8. កង(Anneaux)និង អង្គ(corps) - ឧទាហរណ៍ផ្សេងទៀត ៖ កុងគ្រុយអង់ម៉ូឌុយឡូ p (Anneaux et corps ; autre exemple : les congruences modulo p.

យើងចាប់ផ្តើមដោយប្រមូល កម្មសិទ្ធិពីជគណិតទាំងឡាយនៃ Z និង Q ។

a) Z ជាសំនុំមួយ មានច្បាប់ក្នុងពីរ គឺ បូក និង គុណ ដែលមាន លក្ខណៈ ប្រជុំ និង ត្រលប់ មួយៗមានធាតុ នប៉ុសកលិង្គ 0ចំពោះលេខបូក និង 1ចំពោះលេខគុណ ហើយ និង លេខគុណបំបែកធៀបទៅនឹងលេខបូក ។ លើសពីនេះទៅទៀត ធាតុនីមួយៗនៃ Z មានធាតុផ្ទុយ ចំពោះលេខបូក ដែលធ្វើឲ្យលេខគុណ កំណត់ទៅលើ Z នូវរចនាសម្ព័ន្ធ ជាគ្រុបអាបេលីអៀង។ ដោយធ្វើឲ្យកាន់តែទូលំទូលាយទៅនូវកម្មសិទ្ធិទាំងអស់នេះ គេបានសញ្ញាណនៃ កង (anneau) ។

និយមន័យ

គេហៅថា កង គឺ សំនុំ A មួយមានច្បាប់ក្នុងពីរ (បូក និង គុណ) បំពេញនូវល័ក្ខខ័ណ្ឌដូចតទៅ៖

1°/ A ជាគ្រុបអាបេលីអៀង ចំពោះលេខ បូក

2°/ លេខគុណមានលក្ខណៈប្រជុំ ហើយបំបែកធៀបទៅនឹងលេខបូក ។

កង A ត្រលប់ កាលណាលេខគុណមាន លក្ខណៈត្រលប់ ហើយ «សុចរិត» (intègre) កាលណា បើទំនាក់ទំនង $ab = 0 \Rightarrow a = 0$ ឬ $b = 0$ ។

គេទុកពាក្យ « កងសុចរិតបំផុត » (anneau d'intégrité) ចំពោះកងទាំងឡាយណា ត្រលប់និងសុចរិត។ ចំពោះ កង ធម្មតាជាទូទៅ គេហៅថា «តួចែកនៃសូន្យ» (diviseur de zéro) គឺជាតុ a ណាក៏ដោយ (tout élément a) ដែលផ្សំនឹងជាតុ b មិនសូន្យ

ឲ្យផលបានជា $ab = 0$ ឬ $ba = 0$។ ដូច្នេះ កង់ សុចរិត គឺជាកង់ដែលគ្មាន តួចែកនៃសូន្យ

(*un anneau intègre est donc un anneau sans diviseur de zéro*) ។

<u>ឧទាហរណ៍</u>

I.ដោយនិយមន័យខាងលើនេះ គេអាចថា Z ជាកង់សុចរិត មានធាតុ ឯកតា ។ យើងនឹង ឃើញ នៅ §10 ថាពហុធា (les polynômes) ដែលមានមេគុណជាចំនួនពិត ឬ កុំផ្លិច ក៏ជា កង់ ដែរ ។

II. អនុគមន៍ដែលកំណត់លើសំនុំជាទូទៅ E មួយ ហើយយកតម្លៃក្នុង កង់A នោះជាកង់ បើកាលណាគេកំណត់ ការបូក $h = f + g$ នៃពីរអនុគមន៍ f និង g ដោយ $h(x) = f(x) + g(x)$ ហើយនិងការគុណ $k = f \times g$ ដោយ $k(x) = f(x) \times g(x)$ ។ តែ កង់នេះ មិនមែនជា កង់សុចរិតបំផុតនោះទេ ពីព្រោះថាកាលណា E មានលើស ពីមួយធាតុឡើងទៅ នោះការគុណ fg អាចស្មើនឹងសូន្យ ដោយគ្មាន f ឬ g ណាមួយ ស្មើនឹងសូន្យឡើយ ៖

ដោយតាង A ជាផ្នែកមួយនៃ E ហើយមិនទទេ និងមិនស្មើនឹង E ហើយ B ជាសំនុំបំពេញ ($B = E - A$) នោះយើងបាន អនុគមន៍ របៀបនេះមួយគូ ដោយដាក់៖

$f(x) = 1$ បើ $x \in A$ និង $f(x) = 0$ បើ $x \in B$ និង

$g(x) = 0$ បើ $x \in A$ និង $g(x) = 1$ បើ $x \in B$ ។

b) សំនុំ Q នៃចំនួនសនិទាន ក៏មានរចនាសម្ព័ន្ធ ជាកង់ដែរ។ តែលើពីនេះទៅទៀត ធាតុនីមួយៗនៃ Q ក្រៅតែពីសូន្យចេញនោះមានចំរាសចំពោះលេខគុណ។ ដោយធ្វើឲ្យកាន់តែទូលំទូលាយទៅចំពោះកម្មសិទ្ធិនេះ គេបាន សញ្ញាណនៃ អង្គ

(*Par généralisation de ctte propriété, on obtient la notion de corps*)។

<u>និយមន័យ</u>

អង្គ K (un corps K) គឺជាសំនុំមួយ ដែលនៅលើនោះគេបានកំណត់ ច្បាប់ក្នុងពីរ (គឺ បូក និង គុណ) ដែបំពេញ៖

1° K ជាគ្រុបអាបេលីអៀង ចំពោះ បូក

2° $K - \{0\}$ ជាគ្រុប ចំពោះ គុណ ។

បើនិយាយមួយបែបទៀត អង្គ គឺជា កង ដែលនៅក្នុងនោះ ការធ្វើលេខចែកដោយចំនួនមួយមិនសូន្យ អាចធ្វើបានជានិច្ច ។ យើងសង្កេតឃើញថានៅក្នុង អង្គ គ្មាន តួចែកនៃសូន្យទេ ៖ ពីព្រោះបើ $a \neq 0$ នោះចំរាស a^{-1} របស់វាមាន ហើយទំនាក់ទំនង

$ab = 0 \Rightarrow a^{-1}ab = 0 \Rightarrow b = 0$ ហើយក៏ដូចគ្នា $ba = 0 \Rightarrow ba\,a^{-1} = 0$ ឬ

$b(aa^{-1}) = 0 \Rightarrow b \times 1 = 0$ ដូច្នេះ $b = 0$ ។

អង្គ ត្រលប់ បើកាលណា ការគុណ ត្រលប់។

ដោយនិយមន័យទាំងនេះ គេអាចថា Q ជាអង្គត្រលប់។

ឧទាហរណ៍អំពី កង និង អង្គ ៖ កុងគ្រុយអង់ម៉ូឌុយឡូ p

N ជាសំនុំនៃចំនួនគត់ធម្មជាតិជានិច្ច ហើយ p ជាធាតុមួយនៅក្នុង N ហើយយើងកំណត់តម្លៃ p នោះដែលមិនផ្លាស់ផ្តូរ ហើយ៉ាងតិចណាស់ស្មើនឹង២ ។ យើងដាក់ថា $a \equiv b$ បើ $|a - b|$ ចែកដោយ p ដាច់ ៖ យើងឃើញថាដូច្នេះយើងបាន ទំនាក់ទំនងសមមូល មួយកំណត់លើ N ពីព្រោះទំនាក់ទំនងនេះ ឆ្លុះ រ៉េផ្លិចស៊ីវ ហើយម្យ៉ាងទៀត ទំនាក់ទំនង $a \equiv b$ និង $b \equiv c$ នោះបណ្តាលឲ្យមាន ចំនួនគត់សនិទាន α និង β ដែលឲ្យ $a - b = \alpha p$ និង $b - c = \beta p$ ដូច្នេះយើងទាញបាន $a - c = p(\alpha + \beta)$ ដែលបង្ហាញថា $a \equiv c$ ហើយទំនាក់ទំនង ត្រង់ស៊ីទីវ ។

ទំនាក់ទំនង $a \equiv b$ ក៏អាចកំណត់ដោយថ្លែងថា "a ចែកដោយ p និង b ចែកដោយ p

មាន សំណល់ស្មើគ្នា » ។ ដែលធ្វើឲ្យយើងមើលឃើញកាន់តែច្បាស់នូវ កម្មសិទ្ធិនេះ[1]។

<u>សង្កេត</u>

យើងអាចបង្ហាញថា ចំនួនគត់ពីរកុងគ្រុយនឹងគ្នា ម៉ូឌុយឡូ p កាលណាសំណល់ក្នុងការចែក ចំនួននីមួយៗដោយ p នោះស្មើគ្នា ដូចតទៅ៖

ដោយចែក a ដោយ p យើងអាចសរសេរ៖ $a = pq1 + r1$ $(0 \le r1 < p)$

$a - r1 = pq1 \Rightarrow a \equiv r1$ (តាមនិយមន័យ ហើយ $r1$ ជាសំណល់)

ដោយចែក b ដោយ p យើងអាចសរសេរ៖ $b = pq2 + r2$ $(0 \le r2 < p)$

$b - r2 = pq2 \Rightarrow b \equiv r2$ (តាមនិយមន័យ ហើយ $r2$ ជាសំណល់)

បើ $a \equiv b$ នោះដោយ ត្រង់ស៊ីទីវ $r1 \equiv r2 \Rightarrow r1 - r2$ ចែកនឹង p ដាច់ តែដោយ $0 \le r1 < p$ និង $0 \le r2 < p$ ដូច្នេះ បើ $r1 \ge r2$ នោះ $0 \le r1 - r2 < p$ ហើយដើម្បី $r1 - r2$ ចែកនឹង p ដាច់ ទាល់តែ $r1 - r2 = 0$ ពីព្រោះ $p \ge 2$។ ដូច្នេះ $r1 = r2$ ។

ដោយហេតុនេះហើយបានជាគេហៅថា ថ្នាក់សមមូល នៃទំនាក់ទំនងសមមូលនេះ ជា « ថ្នាក់សមមូលសំណល់ម៉ូឌុយឡូ p "(*classes résiduelles modulo* p) ហើយ ទំនាក់ទំនងនេះ គេហៅថា « <u>កុងគ្រុយអង់ម៉ូឌុយឡូ p</u> »។ ហើយគេថ្លែង ទំនាក់ទំនង $a \equiv b$ ដោយនិយាយថា « a កុងគ្រុយនឹង b ម៉ូឌុយឡូ p »។

នៅទីនេះយើងតាងដោយ (a) ថ្នាក់សមមូល ដែលមានធាតុ a ហើយដោយ Z_p

---

[1] ឧបមា $p = 3$ យើងឃើញថា $7 \equiv 16$ ពីព្រោះ $|7 - 13| = 6$ ដែលចែក ដោយ 3 ដាច់។ ហើយបើយើង ចែក 7 ដោយ 3 យើងបានសំណល់ ស្មើនឹង 1 ដែលស្មើនឹងសំណល់ នៃការចែក 13 ដោយ 3 ដែរ ។

សំនុំនៃថ្នាក់ទាំងអស់នោះ (Z_p គឺជាសំនុំដើងលព្ធ - *ensemble quotient*)។ យើងសង្កេត ថា ថ្នាក់នីមួយៗ មានដំណាង α តែមួយគត់ ដែលបំពេញ $0 \leq \alpha < p$ ដោយ αដែលជា សំណល់ក្នុងការចែក a ដោយ p ។

<u>វិធីគណនា (opérations)</u>

យើឃើញភ្លាមថាទំនាក់ទំនង $a' \equiv a$ ហើយ $b' \equiv b$ => $a' + b' \equiv a + b$ និង $a'b' \equiv ab$ ។ ដូច្នេះ ថ្នាក់ $(a + b)$ និង ថ្នាក់ (ab) ជាប់ទាក់ទងតែនឹង (a) ហើយនិង (b) ហើយគេអាច កំណត់ វិធីគណនា លើ Z_p (លេខបូក និង លេខគុណ) ដោយៈ

$$(F1) \qquad (a) + (b) = (a + b) \quad ; \quad (a) \times (b) = (ab)$$

ដូច្នេះតាមនិយមន័យនេះ វិធីគណនានេះ មានកម្មសិទ្ធិ ដូចគ្នានឹង លេខបូក លេខគុណ នៃចំនួនគត់ធម្មជាតិ។ លើសពីនេះទៅទៀត ជាតុ (a) មានជាតុផ្ទុយជានិច្ច ដើម្បីនឹងឃើញជាតុផ្ទុយនោះ យើងអាចសន្មតថា $0 \leq a < p$ ហើយយើងឃើញដោយ ច្បាស់ថា $(p - a)$ ជាជាតុផ្ទុយរបស់ (a) [ពីព្រោះដោយ(F1) $(p - a) + (a) = (p - a + a) = (p)$ => $(p - a) + (a) = (p)$ ហើយដោយ $p \equiv 0$ ដូច្នេះ $(p - a) + (a) = (0)$ ដែលបង្ហាញថា $(p - a)$ ជាជាតុផ្ទុយ របស់ (a)] ។ ដូច្នេះ Z_p ជា កង ត្រលប់ (*un anneau commutatif*) ដោយមាន (1) ជាជាតុនប៉ុសកលិង្គចំពោះ លេខគុណ ។

<u>តួចែកនៃសូន្យ</u>

ដើម្បីទំនាក់ទំនង $(a) \times (b) = 0$ ផ្ទៀងផ្ទាត់ នោះត្រូវតែនិងគ្រាន់តែ ផលគុណ ab ចែក ដោយ p ដាច់ (គឺថា $ab \equiv 0$ ម៉ូឌុយឡូ p) ៖ បើ p ជាចំនួនបឋម នោះដោយទ្រឹស្តី ហ្គោស (*théorème de Gauss*) នោះត្រូវចំនួនណាមួយក្នុងចំណោម a ឬ b អាចចែក ដោយ p

ដាច់ គឺជាកុងគ្រុយនឹង សូន្យ។ ដូច្នេះ បើ p ជាចំនួនបឋម ទំនាក់ទំនង $(a)\times(b)=0$ => $(a)=0$ ឬ $(b)=0$ ហើយ Z_p ជាកងសប្បុរស (anneau d'intégrité) មួយ ។ តែបើ p មិនមែនជាចំនួនបឋមទេ នោះមានចំនួនគត់ពីរ a និង b ដែលបំពេញ $p=ab$ [2] និង $0<a<p$, $0<b<p$; ដូច្នេះគេមានថ្នាក់ $(a)\times(b)=(0)$, $(a)\neq 0$ និង $(b)\neq 0$ ដែលបង្ហាញថា (a) និង (b) ជាតួចែកនៃសូន្យ ក្នុង Z_p ។

<u>ធាតុបំរាស (éléments inversibles)</u>

ដើម្បី ធាតុ (a) ទទួល (b) ជាចំរាស នោះត្រូវតែនិងគ្រាន់តែ គេមាន $ab\equiv 1$ ក៏ដូចជាថាមាន ចំនួនគត់សនិទាន $\propto$ មួយដែលបំពេញ $ab=1+\propto p$ (ពីព្រោះ តាមនិយមន័យ $ab\equiv 1\,[p]$ => $ab-1\equiv 0\,[p]$ <=> $ab-1=\propto p$) ។ ដូច្នេះ $ab=1+\propto p$ => ដោយ a ចែក ab ដាច់ ដូច្នេះ a ចែក $1+\propto p$ ហើយដើម្បី មាន $\propto$ នោះទាល់តែa ហើយនិង p បឋមនឹងគ្នា[3] គឺថា a មិនអាចចែក p ទេ ដើម្បីមាន p នៅក្នុងកន្សោម $\propto p$។ ទ្រឹស្តី បឺស៊ូត (théorème de Bezout) (មើល T04 – 007) ចែងថា៖

បើ d ជា P.G.C.D. នៃចំនួន a និង b នោះគេអាចរកចំនួតគត់ធម្មជាតិពីរ x និង y ដែលឲ្យ $d=ax-by$ ។

ដូច្នេះ បើ a និង p ជាបឋមទៅវិញ នោះ P.G.C.D.(a,p) = 1 ដូច្នេះ តាមទ្រឹស្តីប៊ឺស៊ូត គេអាចរកបានន្ធូវ ចំនួន b និង $\propto$ ដែលឲ្យ $1=ab-\propto p$ => $ab=1+\propto p$ ។ បានន័យថាបើគេឲ្យធាតុ a នោះបើ a បឋមនឹង p នៅពេលនោះ a មានចំរាសធាតុ b ដែលកំណត់ដោយ ទំនាក់ទំនង $1=ab-\propto p$ ។ ដូច្នេះ យើងអាចថ្លែងថា ៖

<u>ការស្នើ (V, 8, 1)</u>

សំនុំ Z_p នៃថ្នាក់សំណល់ ម៉ូឌុយឡូ p ជា កង ត្រលប់មួយ (un anneau commutatif)

---

[2] បើ $p=6$ នោះ $2\times 3=6$ => $(2)\times(3)=0$

[3] $P.G.C.D(a,p)=1$

មាន តួចែកនៃសូន្យ បើ p មិនមែនជាចំនួនបឋម ។ ថ្នាក់ (a) មានថ្នាក់ចំរាស លុះត្រាតែ និងគ្រាន់តែ a និង **p** បឋមនឹងគ្នា[4] ។ ដូច្នេះ Z_p គឺជា អង្គ $(un\ corps)$ លុះត្រាតែ និងគ្រាន់តែ **p** ជាចំនួនបឋម ។

[4] ចំនួនពីរ បឋមនឹងគ្នា កាលណា $P.G.C.D.$ នៃចំនួនទាំងពីរនោះ ស្មើនឹង 1។ ឧទាហរណ៍ ដូចជា 6 និង 35 បឋមនិងគ្នា ។ តែ 6 និង 27 មិនបឋមនឹងគ្នាទេ ពីព្រោះ ចែកនឹង 3 ដាច់ ។ បើ p ជាចំនួនបឋម នោះចំនួនគត់ $0 < a < p$ ណាក៏ដោយ ក៏បឋមនឹង p ដែរ គឺថា $P.G.C.D.(a,p) = 1$។