи B і E з другою кривою, то прямі AF і AK, поведені рівнобіжно до BD і CE, визначать на оси CD постійний відтинок KF, незалежний від положеня точки A на першій кривій. *М. Ч.*

K[1] 6 a, O[1] 2 b. Láska V., O sestrojování tečen jistých křivek rovinných. Ibid. ročnik XLII, (1912) стр. 13—20.

Автор подає способи рисованя стичних до деяких плоских кривих при помочи номографічних сорядних. Рівнане прямої прямої в тих сорядних звучить

$$\frac{a}{u}+\frac{b}{v}=1;$$

коли вона переходить через дві точки (u_1, v_1), (u_2, v_2), то має рівнане

$$\begin{vmatrix} u & v & u\,v \\ u_1 & v_1 & u_1\,v_1 \\ u_2 & v_2 & u_2\,v_2 \end{vmatrix}=0.$$

Відтинки a, b на осях U і V є

$$a=u_1\,u_2\,\frac{v_2-v_1}{u_1\,v_2-v_1\,u_2},\quad b=v_1\,v_2\,\frac{u_2-u_1}{v_1\,u_2-v_2\,u_1},$$

а в границях маємо для відтинків стичних:

$$t_a=\frac{d\,v}{d\left(\frac{v}{u}\right)}\,t_b=\frac{d\,u}{d\left(\frac{u}{v}\right)}.$$

На основі тих взірців одержуємо легким способом стичні до таких кривих: еліпси, якої рівнане в тих сорядних є $u\,v=c^2$, гіперболї ($u\,v=-c^2$), Діоклевої кісоіди ($v^3-D^2\,u=0$), еліптичної версіери[1]) і кривої „conchoida punctata“. Врешті доказує загальне твердженє, що коли для кривої $(u\,v)$ знаємо відтинки стичної t_a, t_b і маємо дану другу криву, що з першою є звязана реляцією $u\,u_1=a^2$, $v\,v_1=b^2$, то відтинки її стичної є

$$t_a'=\left(\frac{u_1}{a}\right)^2 t_a,\ t_b'=\left(\frac{v_1}{b}\right)^2 t_b,$$

тому її легко построїти.

Замітні тут легкі й незвичайно елеґантні конструкції стичних.

M. Ч.

Roman Cegielskij: Über das Sieden von Elektrolyten bei Stromdurchgang. (Sonder-Abdruck aus den Verhandl. d. Deutschen Phys. Gesellsch. XVII. 1911. p. 227—248).

Ся розвідка містить висліди експериментальних дослідів автора над впливом електричної струї на кипінє електролітів. Вона складає ся з трех частий. У першій части (вступі) подано ріжні можливі

[1]) Loria, Spez. alg. u. transz. Kurven, стр. 78.

роди теплянних проявів, що виступають у електролїтї, через який пливе електрична струя, н. пр. тепло Joule-a, тепло хемічних процесів; дальше обговорює ся вплив температури на електролїтичні прояви і лїтературу сего предмету. У другій (теоретичній) части є розвинена звязь між теплом (Q), витвореним в електролїтї або впровадженим до нього, а силою струї J, що пливе через нього. Вона зображена рівнанєм параболї $Q=A-B\,J+C\,J^2$, де на поодинокі члени складають ся отсї тепляні прояви: виміна тепла з окруженєм (огріванє електролїта ґазовою полуміню, випроміньованє), пароване, тепло Joule-a і т. д. Член $B\,J$ мусить мати відємний знак тому, що він представляє завсїди забсорбоване тепло; він став зером лише тодї, як на електродах не вивязують ся ґази. З дискусії рівнаня бачимо, що заходять чотири можливі випадки: а) $B=0$, б) $A>\frac{B^2}{4C}$, в) $A=\frac{B^2}{4C}$, ґ) $A<\frac{B^2}{4C}$.

Коли огріємо електролїт до кипіня і пустимо через нього електричну струю, то в першім випадку з ростучим J буде збільшати ся Q, отже пароване буде відбувати ся щораз живійше. В прочих трех випадках має Q minimum; тому пароване буде зразу досить живе, відтак слабне з ростучою натугою струї, опісля знов збільшає ся. Замітне, що для випадку ґ) наступає для певних вартостий J остудженє електролїта низше точки кипіня.

По причині опізненя кипіня (Siedeverzug) перебіг явища є відмінний, як се виходило би з теорії. В разї $B=0$ спричинює приріст тепл, що походить з однонапрямної або перемінної струї, дальше опізненє кипіня в міру зросту натуги струї; тому підносить ся тодї температура в анальоґічний спосіб до висше згаданого перебігу функції Q із збільшенєм J. Коли-ж при електродах вивязують ся ґази, тодї можна ожидати бодай частинного усуненя опізненя кипіня при введеню навіть слабої однонапрямної струї; се обявляло би ся в зниженю температури. Із зростом натуги струї можуть проявити ся сильні від'ємні тепляні явища і то в такій мірі, що температура може обнизити ся понизше точки кипіня. Однак при переходї ще сильнійших струй через електролїт переважати ме тепло Joule-a; тому температура буде підносити ся і зможе навіть осягнути високий степень понад точкою кипіня, коли з'явить ся опізненє кипіня; останнє є майже завсїди. Як через електролїт пливе перемінна струя і при слабій її натузї є $B=0$ або дуже мале, а за те при більшій натузї її B досягає значної величини, то можемо ожидати, що зразу температура електролїта буде підносити ся, відтак буде спадати, щоби опісля знова рости по причині щораз

сильнїйшого тепла Joule-a. Як бачимо вплив перемінної струї на кипіне електролїтів нагадує в дечім вплив однонапрямної струї.

В третій (експериментальній) части описано перебіг досвідів і зображено його численними фіґурами, що подають звязь між натугою струї J і температурою t. Висліди їх дадуть ся зібрати коротко в отсих кількох словах. Електролїти розпадають ся на дві ґрупи відповідно до впливу електричної струї на їх кипінє. До першої належать сї електролїти, що при переході однонапрямної струї видїлюють водень і кисень (н. пр. розрідженний сїрковий і азотовий квас, розчин содового сїркану). У них бачимо враз із зростом натуги струї: зразу обниженє температури (деколи низше точки кипіня води н. пр. в разї 0·15% H_2SO_4, 0·03% H_2SO_4, 1% HNO_3), опісля зріст температури, часто вище точки кипіня розчину. До сеї громади електролїтів належить зачислити також такі, що в них підчас електролїзи виявзують ся инші ґази; однак описані явища не виступають у них так виразно (н. пр. у NaCl). До другої ґрупи належать електролїти, що підчас електролїзи не видїлюють ґазів, їзза чого їх елзктро-хемічне явище тепла є зером. У них температура не спадає взагалї підчас зросту натуги струї, але противно підносить ся високо понад точку кипіня (н. пр. у $CuSO_4$, $ZnSO_4$). Перемінна струя має подібний вплив на електролїти другої ґрупи, як однонапрямна. Однак відмінне поведенє бачимо у електролїтів першої ґрупи. Коли переходить через них перемінна струя, хоч в головних рисах характер функції $t = \varphi(J)$ є також тут такий сам, як в разї однопрямної струї.

Інтересний є перебіг остиганя киплячого електролїта, коли возьмемо полумінь на бік і рівночасно пустимо через нього електричну струю. Як електролїт належить до першої ґрупи, то остиганє відбуває ся під впливом електричної струї борше, як без неї; у прочих електролїтів повільнїйше. В разї перемінних струй остигають всї електролїти взагалї повільнїйше під впливом їх, як без них.

Наведені досвіди надають ся дуже добре до демонстрації в часї викладів про тепляні явища у електролїтів під впливом електричної струї. Вони послужили також авторови до ствердженя теоретичної основи описаних досвідів. *Р. Ц.*

Roman Cegielskij: Zur Frage der „Zerlegung hochkomplizierter chemischer Verbindungen im schwankenden magnetischen Kraftfelde“. (Sonder-Abdruck aus den Verhandl. d. Deutschen Phys. Gesellsch. XV. 1913. p. 566–570).

Під заголовком „Zerlegung etc.“ оголосив J. Rosenthal[1]) висліди своїх досвідів, з яких виходить, що йому пощастило ся розложити зложені хемічні орґанічні сполуки при помочи змінного маґнетного поля. А саме мало йому повести ся розложити крохмаль, тростиновий цукор і деякі білковаті тїла на складові части, які можна вдержати через гідролїзу сих субстанцій. Умовою сего розкладу є лише певна частота зміни поля (скількість перемін маґнетного поля на секунду), яка для кождої субстанції є инша, нпр. для крохмалю обертає ся вона в межах між 440 і 480. Rosenthal витворював змінне маґнетне поле при помочи перемінної або перериваної однонапрямної електричної струї. Провідною думкою його досвідів, котрі він впрочім описує лише побіжно, був факт, що світло розкладає деякі субстанції; отже не є неможливим, що електромаґнетні дроганя з повільною періодою можуть викликувати той сам ефект. Автор рішив ся повторити сї дивні досьвіди, навязуючи до досвідів, початих дром Lederer-ом в Чернівцях, котрий не міг продовжати їх по причині свого виїзду. Останнїй зробив кілька досвідів з розчином крохмалю і цукру, однак безуспішно. Автор сеї працї уживав по змозї сильного маґнетного поля. Тому взяв цївку відповідних розмірів, на котрій було около 400 звоїв грубого дрота, і в середині її передержував субстанцію. Електричну струю переривав при помочи переривача Wehnelt-a і старав ся придержувати числа переривань, поданою Rosenthal-ом. Досвіди робив з розчинами крохмалю і тростинового цукру, а час треваня їх виносив більшу скількість годин. Однак вислід був завсїди відємний. З того виводить автор висновок, що або не повело ся ні йому ні дрови Lederer-ови осягнути вимаганих умов (н. пр. певного числа перемін маґнетного поля на секунду) або явище, винайдене Rosenthal-ом, не залежить взагалї від маґнетного поля[2]). *Р. Ц.*

Р. Суппанчіч. Ґеометрия для I. кляси середних шкіл. За нїмецким підручником проф. Суппанчіча зладив проф. Іван Сїтницкий. Жовква 1912. Накладом автора. Стор. 47. Ціна бр. 60 с.

Михайло Грицак. Учебник ґеометриї для середних шкіл. Низший степень (II і III кляса). У Львові 1913. Накладом

[1]) Університетський професор, фізіольоґ. Гл. Rosenthal. Sitzungsber. d. Königl. Preuss. Akad. d. Wiss. 1908, I. S. 20.

[2]) Недавно помістив G. W. Heimrod розвідку на ту саму тему у Zeitschrift f. Elektrochemie 19, 1913, p. 812. Згадавши про висліди автора, подає він цїлий ряд своїх досвідів, що вповнї збивають виводи Rosenthal-a.

Українського Педагогічного Товариства. Стор. VIII + 179. Ціна опр. 2 К 20 с.

Михайло Грицак. Учебник аритметики для середних шкіл. Середних степень (IV і V кляса). У Львові 1913. Накладом українського Педагогічного Товариства. Стор. IV + 240 + табл. Ціна опр. 3 К.

Конрад Кравс. Основи хемії. Після підручника проф.... приладив Роман Цегельский. Чернівці 1910. Заходом тов. „Українська Школа" в Чернівцях. Стр. II + 151. Ціна опр. 3 К.

Др. Юліян Гірняк. Начерк мінералогії і хемії для середних шкіл. У Львові 1912. Накладом Руского Товариства Педагогічного. Стор. IV + 123. Ціна опр. 2 К 40 с.

Др. Володимир Левицкий. Фізика для висших кляс середних шкіл. У Львові 1912. Накладом краєвого Фонду. Стор. VIII + 672 + 2 табл. Ціна опр. 4 К.

Др. Микола Чайковський. Начерк висших рахунків для ужитку учеників середних шкіл. VII. Звіт Дирекції ц. к. гімназії Франц-Йосифа І. за р. 1911/12 і окремою відбиткою, Тернопіль 1912, стр. 3 + 43 + 1 табл.

Др. Микола Чайковський. Новочасне „perpetuum mobile". „Ілюстрована Україна" 1913, чч. 13—14.

Популярна розвідка про велику теорему Фермата.

Др. Микола Чайковський. Безконечність. „Учитель" 1913/14, чч. 1, 2, 3, 5—6.

Володимир Кучер. Електронова теория металів. VIII. Звіт Дирекції ц. к. гімназії Франц-Йосифа І. за р. 1912/13 і окремою відбиткою, Тернопіль 1913, стр. 3—29.