Leçon 121 Nombres premiers, applications

Dorian Cacitti-Holland

2020-2021

Références.

1. Algèbre et géométrie de Jean-Etienne Rombaldi
2. Cours d'algèbre de Daniel Perrin
3. Oraux X-ENS algèbre 1
4. Extensions de corps Théorie de Galois de Josette Calais
5. Eléments de théorie des anneaux de Josette Calais
6. Histoires hédonistes de groupes et de géométries tome 1 de Caldero et Germoni
7. Eléments de théorie des groupes de Josette Calais

Développements.

1. Equations des deux carrés par les entiers de Gauss
2. Théorème de Sophie Germain
3. Critère d'irréductibilité d'Eisenstein
4. Théorèmes de Sylow

Table des matières

1 Arithmétique sur les entiers avec les nombres premiers

1.1 Factorialité de l'anneau des entiers

(Chapitres 11.1 et 7.6, d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Définition : Soit $p \in \mathbb{N}$, alors on dit que p est premier s'il admet exactement deux diviseurs positifs (1 et p), et on note $\mathcal{P}$ leur ensemble
2. Exemple : 2 est premier, 21 ne l'est pas
3. Théorème d'Euclide : Soit $n \in \mathbb{Z}\backslash\{-1, 0, 1\}$, alors n admet un diviseur premier
4. Exemple : Un diviseur premier de 27 est 3
5. Définition : Soit A un anneau intègre commutatif unitaire, alors on dit que A est factoriel si tout $a \in A$ s'écrit $a = u\prod_{i=1}^{r} p_i$ avec $u \in A^\times$ et $p_i \in A$ irréductibles, et si $a = u\prod_{i=1}^{r} p_i = v\prod_{j=1}^{s} q_j$ deux telles décompositions, alors u et v sont associés, $r = s$ et il existe $\sigma \in S_r$ tel que $p_i = q_{\sigma(i)}$
6. Théorème : Soit A un anneau euclidien, alors A est factoriel
7. Proposition : $\mathbb{Z}$ muni du stathme $|\cdot|$ est un anneau euclidien
8. Corollaire : Théorème fondamental de l'arithmétique : $\mathbb{Z}$ est un anneau factoriel
9. Exemple : $314 = 2 \times 157$

1.2 Résolutions d'équations diophantiennes

(Chapitre II.6 du Cours d'algèbre de Daniel Perrin et Exercice 4.39 de Oraux X-ENS algèbre 1)

1. Définition : L'anneau des entiers de Gauss est $\mathbb{Z}[i] = \{a + ib, a, b \in \mathbb{Z}\}$, et on définit $\Sigma = \{n \in \mathbb{N}, \exists (x, y) \in \mathbb{N}^2, n = x^2 + y^2\}$
2. Lemme : On a $\mathbb{Z}[i]^\times = \{-1, 1, i, -i\}$
3. Lemme : Soit $n \in \mathbb{N}$, alors $n \equiv 3[4] \Longrightarrow n \notin \Sigma$ et $n \in \Sigma \Longleftrightarrow \exists z \in \mathbb{Z}[i], n = N(z)$
4. Proposition : L'ensemble Σ est stable par multiplication
5. Lemme : Soit $p \in \mathcal{P}$, alors $p \in \Sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$
6. Théorème : Soit $p \in \mathcal{P}$, alors $p \in \Sigma \Longleftrightarrow p = 2$ *ou* $p \equiv 1[4]$
7. Exemple : $41, 53$ et 61 sont congrus à 1 modulo 4, donc sont sommes de deux carrés, effectivement $41 = 5^2 + 4^2, 53 = 7^2 + 2^2, 61 = 6^2 + 5^2$
8. Théorème : Soit $n \in \mathbb{N}$, alors, si $n \in \{0, 1\}$ alors $n \in \Sigma$, sinon on décompose n en facteurs premiers $n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$ et ainsi $n \in \Sigma \Longleftrightarrow \forall p \in \mathcal{P}, p \equiv 3[4] \Rightarrow \nu_p(n) \in 2\mathbb{N}$
9. Théorème de Sophie Germain : Soit $p \in \mathcal{P}$ impair tel que $q = 2p + 1 \in \mathcal{P}$ (p est appelé nombre de Sophie Germain), alors il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que p ne divise pas xyz et $x^p + y^p + z^p = 0$
10. Remarque : Le théorème de Fermat nous dit qu'il n'existe pas $x, y, z \in N^*$ tel que $x^n + y^n = z^n$ dès que $n \geq 2$ (admis)

1.3 Fonctions liées : valuations, fonctions d'Euler et de Möbius

(Chapitres 11.2, 11.4, 10.2 et 11.7 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Définition : Soit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec p_i distincts, alors la valuation p_i-adique est $\nu_{p_i}(n) := \alpha_i$
2. Remarque : Soit $n \in \mathbb{N}$ et $p \in \mathcal{P}$, alors $p \mid n \iff \nu_p(n) > 0$
3. Proposition : Soit $a, b \in \mathbb{N}$, alors $a \mid b \iff \forall p \in \mathcal{P}, \nu_p(a) \leq \nu_b(p)$, $\nu_p(ab) = \nu_p(a) + \nu_p(b)$, $\nu_p(a^b) = b\nu_p(a)$ et $\nu_p(a+b) \geq min(\nu_p(a), \nu_p(b))$
4. Application : $PGCD(a,b) = \prod_{p \in \mathcal{P}} p^{min(\nu_p(a), \nu_p(b))}$ et $PPCM(a,b) = \prod_{p \in \mathcal{P}} p^{max(\nu_p(a), \nu_p(b))}$
5. Définition : Soit $n \in \mathbb{N}^*$, alors la fonction d'Euler en n est $\varphi(n)$ le nombre d'entiers compris entre 1 et n premiers avec n
6. Exemple : Soit $p \in \mathcal{P}$, alors $\varphi(p) = p - 1$
7. Théorème d'Euler : Soit $n, a \in \mathbb{N}^*$ premiers entre eux, alors $a^{\varphi(n)} \equiv 1[n]$
8. Corollaire : Théorème de Fermat : Soit $p \in \mathcal{P}$ et $a \in N^*$ premier avec p, alors $a^{p-1} \equiv 1[p]$, donc pour tout $a \in \mathbb{N}$, $a^p \equiv 1[p]$
9. Théorème : $n = \sum_{d \mid n} \varphi(d)$
10. Définition : Soit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, alors la fonction de Möbius en n est $\mu(n) = 1$ si $n = 1$, $\mu(n) = (-1)^r$ si $n = \prod_{i=1}^{r} p_i$ et $\mu(n) = 0$ sinon
11. Proposition : Soit $n \in \mathbb{N}^*$, alors $\sum_{d \mid n} \mu(d) = 0$ si $n \geq 2$ et $\sum_{d \mid n} \mu(d) = 1$ si $n = 1$
12. Théorème : Formule d'inversion de Möbius : Soit $u(n) = \sum_{d \mid n} v(d)$, alors $v(n) = \sum_{d \mid n} \mu(d) u\left(\frac{n}{d}\right)$
13. Application : $\varphi(n) = \sum_{d \mid n} \mu(d) \frac{n}{d}$

2 A la recherche des nombres premiers

2.1 Répartition des nombres premiers

(Chapitres 11.1 et 11.3 d'Algèbre et géométrie de Jean-Etienne Rombaldi et Exercices 11.9.10, 11.9.12 et 11.9.13 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Théorème d'Euclide : $|\mathcal{P}| = +\infty$
2. Définition : Soit $n \in \mathbb{N}^*$, alors on note $\mathcal{P}_n$ l'ensemble des nombres premiers compris entre 1 et n, et $\pi(n) = |\mathcal{P}_n|$
3. Remarque : $\pi(n) \underset{n \to +\infty}{\longrightarrow} +\infty$
4. Théorème (admis) : $\pi(n) \underset{n \to +\infty}{\sim} \frac{n}{ln(n)}$
5. Corollaire : Théorème de raréfaction de Legendre : $\frac{\pi(n)}{n} \underset{n \to +\infty}{\longrightarrow} 0$

6. Proposition : Soit $n \geq 2$, alors il existe n entiers consécutifs non premiers
7. Exemple : $m_k = (n+1)! + k$ pour $k \in [\![2, n+1]\!]$
8. Lemme : En notant p_n le n-ième nombre premier, on a $2n - 1 \leq p_n \leq 2^{2^{n-1}}$ et $p_n \underset{n \to +\infty}{\sim} nln(n)$
9. Proposition : Soit $n \geq 2$, alors $\pi(n) > ln(ln(n))$
10. Théorème : $\sum_{n=1}^{+\infty} \frac{1}{p_n} = +\infty$

2.2 Critères de primalité

(Chapitres 11.1 et 11.5 d'Algèbre et géométrie de Jean-Etienne Rombaldi)
On considère $n \geq 2$.

1. Théorème : Si n non premier alors il existe $p \in \mathcal{P}$ tel que $p \mid n$ et $p \leq \sqrt{n}$
2. Corollaire : En effectuant les divisions euclidiennes de n par tous les $d \in [\![2, \sqrt{n}]\!]$, on peut tester la divisibilité de n par les nombres premiers $p \leq \sqrt{n}$
3. Théorème : Crible d'Erathostène : Soit m la partie entière de $\sqrt{n}$, on se donne la liste $[\![2, m]\!]$, on garde 2 et on supprime les multiples de 2 de cette liste, pareil pour 3 et pour tous les autres nombres premiers $p \leq \sqrt{n}$
4. Théorème : $n \in \mathcal{P}$ si et seulement si pour tout $\alpha \in \mathbb{N}^*$, $\varphi(n^\alpha) = (n-1)n^{\alpha-1}$ si et seulement si $\varphi(n) = n - 1$
5. Proposition : n est premier si et seulement si n est premier avec tout entier de $[\![1, n-1]\!]$
6. Théorème : n premier si et seulement si $\mathbb{Z}/n\mathbb{Z}$ un corps si et seulement si $\mathbb{Z}/n\mathbb{Z}$ intègre
7. Exemple : $\mathbb{Z}/4\mathbb{Z}$ n'est pas un corps

3 Utilisation en théorie des corps finis

3.1 Propriétés des corps finis

(Chapitres 13.4 d'Algèbre et géométrie de Jean-Etienne Rombaldi, III.2.b du Cours d'algèbre de Daniel Perrin et 4.3 de Extensions de corps de Josette Calais)
On considère $q = p^n$ avec $p \in \mathcal{P}$.

1. Proposition : Soit K un corps fini, alors la caractéristique de K est un nombre premier
2. Définition : On note $U_n(p)$ l'ensemble des polynômes unitaires irréductibles de degré n dans $\mathbb{F}_p[X]$ et $I_n(p) = |U_n(p)|$
3. Proposition : Soit $P \in U_n(p)$, alors $\mathbb{F}_p[X]/(P)$ est un $\mathbb{F}_p$-espace vectoriel de dimension n et est un corps de cardinal $q = p^n$
4. Exemple : $\forall \lambda \in \mathbb{F}_p, X - \lambda \in U_1(p)$ donc $I_1(p) = p$ et tous ces corps $\mathbb{F}_p[X]/(X - \lambda)$ sont isomorphes à $\mathbb{F}_p$
5. Exemple : Comme $P = X^2 + \lambda X + \mu$ est irréductible si et seulement si sans racines, $I_2(p) = \frac{p(p-1)}{2}$

6. Lemme : En notant $P_n = X^{p^n} - X = X^q - X$, tout diviseur irréductible de P_n dans $\mathbb{F}_p[X]$ est de degré divisant n, réciproquement pour tout diviseur d de n, tout polynôme $P \in U_n(d)$ divise P_n
7. Théorème : P_n est sans facteur carré dans $\mathbb{F}_p[X]$ et on a la décomposition en irréductibles $P_n = \prod_{d|n} \prod_{P \in U_d(p)} P$
8. Théorème : A isomorphisme près, il existe un unique corps à q éléments, on le note $\mathbb{F}_q$, il s'agit de $\mathbb{F}_p[X]/(P)$ avec $P \in U_n(p)$, et du corps de décomposition de P_n sur $\mathbb{F}_p$
9. Exemple : $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}, \mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+1)$

3.2 Critères d'irréductibilité des polynômes

(Chapitres 5.6.C de Eléments de théorie des anneaux de Josette Calais, II.4.a du Cours d'algèbre de Daniel Perrin)

1. Définition : Soit $f \in \mathbb{Z}[X]\backslash\mathbb{Z}$, alors le contenu de f est $c(f)$ le PGCD des coefficients de f, et on dit que f est primitif si 1 est le PGCD des coefficients de f
2. Remarque : Soit $f \in \mathbb{Z}[X]\backslash\mathbb{Z}$, alors il existe $f_0 \in \mathbb{Z}[X]\backslash A$ primitif tel que $f = c(f)f_0$, de plus tout polynôme unitaire est primitif
3. Lemme de Gauss : Soit $f, g \in \mathbb{Z}[X]$, alors $c(fg) = c(f)c(g)$
4. Proposition : Soit $r \in \mathbb{Z}[X]^*$, alors :
   — r irréductible dans $\mathbb{Z}[X]$ et $deg(r) = 0$ si et seulement si r irréductible dans $\mathbb{Z}$
   — r irréductible dans $\mathbb{Z}[X]$ et $deg(r) > 0$ si seulement si r primitif dans $\mathbb{Z}[X]$ et irréductible dans $\mathbb{Q}[X]$
5. Théorème : $\mathbb{Z}[X]$ est factoriel
6. Théorème : Critère d'irréductiblité d'Eisenstein : Soit $f \in \mathbb{Z}[X]$ de degré $n = deg(f) > 0$, s'il existe $p \in \mathcal{P}$ tel que $\forall i \in [\![0, n-1]\!], p \mid a_i$, p^2 ne divise pas a_i et p ne divise pas a_n alors f irréductible dans $\mathbb{Q}[X]$, si de plus f primitif alors f irréductible dans $\mathbb{Z}[X]$
7. Exemple : Dans $\mathbb{Z}[X]$, $X^5+4X^3+15X+2$ est irréductible dans $\mathbb{Z}[X]$, $\sum_{i=0}^{p-1} X^i$ également
8. Application : $P = X^n - p$ avec $p \in \mathcal{P}$, est irréductible et de degré n

3.3 Résidus quadratiques et symbole de Legendre

(Chapitres 13.6 et 13.7 d'Algèbre et géométrie de Jean-Etienne Rombaldi, III.2.d du Cours d'algèbre de Daniel Perrin et V.C de Histoires de groupes et de géométries de Caldero et Germoni)

On considère $p \in \mathcal{P}$ impair et $q = p^n$.

1. Définition : $\mathbb{F}_q^2$ est l'ensemble des $x \in \mathbb{F}_q$ tel qu'il existe $y \in \mathbb{F}_q$ tel que $x = y^2$
2. Théorème : Soit $x \in \mathbb{F}_q$, alors x est un carré dans $\mathbb{F}_q^*$ si et seulement si $x^{\frac{q-1}{2}} = 1$
3. Corollaire : -1 est un carré dans $\mathbb{F}_q$ si et seulement si $q \equiv 1[4]$
4. Application : Il existe une infinité de nombre premiers $p \equiv 1[4]$

5. Définition : On dit que a non multple de p est un résidu quadratique modulo p si $\overline{a}$ est un carré dans $\mathbb{F}_p^*$ et on note $\left(\frac{a}{p}\right) = 1$ si a est résidu quadratique et $\left(\frac{a}{p}\right) = -1$ sinon, appelé symbole de Legendre
6. Proposition : Soit $a \in \mathbb{F}_p^*$, alors $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)[p]$ et $a \in \mathbb{F}_p^* \longmapsto \left(\frac{a}{p}\right) \in \{-1, 1\}$ est l'unique morphisme de groupes non trivial
7. Exemple : $2^{\frac{5-1}{2}} = 2^2 = 4 \equiv -1[5]$, donc 2 n'est pas un résidu quadratique modulo 5
8. Corollaire : Si $n = \pm\prod_{i=1}^{r} p_i^{\alpha_i}$ alors $\left(\frac{n}{p}\right) = (\pm 1)^{\frac{p-1}{2}} \prod_{i=1}^{r} \left(\frac{p_i}{p}\right)^{\alpha_i}$
9. Lemme de Gauss : Soit $a \in \mathbb{Z}$ et $\overline{a}$ l'unite entier tel que $a \equiv \overline{a}[p]$ et $-\frac{p-1}{2} \leq \overline{a} \leq \frac{p-1}{2}$ et l le nombre d'entiers négatifs dans $\{\overline{a}, \overline{2a}, ..., \overline{\frac{p-1}{2}a}$, si p ne divise pas a alors $\left(\frac{a}{p}\right) = (-1)^l$
10. Proposition : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
11. Théorème : Loi de réciprocité quadratique : Soit p et q deux nombres premiers impairs distincts, alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
12. Exemple ! $\left(\frac{11}{83}\right) = 1$ donc 11 est un résidu quadratique modulo 83
13. Exemple : $\left(\frac{219}{383}\right) = 1$ donc 219 est un résidu quadratique modulo 383

4 Utilisation en théorie des groupes

4.1 Théorèmes de Sylow

(Chapitre 1.5 du Cours d'algèbre de Daniel Perrin)

On considère G groupe fini de cardinal $n = p^\alpha m$ avec p diviseur premier de n tel que $p \wedge m = 1$.

1. Définition : Soit H sous-groupe de G, alors on dit que H est un p-sous groupe de Sylow de G si $|H| = p^\alpha$
2. Autrement dit H est un p-groupe est $[G : H]$ est premier avec p
3. Exemple : Soit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et $G = GL_n(\mathbb{F}_p)$, alors $|GL_n(\mathbb{F}_p)| = (p^n - 1)...(p^n - p^{n-1}) = mp^{\frac{n(n-1)}{2}}$ avec $p \wedge m = 1$, et le sous-groupes des matrices triangulaires supérieures de diagonale unitaire est un p-sous groupe de Sylow de G
4. Lemme : Soit H un sous-groupe de G et S un p-sous groupe de Sylow de G, alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-sous groupe de Sylow de H
5. Théorème de Sylow (premier) : G contient au moins un p-sous groupe de Sylow
6. Théorème de Sylow (second) : Soit H p-sous-groupe de G, alors H est inclus dans un p-sous groupe de Sylow de G, de plus les p-sous groupes de Sylow sont tous conjugués et leur nombre k vérifie $k \mid n, k \equiv 1[p]$
7. Corollaire : Soit S un p-sous groupe de Sylow de G, alors $S \triangleleft G$ si et seulement si S est l'unique p-sous groupe de Sylow de G

4.2 Conséquences sur les groupes finis d'un cardinal donné

(Chapitre VI.2 de Eléments de théorie des groupes de Josette Calais)

1. Théorème : Si $|G| = pq$ avec p, q premiers distincts tels que $q \neq 1[p]$ alors G admet un unique p-sous groupe de Sylow
2. Exemple : S_3 admet un unique 3-sous groupe de Sylow, il s'agit du groupes des 3-cycles
3. Théorème : Si G simple non abélien et p diviseur premier de $|G|$ alors le nombre k de p-sous groupes de Sylow de G vérifie $k > 1$
4. Corollaire : Si G simple et p diviseur premier de $|G|$ tel que G admette un unique p-sous-groupe de Sylow alors G est abélien
5. Proposition : Si $|G| = pq$ avec p, q premiers distincts, alors G n'est pas simple
6. Proposition : Si $|G| = pq$ avec p, q premiers distincts tels que $p \neq 1[q], q \neq 1[p]$ alors G est cylique
7. Théorème : Soit p nombre premier impair, si $|G| = 2p$ alors $G \simeq \mathbb{Z}/2p\mathbb{Z}$ ou $G \simeq D_{2p}$