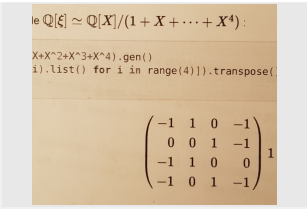


Théorie des nombres effective stream events

Notification Bot 13:45

Public stream created by **F-X. Dehon** . **Description:**

> Description du sujet (sujet 1)

Vous et Notification Bot

Notification Bot 19:32

Marie-Victoire < `user606797@stage-l3-23.zulipchat.com` > a accepté votre invitation à rejoindre Zulip !

core team signups

Notification Bot 19:32

Marie-Victoire just signed up for Zulip. (total: 2)

Vous et Notification Bot

6 AVR.

Notification Bot 10:49

C Cazanave < `user607531@stage-l3-23.zulipchat.com` > a accepté votre invitation à rejoindre Zulip !

core team signups

Notification Bot 10:49

C Cazanave just signed up for Zulip. (total: 3)

Théorie des nombres effective Le sujet

F-X. Dehon MODIFIÉ 15:14

En construction

1. Soient P∈ℤ[X], L le sous-corps de ℂ engendré par les racines complexes de P. Peut on déterminer algorithmiquement le groupe des automorphismes de L comme fonction des coefficients de P ?
   Peut on expliciter les racines lorsque celles ci sont exprimables par radicaux ?
   Notamment :
2. Peut on retrouver les formule de Cardan pour les racines complexes d'un polynômes de degré 3 en calculant le groupe de Galois associé à ce polynôme ?
3. 🆕 A quel point un nombre exprimé avec des radicaux est il "explicite" ? Par exemple comment voit on si le nombre
   $$-\frac{1}{9}\sqrt[3]{351\sqrt{\frac{1}{3}}+170}+\frac{1}{9}\sqrt[3]{351\sqrt{\frac{1}{3}}-170}$$
   est rationnel ?
4. 🆕 Comment décider si le corps de rupture d'un polynôme irréductible (par exemple de degré 3) est déjà le corps de décomposition ? Quelle condition apparait sur le polynôme irréductible de départ ?
5. Peut on expliciter une construction à la règle et au compas d'un nombre complexe lorsqu'une telle construction existe ?

Quelques références :

- Ramis - Warusfel - Moulin, *Cours de mathématiques pures et appliquées vol 1 Algèbre et géométrie*, de boeck 2010, chapitre 2 Corps.
- Notice Wikipedia sur la constructibilité des polygones réguliers

general symboles

F-X. Dehon MODIFIÉ 15:22

ℰℰℱℋℒℛℬℳ ℘ℭ
ℕℤℚ ℝℂ 𝔽𝕂𝕃𝕜
ΓΔΘΛΠΣΦΨΩ
αβγδεζηθικλμνξπρστφϕχψω ζ
∀∃∄⇒⇔⇐⊢
→←↦↝↪↠↺↶⟳ ↿↑↓↔⇄⇉⇇
⟶⟵⟷
⋃⋂∪∩⊔⊂ ⊂⊆⊇⊄∈∉∈∅
∇∆∑⋃⋂⋀
∞± ()+− 0123456789 ()+− 0123456789
‰‰‱ ⅓⅔∘·∫∂⊥⊕⊗×⋀√∛ ‖
×÷ ∧∨ |∤
≝≟≠≈≠≃≠≡≠≤≥≪≺≻
A²⊥
⏳⏱✔ ❗🆕
✍ ❀★
⇝↳ ↿🗘
↗️
📄🗒📖🖥💻
🎥🎬📄📎📝

Egalement formatage LaTeX :

```
$$\begin{pmatrix} 1 & a \\ b & 2 \end{pmatrix}$$
```

$$\begin{pmatrix} 1 & a \\ b & 2 \end{pmatrix}$$

Théorie des nombres effect Lecture dirigée de camarades de mon école sur l… **15 MAI**

Marie-Victoire MODIFIÉ 12:28

(deleted)

Théorie des nombres effective Petite rérérence

Marie-Victoire 12:30

Lecture_dirig_e.pdf

C'est autour de la constructibilité (Sans théorie de Galois) 12:33

Chat stream events

Notification Bot 18:33

Public stream created by **F-X. Dehon** . **Description:**

> discussion - organisation

Chat discussion

F-X. Dehon MODIFIÉ 18:39

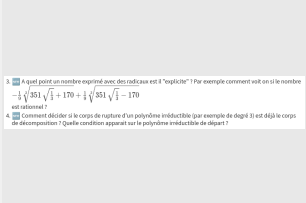
Bonjour,

Une première lecture serait le chapitre 2 "Corps" du livre de Ramis - Warusfel - Moulin "Cours de mathématiques pures et appliquées vol 1 Algèbre et géométrie",

environ 60 pages. Si vous n'avez pas accès à ce livre, je vous transmettrai un extrait.

Le livre de Stewart "Galois theory" est agréable à lire. Ce n'est pas l'approche effective.

A partir de ces lectures, vous pourriez réfléchir aux deux questions "naïves" que j'ai ajoutées sur Zulip :
image.png



Nous pouvons convenir d'un rendez-vous demain ou les jours qui suivent pour en discuter.

C'est mieux d'utiliser un canal pour nos échanges au jour le jour. J'ai créé le canal "Chat" à cet effet. J'y recopierai le texte de cet échange.

Cordialement,
François-Xavier D.

On 5/15/23 12:27, Sylvain Marie-victoire wrote:

> Bonjour,
>
> Étant donné que mon stage a commencé, puis-je avoir d'autres références sur lesquelles travailler ? J'ai d'hors et déjà regardé le lien wikipedia et ait trouvé un rapport de lecture dirigée de mes camarades traitant du sujet. Je mets cela sur le canal zulip.
>
> Bien cordialement,
>
> Sylvain Marie-victoire

[Afficher moins]

Marie-Victoire 18:57

Bonjour, j'ai pu obtenir le livre "cours de mathématiques ...". Je vous propose de convenir d'un rendez vous après demain le temps que j'étudie cette référence, et celle de Stewart si je la trouve.

17 MAI

F-X. Dehon 00:06

Je vous réponds un peu tard.
Je peux discuter avec vous demain mercredi entre 11h et 12h30, mais pas l'après-midi. Sinon probablement vendredi.

Marie-Victoire 10:22

Bonjour, à 12h cela irait ?

F-X. Dehon 11:03

Oui. Je vous enverrai un lien zoom

MODIFIÉ **Discussion du 17mai** 17:38

Essayer de répondre de façon élémentaire à des questions "naïves", comme les deux mises en évidence plus haut, ou bien :
Les extensions de degré 3 sur Q sont elles toutes isomorphes, sinon quelles sont les classes d'isomorphisme ?

"élémentaire" est tout relatif. On prend comme base culturelle la notion de nombre complexe algébrique sur Q, la notion de polynôme minimal et

l'isomorphisme canonique entre Q[X]/(m) (le corps de rupture de m) et le sous corps de C engendré par le nombre algébrique.

A l'opposé de cette démarche il y a la lecture d'un exposé abouti, comme celui de Bourbaki, et son application à des exercices. A ce propos, à quoi ressemblent les exercices de Bourbaki sur notre sujet ?

Marie-Victoire MODIFIÉ 18:52

A la fin de la page 113 du livre "cours de mathématiques ", il est expliqué que le groupe de Galois d'un polynôme $P \in k[X]$ de degré n est inclus dans A_n si et seulement si le discriminant de P est un carré dans k (en caractéristique différente de 2).
Ainsi, si $P \in \mathrm{Q}[X]$ est irréductible, unitaire de degré 3, on note L son corps de décomposition. Comme on a $3 \mid [L : k] \mid 3! = 6$ (Exercice 5 page 85), le groupe $$\Gal(K/k)$$ est de cardinal 3 ou 6, il vaut donc soit A_3 (dans quel cas L est le corps de rupture de P et P de discriminant carré dans $$\mathbb{Q}) soit S_3 (discriminant non carré).
Une méthode algorithmique rapide pour savoir si le corps de rupture de P est Galoisien ou non est donc de se ramener par translation à un polynôme de la forme $X^3 + pX + q$, de calculer son discriminant donné par $-(4p^3 + 27q^2)$ puis de vérifier si c'est un carré ou non, par exemple par une décomposition en facteurs premier du numérateur et du dénominateur.

DÉPLACÉ Mon observation à cet instant: Pour savoir si le corps de décomposition par rapport au corps de rupture était d'indice 2 ou non, on s'est ramené à étudier les racines d'un polynôme de degré 2 (à savoir $X^2 - \Delta$ où Δ est le discriminant de P). D'autre part, à la page 115 est donné une méthode où l'on se ramène à un polynôme de degré 3 pour savoir si un polynôme de degré 4 a un corps de décomposition d'indice divisible par 3 ou non. J'imagine que la théorie utilise la notion de résolvante. 19:31

24 MAI

F-X. Dehon 18:17

Bonjour,
Voulez vous discuter cette semaine ? Ou bien êtes vous dans vos oraux ?

Ce serait bien de donner des exemples de polynôme à coefficients entiers dont le discriminant est un carré puis de comprendre (il y a peut-être qqch à comprendre) ce qui les distingue des polynômes à coefficients entiers génériques.
Également regarder les formules de Cardan pour les racines. Elles font naturellement apparaître une extension de degré 6 contenant les racines (on forme d'abord une racine carré puis une racine cubique). On ne voit probablement pas dans l'expression des racines que l'extension sera de degré 3 plutôt que 6.

Marie-Victoire 21:41

Bonsoir,
Non je ne suis plus dans mes oraux, pouvons nous nous appeler demain ?

F-X. Dehon 21:50

Oui, plutôt le matin, à 11h si ça vous va.

Marie-Victoire 22:05

C'est d'accord alors

28 MAI

F-X. Dehon MODIFIÉ 10:52

Discussion du 25 mai

Sur le point 3 du sujet, on peut l'aborder par exploration de ce qui se prête au calcul algébrique habituel (existance d'une forme normale, algorithme de calcul de la forme normale d'une somme, d'un produit, etc.)

Ainsi a quoi ressemble le calcul algébrique dans le corps des rationnels auquel on a ajouté une seule racine carrée ? Une seule racine n-ième ? Plusieurs radicaux ? Des radicaux itérés ?

Sur le point 4, autre formulation du thème :
Que peut on dire du corps de décomposition de P (de degré 2 puis 3 puis...) à partir de l'expression des racines de P par des radicaux. Quels sont les classes d'isomorphisme de tels corps ? (Qu'est-ce qui caractérise une telle classe).

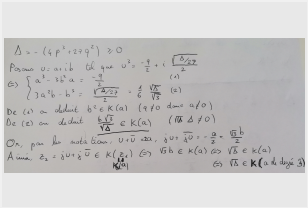
31 MAI

Marie-Victoire 21:33

Bonjour monsieur, pourrions nous nous voir demain ducoup si vous êtes disponible ?

21:36

J'ai reussi à expliquer la carractérisation des groupes de galois par le determinant en degré 3 de manière élementaire. Je n'arrive pas à faire à faire les degrés plus haut, je lis donc le stewart.
385da426-4706-470a-b466-be957c1da4c6.jpg



F-X. Dehon 22:31

Bonjour,
Comme la semaine dernière à 11h sur Zoom ?

1 JUIN

Marie-Victoire 04:35

Bonjour, d'accord parfait

10:29

Re bonjour, excusez moi mais finalement je ne vais pas pouvoir être présent en distanciel, êtes vous disponible la semaine prochaine ?

F-X. Dehon 10:33

Oui, lundi vers 15h30 ou mardi.
Avez vous des nouvelles sur votre séjour à Nice ?

Marie-Victoire 10:34

Oui en fait je suis à Nice en ce moment même, c'est là mes problèmes de connexion

F-X. Dehon 10:34

Mais vous pouvez venir au labo alors.

Marie-Victoire 10:36

Effectivement, je pensais vous avoir dit que je venais en debut de semaine et que vous vouliez que l'on reste en distanciel avec votre message d'hier.

10:36

J'y serai cet après midi, ce sera dans quel batiment ?

F-X. Dehon 10:39

Non, il n'y a pas de raison.
Je suis dans le bâtiment LJAD, 2ème étage dans le campus Valrose. Venez avec

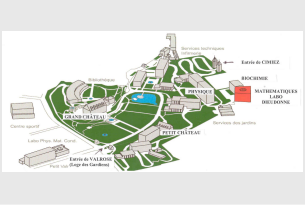
une carte étudiant et dites que vous avez rdv avec moi : il y a un filtrage à l'entrée du campus.

Marie-Victoire 10:41

D'accord quelque chose comme 14h vous irait ?

F-X. Dehon MODIFIÉ 10:44

plan_campus.jpg
Bâtiment en rouge sur le plan



Oui, entre 14h et 17h. 10:48

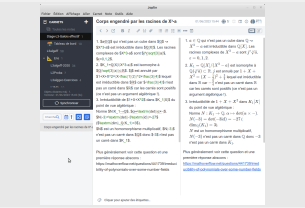
Marie-Victoire 10:48

D'accord parfait

general Prise de notes

F-X. Dehon MODIFIÉ 16:05

J'utilise Joplin comme application de prise de notes Markdown - Latex. Il y en a d'autres comme Obsidian
image.png



On peut comme dans Zulip facilement insérer des images, notamment des photo-scan prises avec smartphone et corrigées avec Office Lens.

Théorie des nombres effective Factorisation des polynômes

F-X. Dehon MODIFIÉ 16:14

Factorisation dans ℚ(α)[X] où α est un nombre complexe algébrique selon la méthode de Kronecker
Article de S. Landau dans l'espace Dropbox partagé

[SIAM Journal on Computing 1985 feb vol 14 iss 1] Landau, Susan

Théorie des nombres effective Bibliographie

F-X. Dehon 16:40

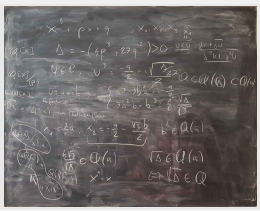
Dossier partagé en lecture-écriture sur Dropbox (pour notre seul usage !)
Pour l'instant : Un extrait du livre de Ramis-Warusfel-Moulin, Bourbaki Algèbre 4-7, un article de S. Landau sur la factorisation des polynômes.

Chat discussion

F-X. Dehon MODIFIÉ 17:22

Discussion du 1er juin

Sylvain : $X^3 + pX + q$ supposé irréductible et de discriminant $\Delta = -(4p^3 + 27q^2) > 0$, alors son corps de décomposition est égal à son corps de rupture ssi Δ est un carré dans $\mathbb{Q}$, cf ce message dans le canal #Chat.
tableau.jpg



Questions :

- Comment décider si un élément d'une extension $\mathrm{Q}[X]/(P)$ est un carré ou pas ? Plus généralement comment factoriser un polynôme à coefficients dans $\mathrm{Q}[X]/(P)$? Cf article de S. Landau.
- (discussion du 25 mai) : quels sont les couples p,q∈$\mathbb{Q}$ tels que Δ soit un carré dans $\mathbb{Q}$?

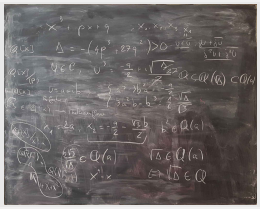
Construction du corps de décomposition :
On suit la preuve d'existence : $P \in \mathrm{Q}[X]$ de degré ≥1. On calcule (plutôt que seulement considérer) un facteur irréductible Q_1 de P ; on forme $K_1 = \mathrm{Q}[X_1]/(Q_1(X_1))$; P s'écrit $(X - X_1)P_1$ dans $K_1[X]$; on recommence avec P_1 dans $K_1[X]$.
On a besoin d'un algorithme de factorisation dans les $K_i[X]$.

[SIAM Journal on Computing 1985 feb vol. 14 iss. 1] Landau, Susan

Vous et F-X. Dehon

F-X. Dehon 17:36

2023_06_01 17_35 Office Lens.jpg



Théorie des nombres effective Factorisation des polynômes **6 JUIN**

F-X. Dehon MODIFIÉ 17:43

Factorisation dans $\mathrm{Q}[X]$ et $\mathrm{Q}(\alpha)[X]$

1. Méthode de Schubert-Kronecker pour la factorisation dans $\mathrm{Q}[X]$ par factorisation des valeurs prises dans Z et interpolation. Mise en perspective historique par Mignote-Stefanescu.
Mignotte-Stefanescu-RHM_2001__7_1_67_0.pdf

2. Méthode de factorisation dans $\mathrm{Q}(\alpha)[X]$ exposée dans le livre de van der Waerden
Extrait van-der-Waerden-section-42.pdf
A comparer avec l'exposé de S. Landau
3. Article de synthèse de Kaltofen
Kaltofen-Factorization-of-Polynomial-Ka82_survey.pdf
Mentionne mais n'expose pas les méthodes 1-2 ci-dessus, cite Trager-76
Trager-Algebraic-factoring-76.pdf
Expose plutôt les méthodes p-adiques : Berlekamp et lemme de Hensel.

4. Exposé de Knuth The Art of Computer Programming vol.2 section 4.6.2 : notes historiques et méthodes p-adiques pour $\mathrm{Q}[X]$.

Rq : la méthode de Kronecker s'applique telle quelle à $D[X]$ où D est un anneau intègre tel que tout élément non nul n'a qu'un nombre fini de diviseurs, et donc récursivement à $\mathrm{Z}[X_1, ..., X_n]$.
Elle ne s'applique pas telle quelle à $\mathrm{Z}[\sqrt{5}]$: le groupe des unités est infini.

Vous et Marie-Victoire

F-X. Dehon 19:27

Bonjour,
Où en êtes vous depuis jeudi ?
Je serai peu disponible demain, seulement le matin avant midi, mais vous pouvez aussi essayer de voir mon collègue Christophe (postez lui un message pour cela). Je serai beaucoup plus disponible jeudi et vendredi matin.
Cordialement.

Chat discussion

F-X. Dehon 19:44

J'ai posté cet après-midi des références sur la factorisation selon l'approche de Kronecker, maintenant dans le canal #Théorie des nombres effective > Factorisation des polynômes.
On pourrait par exemple tester par les méthodes indiquées l'irréductibilité de $(X^4 - 2)//(X - \sqrt[4]{2})$ dans $\mathrm{Q}(\sqrt[4]{2})$.

Vous et Marie-Victoire

Marie-Victoire MODIFIÉ 21:06

Bonjour,
J'*essaye* de m'avancer dans les lectures de l'article de Suzan Landau et du livre de Bourbaki. Pour ce qui est de l'article de Landau je suis bloqué à la demonstration de la proposition 1.2: l'ensemble des entiers algébriques de $Q[\alpha]$ est contenu dans $\frac{1}{d}Q[\alpha]$ où d diviserait le discriminant du polynome minimal de α. Je n'ai trouvé ca nul part ailleurs que dans cet article.

Chat discussion AUJOURD'HUI

Marie-Victoire 21:42

Bonsoir, seriez vous disponible vendredi ?

F-X. Dehon 21:54

Oui, mais seulement le matin entre 9h et 12h.
Ne pourrez vous venir demain également ?

Marie-Victoire 21:55

Oui demain serait possible aussi, vous êtes disponible le matin ou l'après midi

F-X. Dehon 22:05

Toute la journée (de 9h à 17h). On peut se voir au café de 10h par exemple.

Marie-Victoire 22:30

Très bien alors à demain 10h

AUJOURD'HUI

Marie-Victoire 13:14

Bonjour monsieur, je ne vous trouve pas dans votre bureau, où seriez vous ?

F-X. Dehon 13:16

Ecrivez vous maintenant à 13h15 ? Ou bien je reçois le message avec retard ?
Je serai dans mon bureau vers 13h45

Marie-Victoire 13:26

oui je vennais de l'ecrire

F-X. Dehon MODIFIÉ 16:29

Discussion du 8 juin

0. [S. Landau] D'où vient cette référence ? Réponse : de ma recherche documentaire sur Internet qui m'a mené à cette page personnelle , laquelle fait référence à cette page sur MathOverFlow.
L'article de S. Landau porte en fait sur la complexité (temps polynomial) plutôt que l'algorithme même, lequel semble repris de celui exposé dans [van der Waerden]. Plutôt lire ce dernier, voir #Théorie des nombres effective > Factorisation des polynômes

1. Norme de $f \in \mathrm{Q}(\alpha)[X]$: Différents exposés.
La composée $\mathrm{Q} \xrightarrow{f} \mathrm{Q}(\alpha) \xrightarrow{N} \mathrm{Q}$ est elle bien une fonction polynômiale, égale à $N(f)$?

2. Groupe des automorphismes de $K = \mathrm{Q}(\alpha)$: Soit m le polynôme minimal de α. L'application $\mathrm{Aut}(K) \longrightarrow R = \{\text{racines de } m \text{ dans } K\}$, $\varphi \mapsto \varphi(\alpha)$ est une bijection d'ensembles. $\mathrm{Aut}(K)$ est donc un sous groupe de S_R de même cardinal que R et agissant transitivement sur R. Quel peut il être ?
Lien avec le théorème de l'élément primitif (tout groupe de Galois est de la forme $\mathrm{Aut}(\mathrm{Q}(\alpha))$ pour des α (ou m_α) particuliers), expérimentations Sagemath.

3. $K_1 = \mathrm{Q}(\alpha)$, $K_2 = K_1(\beta)$. Comment s'écrit $\mathrm{Aut}_{\mathrm{Q}}(K_2)$ en fonction de $\mathrm{Aut}_{\mathrm{Q}}(K_1)$ et $\mathrm{Aut}_{K_1}(K_2)$?

Plus directement : $\sum_n \circlearrowright \mathrm{Q}[X_1, \ldots, X_n] \longrightarrow \mathrm{Q}(\alpha_1, \ldots, \alpha_n) = K$, où $\alpha_1, \ldots, \alpha_n$ sont les racines dans K d'un polynôme irréductible de $\mathrm{Q}[X]$, de noyau I.
Comment se décrit I ? Comment décider si un élément de $\sum_n$ (une permutation de $X_1, \ldots, X_n$) laisse stable I ?

4. Calcul algébrique avec les radicaux
Lire par exemple cet article de S. Landau
S-Landau-Nested-Radical-BF03024284.pdf

5. Références calculabilité, algorithmes efficients de calcul

- G. Dowek, Les démonstrations et les algorithmes, 2010
- Bostan &all, Algorithmes Efficaces en Calcul Formel, 2018, https://hal.archives-ouvertes.fr/AECF/
- D. Knuth, The Art of Computer Programming, vol.2 notamment. L'algorithme LLL n'est pas référencé dans la 1ère édition (1969) mais l'est dans la 3ème (1998) !