Sujets donnés en TER

TER numéro 1

Petits groupes simples finis

Introduction

Le but du TER est d'étudier les plus petits groupes finis simples non triviaux qui sont de cardinaux 60 et 168.

Références principales :

[B] Berger, *Géométrie*, Nathan ou Cassini.

[D] Dieudonné, *La géométrie des groupes classiques*, Springer.

[H] Hartshorne, *Algebraic geometry*, Springer (beaucoup plus difficile).

[P] Perrin, *Cours d'algèbre*, Ellipses.

Un groupe G est dit simple s'il n'a pas d'autres sous-groupes distngués que lui-même et $\{1\}$. C'est une notion essentielle pour la classification des groupes (finis ou non). Dans le cas des groupes finis on a une classification complète de tous les groupes simples (mais cela prend environ 10000 pages de démonstration, ce qui est un peu long pour un TER). Il y a déjà les groupes dits triviaux i.e. les $\mathbf{Z}/p\mathbf{Z}$ avec p premier. Les plus petits non triviaux sont le groupe $\mathfrak{A}_5$ (d'ordre 60) des permutations paires d'un ensemble à 5 éléments et le groupe $PSL(2, \mathbf{F}_7)$ d'ordre 168.

1.1 Ils sont simples

1.1.1 Le cas de $\mathfrak{A}_5$

Voir [P] chapitre I.

1.1.2 Le cas de PSL

Voir [P] chapitre IV ou [D] pour la méthode d'Iwasawa..

1.2 Ce sont les plus petits

1.2.1 $\mathfrak{A}_5$ est le plus petit, PSL le deuxième

Montrer qu'il n'y a pas de groupe simple d'ordre < 60 autre que les triviaux. Cela doit se faire avec les exercices de [P] ch. I et notamment avec Sylow et les théorèmes de Burnside. On peut aussi tout faire à la main (me consulter).

Montrer qu'il n'y a pas de groupe simple d'ordre n avec $60 < n < 168$.

1.2.2 $\mathfrak{A}_5$ est seul à 60

Tout groupe simple d'ordre 60 est isomorphe à $\mathfrak{A}_5$. Voir [P] exercice I F.6 ou, mieux, me consulter pour élaborer une démonstration élémentaire (compter les Sylow, puis regarder le centralisateur d'un élément d'ordre 2).

1.2.3 $PSL(2, \mathbf{F}_7)$ est seul à 168

Tout groupe simple d'ordre 168 est isomorphe à $PSL(2, \mathbf{F}_7)$, cf. [P] IV 5.3. Cas particulier du groupe $PSL(3, \mathbf{F}_2)$.

1.3 Variantes géométriques

Les deux groupes précédents se rencontrent "dans la nature", comme groupes d'automorphismes de structures simples.

1.3.1 Le cas de $\mathfrak{A}_5$

Le groupe des rotations du dodécaèdre régulier (ou de l'icosaèdre régulier) est isomorphe à $\mathfrak{A}_5$. (Voir [B] ou me consulter ; on peut donner de nombreuses démonstrations de ce fait.)

Prolongement : déterminer les sous-groupes finis de $O^+(3, \mathbf{R})$.

1.3.2 Le cas de $PSL(2, \mathbf{F}_7)$

Pour une courbe projective complexe C de genre $g \geq 3$ on montre que le groupe des automorphismes de C est de cardinal $\leq 84(g-1)$, cf. [H]. Pour

$g = 3$, le maximum est atteint pour la quartique de Klein, c'est-à-dire la courbe plane projective K d'équation $X^3Y + Y^3T + T^3X = 0$ et le groupe des homographies de $\mathbf{P}^2(\mathbf{C})$ qui conservent K est le groupe simple d'ordre 168. (Me consulter)

TER numéro 2

Anneaux d'entiers des corps quadratiques imaginaires

Introduction

Le but du TER est d'étudier les anneaux d'entiers des corps $\mathbf{Q}(i\sqrt{d})$ où d est un entier > 0, sans facteur carré.

Références principales :

[BS] Borevitch-Shafarevitch, *Théorie des nombres*, Gauthier-Villars.
[S] Samuel, *Théorie algébrique des nombres*, Hermann.
[ST] Stewart-Tall, *Algebraic number theory*, Chapmann-Hall.
[P] Perrin, *Cours d'algèbre*, Ellipses.

Si A_d est l'anneau des entiers de $\mathbf{Q}(i\sqrt{d})$ il s'agit d'étudier les propriétés arithmétiques de cet anneau (est-il intégralement clos, de Dedekind, factoriel, principal, euclidien, etc.) Il y a de nombreuses applications de cette théorie, notamment l'étude des formes quadratiques à coefficients entiers, les équations diophantiennes de degré 2, la recherche des entiers de la forme $x^2 + dy^2$, etc.

2.1 Anneau des entiers

Premières choses à comprendre : ce que signifie que x est entier sur un anneau A, ce qu'est un anneau intégralement clos et la clôture intégrale d'un anneau qui ne l'est pas et pourquoi factoriel implique intégralement clos.

Calculer l'anneau A_d des entiers de $\mathbf{Q}(i\sqrt{d})$ (cf. [S] ou [ST], c'est $\mathbf{Z}[i\sqrt{d}]$ si $d \equiv 1, 2 \pmod 4$, et $\mathbf{Z}\left[\dfrac{1+i\sqrt{d}}{2}\right]$ si $d \equiv 3 \pmod 4$). On posera $\alpha = \dfrac{1+i\sqrt{d}}{2}$.

On a besoin pour cela d'utiliser la norme et la trace. Noter que $N(zz') = N(z)N(z')$. Écrire des formules de calcul de la norme de $a + ib\sqrt{d}$ ou de $a + b\alpha$, avec $a, b \in \mathbf{Q}$ (ou $\mathbf{Z}$).

Comprendre pourquoi A_d est alors un anneau de Dedekind (cf. [S], [ST]) et pourquoi, pour un tel anneau, factoriel équivaut à principal.

2.2 Etude de l'anneau A_d

2.2.1 Les inversibles

2.2.1 Proposition. *On a $A_d^* = \{+1, -1\}$ sauf pour $d = 1$ et $d = 3$.*

(Indication : regarder la norme et ses valeurs possibles, montrer que $N(z)$ est $\geq d$ ou $\geq \dfrac{1+d}{4}$ pour $z \notin \mathbf{Z}$). Etudier les cas particuliers.

2.2.2 Les irréductibles

2.2.2 Proposition. *Un nombre premier p de $\mathbf{Z}$ est réductible dans A_d si et seulement si c'est une norme. Le nombre 2 est irréductible pour d assez grand.*

2.2.3 Corollaire. *1) Pour $d \equiv 1, 2 \pmod 4$, et $d > 2$, A_d n'est pas factoriel. 2) Pour $d \equiv -1 \pmod 8$ et $d > 7$, A_d n'est pas factoriel.*

(Indication : cf. [P] II 3.19, regarder l'idéal (p) et montrer qu'il n'est pas premier en considérant le quotient $A_d/(p)$.)

Il reste donc essentiellement à regarder le cas $d \equiv 3 \pmod 8$.

2.2.3 Anneaux euclidiens

2.2.4 Théorème. *L'anneau A_d est euclidien si et seulement si on a $d = 1, 2, 3, 7, 11$.*

Indication : cf. les références, en particulier [P] II 3.f et II 5.

2.2.4 Principalité

2.2.5 Théorème. *L'anneau A_d est principal si et seulement si $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$.*

Attention, ce résultat, dans son intégralité, est hors de portée (il date de la fin des années 60). On se contentera de montrer que ces anneaux sont principaux (par la méthode des tiroirs ou des réseaux, me consulter) et que, par exemple, il n'y en a pas d'autres que ceux annoncés pour $d \leq 200$ ou $d \leq 2000$ ou ... (me consulter pour des détails).

2.2.5 Applications

- Comprendre pourquoi $n^2 + n + 41$ est premier pour $0 \leq n \leq 39$.
- Etudier les entiers de la forme $x^2 + 5y^2$, avec $x, y \in \mathbf{Z}$.

TER numéro 3

La loi de réciprocité quadratique

3.1 Introduction

Le but du TER est d'étudier les carrés des corps finis $\mathbf{F}_q$ et de prouver notamment la loi de réciprocité quadratique.

Références principales :

[S] Serre, *Cours d'arithmétique*, Hermann.
[ST] Stewart, *Galois theory*, Chapmann et Hall.
[P] Perrin, *Cours d'algèbre*, Ellipses.

La recherche des carrés dans les corps finis est utile dans nombre de questions d'algèbre (par exemple le quotient k^*/k^{*2} intervient dans l'étude du groupe linéaire, des formes quadratiques, etc., cf. [P] Ch. IV, V et VIII). Elle est aussi essentielle dans de nombreuses questions d'arithmétique (par exemple la recherche des entiers de la forme $x^2 + dy^2$). On pourra expliquer le problème de la recherche des conditions nécessaires pour $d = 5$.

3.2 Les carrés de $\mathbf{F}_q$

Noter déjà le cas particulier de la caractéristique 2 : dans un corps fini de caractéristique 2 tout élément est un carré (c'est Frobenius). On écarte définitivement ce cas.

Soit $\mathbf{F}_q$ un corps fini de cardinal $q = p^n$ (où p est un nombre premier $\neq 2$).

On a deux suites exactes fondamentales (cf. [S] ou [P]) :

$$1 \to \{\pm 1\} \to \mathbf{F}_q^* \xrightarrow{u} \mathbf{F}_q^{*2} \to 1 \tag{1}$$

avec $u(x) = x^2$. Cette suite donne le nombre de carrés non nuls : $(q-1)/2$.

$$1 \to \mathbf{F}_q^{*2} \to \mathbf{F}_q^* \xrightarrow{v} \{\pm 1\} \to 1 \tag{2}$$

avec $v(x) = x^{\frac{q-1}{2}}$.

Cette deuxième suite donne un critère pour que x soit un carré, à savoir $x^{\frac{q-1}{2}} = 1$. Par exemple, -1 est un carré si et seulement si on a $q \equiv 1 \pmod 4$. Pour d'autres démonstrations, voir [P].

Dans le même ordre d'idées on a :

3.2.1 Proposition. *Le nombre* 2 *est un carré de* $\mathbf{F}_q$ *si et seulement si on a* $q \equiv \pm 1 \pmod 8$.

Indication : on notera que si ζ est une racine primitive huitième de 1 dans un corps k on a $(\zeta + \zeta^{-1})^2 = 2$, penser au cas de $\mathbf{C}$ ou noter qu'on a $\zeta^4 + 1 = 0$.

A partir de maintenant on suppose que q est un nombre premier p. Soit $x \in \mathbf{F}_p^*$. Le symbole de Legendre : $(\frac{x}{p})$ est défini par la formule $(\frac{x}{p}) = x^{\frac{p-1}{2}}$. La suite exacte (2) nous indique que le symbole de Legendre est un homomorphisme en x (on dit aussi un caractère) et que x est un carré si et seulement si $(\frac{x}{p}) = 1$. On a vu comment calculer ce symbole lorsque $x = -1$ et $x = 2$. Il reste à calculer $(\frac{n}{p})$ lorsque n est un nombre premier impair. C'est l'objet de la loi de réciprocité quadratique, cf. [S] pour deux preuves autres que celle que je propose.

3.2.2 Théorème. (Loi de réciprocité quadratique). *Soient* n *et* p *deux nombres premiers impairs distincts. On a la formule :*

$$(\frac{n}{p}) = (-1)^{\frac{(n-1)(p-1)}{4}} \ (\frac{p}{n}).$$

(Traduire le signe en termes de congruences modulo 4 et donner un exemple numérique).

3.3 Démonstration de la loi de réciprocité

3.3.1 Rappels sur la théorie de Galois

Lire le chapitre III de [P] pour le b-a ba sur les extensions de corps. Si $K \subset L$ est une extension (finie) de corps (on la note aussi L/K), le groupe de Galois de L sur K, $G = \mathrm{Gal}(L/K)$, est le groupe des automorphismes de corps de L qui laissent fixe K.

On renvoie à Stewart pour les fondements de la théorie (il y a besoin de très peu de choses ici). Cette théorie marche bien lorsque l'extension (finie) L/K est **galoisienne**. Cela englobe deux conditions :

• L/K séparable, condition toujours réalisée en caractéristique 0 ou pour les corps finis, donc toujours vraie ici,

• L/K normale qui signifie que L est un corps de décomposition, $L = D_K(P)$, cf. [P]. Cette condition est toujours vraie sur un corps fini. Dans ce cas on pose $\mathrm{Gal}_K(P) = \mathrm{Gal}(L/K)$ (voire simplement $\mathrm{Gal}(P)$).

Dans le cas galoisien on a le théorème de Galois qui établit une bijection entre sous-groupes de G et sous-extensions de L/K, cf. [ST]. En particulier, $\mathrm{Gal}(L/K)$ est un groupe fini et on a $|\mathrm{Gal}(L/K)| = [L : K]$. De plus, K est exactement l'ensemble des éléments de L fixés par le groupe de Galois.

3.3.2 Galois sur un corps fini

Posons $q = p^n$. On a alors $\mathbf{F}_q = D_{\mathbf{F}_p}(X^q - X)$, avec $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

3.3.1 Proposition. *Le groupe de Galois* $\mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_p)$ *est cyclique d'ordre* n *engendré par l'homomorphisme de Frobenius* F *défini par* $F(x) = x^p$.

3.3.3 Galois pour une extension cyclotomique

Voir [P] Ch. III pour des détails sur les polynômes cyclotomiques Φ_n et leur degré $\varphi(n)$. Si n est premier on a $\varphi(n) = n - 1$. Soit K un corps et $K_n = D_K(X^n - 1) = D_K(\Phi_n)$ (on suppose n premier avec la caractéristique de K).

3.3.2 Proposition. *On a un homomorphisme injectif* $\mathrm{Gal}_K(\Phi_n) = \mathrm{Gal}(K_n/K) \to (\mathbf{Z}/n\mathbf{Z})^*$.

(Un élément du groupe est déterminé par l'image de ζ, racine primitive n-ème de 1. Regarder quelle peut être cette image et en déduire la structure de groupe.)

3.3.3 Proposition. *Avec les notations précédentes, si on décompose Φ_n en produit de polynômes irréductibles sur K : $\Phi_n = P_1 \cdots P_r$, les P_i ont tous même degré d et on a $d = [K_n : K] = |\operatorname{Gal}(\Phi_n)|$. On a $\varphi(n) = rd$.*

(C'est une histoire de polynôme minimal).

3.3.4 Corollaire. *Énoncer et prouver un critère pour que Φ_n soit irréductible.*

3.3.4 Galois et permutations

Voici une propriété importante du groupe de Galois qui a trait aux conjugués :

3.3.5 Proposition. *Soit L/K une extension galoisienne et soient $x, y \in L$. Les conditions suivantes sont équivalentes :*
1) il existe $\sigma \in \operatorname{Gal}(L/K)$ tel que $y = \sigma(x)$,
2) x et y ont même polynôme minimal sur K (cf. [P]).
On dit alors que x et y sont conjugués sur K.

Soient K un corps et $P \in K[X]$ un polynôme de degré m. Posons $L = D_K(P)$ et supposons que P a m racines distinctes $x_1, \cdots, x_m$ dans L (on dit alors que P est séparable et l'extension L/K est galoisienne). Alors, on voit aussitôt que le groupe de Galois $G = \operatorname{Gal}(P) := \operatorname{Gal}(L/K)$ permute les x_i et on peut l'identifier à un sous-groupe du groupe symétrique $\mathfrak{S}_m$. Précisément, si $P = P_1 \cdots P_r$ avec les P_i irréductibles sur K, la proposition 6 montre que les orbites dans l'action de G sur les x_i sont exactement les paquets de racines d'un même P_j.

3.3.6 Corollaire. *Soit $P \in K[X]$ un polynôme séparable de degré m, soient $x_1, \cdots, x_m$ ses racines et soit $P = P_1 \cdots P_r$ sa décomposition en produit d'irréductibles, avec $\deg P_i = d_i$. Supposons $\operatorname{Gal}(P)$ cyclique engendré par σ. Alors, comme permutation des x_i, l'élément σ est produit de r cycles disjoints d'ordre d_i.*

3.3.5 Discriminant

On a vu que le groupe de Galois d'un polynôme séparable P de degré m s'injecte dans $\mathfrak{S}_m$. Pour savoir s'il s'injecte dans $\mathfrak{A}_m$ (les permutations paires), on introduit le discriminant $\Delta(P)$:

3.3.7 Définition. *Soient $x_1, \cdots, x_m$ les racines de P dans $L = D_K(P)$. On pose*

$$\delta(P) = \prod_{i<j} x_i - x_j \qquad \text{et} \qquad \Delta(P) = \delta(P)^2.$$

Le nombre $\Delta(P)$ est dans K^* et s'appelle le discriminant de P.

3.3.8 Proposition. *On a $\mathrm{Gal}(P) \subset \mathfrak{A}_m$ si et seulement si $\Delta(P)$ est un carré de K, i.e. si $\delta(P)$ est dans K.*

La proposition suivante donne des moyens de calculer le discriminant. On l'applique ensuite dans le cas cyclotomique.

3.3.9 Proposition. *Soit P' le polynôme dérivé de P et soient $y_1, y_2, \cdots, y_{m-1}$ ses racines dans une extension de K. On a les formules :*

1) $\Delta(P) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} P'(x_i)$,

2) $\Delta(P) = (-1)^{n(n-1)2}\ n^n \prod_{j=1}^{n-1} P(y_j)$.

3.3.10 Proposition. *Soit n un nombre premier. Le discriminant de Φ_n vaut*

$$\Delta(\Phi_n) = (-1)^{\frac{n(n-1)}{2}}\ n^{n-2}.$$

(Utiliser la formule $X^n - 1 = (X-1)\Phi_n$, valable pour n premier et la première formule de la Prop. 10).

3.3.11 *Remarque.* Comme n est impair, on voit que $\Delta(\Phi_n)$ est un carré dans K si et seulement si $(-1)^{n(n-1)/2}\ n$ est un carré dans K.

3.3.12 Corollaire. *Soient p et n deux nombres premiers impairs distincts. On a $\mathrm{Gal}_{\mathbf{F}_p}(\Phi_n) \subset \mathfrak{A}_{n-1}$ si et seulement si $(-1)^{n(n-1)/2}\ n$ est un carré de $\mathbf{F}_p$.*

3.3.6 Cyclotomie et corps finis

3.3.13 Proposition. *Soit p premier et n un entier tel que p ne divise pas n. On décompose Φ_n en produit de r polynômes irréductibles sur $\mathbf{F}_p$, tous de degré d. Alors le nombre d est l'ordre de p dans $(\mathbf{Z}/n\mathbf{Z})^*$.*

Cela résulte des propositions précédentes (2,3,4) en regardant l'extension $\mathbf{F}_p \subset \mathbf{F}_q = D_{\mathbf{F}_p}(\Phi_n)$, donc $q = p^d$. Il faut comprendre que Frobenius c'est le p de $(\mathbf{Z}/n\mathbf{Z})^*$.

Le point suivant est l'une des clés de la démonstration de la loi de réciprocité :

3.3.14 Corollaire. *On suppose p et n premiers impairs distincts. Alors, avec les notations précédentes, p est un carré de $\mathbf{F}_n = \mathbf{Z}/n\mathbf{Z}$ si et seulement si r est pair.*

Au passage, voici quelques conséquences de la proposition 14 (qui nous éloignent un peu de notre sujet mais ...) (cf. [P]) :

3.3.15 Corollaire. *On a les équivalences :*
1) Φ_n *est scindé sur* $\mathbf{F}_p$*,*
2) Φ_n *a une racine dans* $\mathbf{F}_p$*,*
3) $p \equiv 1 \pmod{n}$*.*

3.3.16 Corollaire. *Soit* $n \geq 2$*, il existe une infinité de nombres premiers* $\equiv 1 \pmod{n}$*.*

3.3.17 Corollaire. *On a les équivalences :*
1) $(\mathbf{Z}/n\mathbf{Z})^*$ *est un groupe cyclique,*
2) $n = 2, 4, p^\alpha$ *ou* $2p^\alpha$ *avec* p *premier impair,*
3) il existe p *premier tel que* Φ_n *est irréductible sur* $\mathbf{F}_p$*.*

3.3.7 Frobenius et décomposition en cycles

Le résultat suivant est conséquence du corollaire 7 :

3.3.18 Corollaire. *Soit* p *un nombre premier impair et* n *un entier tel que* p *ne divise pas* n*. Posons* $\mathbf{F}_q = D_{\mathbf{F}_p}(\Phi_n)$ *et soit* F *l'homomorphisme de Frobenius de* $\mathbf{F}_q$*. Alors, si* d *est le degré des facteurs irréductibles de* Φ_n *sur* $\mathbf{F}_p$*,* F*, vu comme élément de* $\mathfrak{S}_{\varphi(n)}$ *est un produit de* r *cycles disjoints d'ordre* d*. (Rappelons qu'on a* $rd = \varphi(n)$*).*

Supposons maintenant que n est un nombre premier (impair), de sorte que $\varphi(n) = n - 1 = rd$ est pair. On a alors :

3.3.19 Corollaire. *Le groupe de Galois* $\mathrm{Gal}(\Phi_n)$ *sur* $\mathbf{F}_p$ *est contenu dans le groupe alterné* $\mathfrak{A}_{n-1}$ *si et seulement si* $r = (n-1)/d$ *est pair, c'est-à-dire encore si* p *est un carré de* $\mathbf{F}_n$*.*

3.3.8 Conclusion

On considère deux nombres premiers impairs distincts p et n. On regarde le polynôme cyclotomique Φ_n sur le corps $\mathbf{F}_p$. On montre la loi de réciprocité en traduisant de deux façons différentes la condition $\mathrm{Gal}(\Phi_n) \subset \mathfrak{A}_{n-1}$.

TER numéro 4

Résolution par radicaux

4.1 Introduction

Le but du TER est de montrer le théorème de Galois qui fait le lien entre équations résolubles et groupes résolubles, et de montrer notamment que l'équation générale de degré $n \geq 5$ n'est pas résoluble par radicaux. On travaillera exclusivement en caractéristique 0.

Références principales :

[ST] Stewart I., *Galois theory*, Chapmann et Hall.

[VdW] Van der Waerden, *Modern Algebra.*

[H] Hadlock C.-R., *Field theory and its classical problems*, The Carus Mathematical Monographs, 19, 1978.

[P] Perrin *Cours d'algèbre*, Ellipses.

4.2 Extensions radicales, extensions résolubles

4.2.1 Définition. *Une extension $K \subset L$ est dite* **radicale** *si on a une tour : $K = K_0 \subset K_1 \subset \cdots \subset K_n = L$ avec, pour tout $i = 1, \ldots, n$, $K_i = K_{i-1}(\alpha_i)$ où α_i vérifie $\alpha_i^{n_i} = a_i \in K_{i-1}$, avec $n_i \in \mathbf{N}^*$. (Autrement dit, α_i est un radical.)*

4.2.2 Définition. *Une extension $K \subset L$ est dite* **résoluble** *(sous-entendu par radicaux), s'il existe une extension M de L telle que $K \subset M$ soit radicale.*

4.2.3 Définition. *Soit $P \in K[X]$ un polynôme. On dit que l'équation $P(x) = 0$ est* **résoluble par radicaux** *si l'extension $K \subset D_K(P)$ est résoluble.*

Il faut comprendre la différence entre radicale et résoluble, par exemple à partir de l'étude du cas de l'équation de degré 3.

4.3 Exemple 1 : l'équation de degré 3

Il s'agit d'étudier le cas de l'équation $P(x) = x^3 + px + q = 0$, avec $p, q \in K$, et de comprendre la méthode de Cardan en termes de théorie de Galois. On suppose P irréductible sur K. On note x_1, x_2, x_3 les racines de l'équation et on pose $L = K(x_1, x_2, x_3) = D_K(P)$. Le groupe de Galois permute les racines x_1, x_2, x_3. On élucidera en particulier les points suivants :

• Le lien entre le fait que le groupe de Galois soit $\mathfrak{S}_3$ ou $\mathfrak{A}_3$, le fait que le discriminant $\Delta = -4p^3 - 27q^2$ soit un carré de K, et le fait le degré $[L : K]$ vaille 3 ou 6.

• On pose $M = K(\sqrt{\Delta})$. Pour résoudre l'équation par radicaux, il suffit de montrer qu'on a $L = M(y)$, avec y "radical" : y vérifiant $y^3 = a$, avec $a \in M$. On montrera que si on a un tel y, le corps M contient une racine cubique de 1, notée j.

• On adjoint j à K si elle n'y est pas déjà. On se convaincra que $y = x_1 + jx_2 + j^2x_3$ est un candidat plausible pour y. On utilisera aussi $z = x_1 + j^2x_2 + jx_3$ et $x_1 + x_2 + x_3$ pour calculer les x_i. Les éléments y^3 et z^3 sont dans M, et $y^3 + z^3$ et y^3z^3 sont dans K et ils se calculent à partir de p et q. On retrouve ainsi la méthode de Cardan.

4.4 Exemple 2 : l'équation de degré 4

Me consulter sur ce thème.

Le point essentiel est de repérer le corps fixe M par le sous-groupe V_4 de $\mathfrak{S}_4$. Un générateur de ce corps est $x_1x_2 + x_3x_4$. Cet élément vérifie une équation de degré 3 : la "résolvante" de l'équation.

On retrouve ainsi la résolution de l'équation de degré 4 par la méthode de Ferrari. Interprétation en termes de pinceaux de coniques.

4.5 Retour à la théorie

4.5.1 Généralités

4.5.1 Proposition. *Soient $K \subset L \subset M$ des extensions.*
1) Si $K \subset M$ est radicale, $L \subset M$ aussi.
2) Si $K \subset L$ et $L \subset M$ sont radicales, $K \subset M$ aussi.

4.5.2 Proposition. *Soit $K \subset L$ une extension radicale et soit M une clôture normale de L sur K. Alors $K \subset M$ est radicale.*

Attention ce point n'est pas évident. Pour avoir une clôture normale de L sur K, c'est-à-dire la plus petite extension normale sur K et contenant L, on écrit $L = K(\alpha)$ (théorème de l'élément primitif), on appelle P le polynôme minimal de α et on pose $M = D_K(P)$.

4.5.3 Proposition. *Soient $K \subset L \subset M$ des extensions.*
L'extension $K \subset M$ est résoluble si et seulement si $K \subset L$ et $L \subset M$ le sont.

4.5.2 Groupes résolubles

Revoir les définitions et les principales propriétés des groupes résolubles. Lien avec les groupes abéliens, le groupe dérivé. Exemples : $\mathfrak{S}_3, \mathfrak{S}_4$, contre-exemple $\mathfrak{S}_n$ pour $n \geq 5$. Propriétés de stabilité par sous-groupe, quotient, extension. Un groupe résoluble simple est cyclique d'ordre premier.

4.5.3 L'énoncé du théorème

4.5.4 Théorème. *Soit $K \subset L$ une extension galoisienne. Alors l'extension est résoluble si et seulement si son groupe de Galois l'est.*

4.5.5 *Exemple.* L'équation $x^5 - 6x + 3$ n'est pas résoluble par radicaux sur $\mathbf{Q}$. En effet, son groupe de Galois est $\mathfrak{S}_5$, non résoluble. Cela résulte du lemme suivant.

4.5.6 Lemme. *Soit p un nombre premier ≥ 3, $F \in \mathbf{Q}[X]$ un polynôme irréductible de degré p. On suppose que F admet, dans $\mathbf{C}$, $p-2$ racines réelles et 2 racines imaginaires conjuguées. Alors on a $Gal(F) \simeq \mathfrak{S}_p$.*

Démonstration. On montre que le groupe de Galois contient une transposition (la conjugaison complexe) et un cycle d'ordre p.

On peut montrer que le groupe de Galois de l'équation $X^n - X - 1$ est toujours égal à $\mathfrak{S}_n$, mais c'est beaucoup plus difficile.

4.5.4 La preuve du théorème, le sens direct

On étudie trois exemples.

4.5.7 Proposition. *Soit $K \subset L = K(\zeta)$ avec $\zeta^n = 1$. L'extension $K \subset L$ est galoisienne et son groupe de Galois s'injecte dans $(\mathbf{Z}/n\mathbf{Z})^*$, donc est abélien.*

4.5.8 Proposition. *Soit $K \subset L = K(\alpha)$ avec $\alpha^n = a \in K$. On suppose que K contient une racine primitive n-ième de l'unité. L'extension $K \subset L$ est galoisienne et son groupe de Galois s'injecte dans $\mathbf{Z}/n\mathbf{Z}$ (donc est cyclique).*

4.5.9 Proposition. *Soit K un corps, $a \in K$, $n \in \mathbf{N}^*$ et posons $L = D_K(X^n - a)$. L'extension $K \subset L$ est galoisienne et se scinde en $K \subset K(\zeta) \subset L$ avec $\zeta^n = 1$. Le groupe de Galois de L sur K est extension d'un groupe abélien par un groupe cyclique et il est donc résoluble.*

Finir le sens direct : si l'extension est résoluble, le groupe l'est aussi. On raisonnera par récurrence sur le degré de l'extension.

4.5.5 Le sens réciproque

On raisonne par récurrrence sur $|G|$. Par dévissage on se ramène au cas où G est résoluble et simple, c'est-à-dire cyclique d'ordre p premier. On conclut grâce au lemme suivant :

4.5.10 Lemme. *Soit $K \subset L$ une extension galoisienne de groupe $\mathbf{Z}/p\mathbf{Z}$. On suppose que K contient une racine p-ième primitive de 1. Alors $L = K(\alpha)$, avec $\alpha^p = a \in K$.*

Démonstration. De nombreuses méthodes ! On note τ un générateur de G. Il suffit de trouver $\alpha \in L$, $\alpha \notin K$, tel que $\tau(\alpha) = \zeta\alpha$.

1) On peut chercher α sous la forme :

$$\alpha = x + \zeta\tau(x) + \zeta^2\tau^2(x) + \cdots + \zeta^{p-1}\tau^{p-1}(x),$$

le tout est de trouver un $x \in L$ tel que α soit non nul.

2) On peut aussi penser en termes de valeurs propres.

4.6 Compléments

4.6.1 Le cas "irréductible" de l'équation de degré 3

Ou la nécessité de l'invention des nombres complexes.

4.6.2 Les équations de degré 5

Classification des groupes de Galois possibles. Exemples.

4.6.3 L'équation "générique" de degré n

Il s'agit de l'extension $k(\Sigma_1, \ldots, \Sigma_n) \subset k(X_1, \ldots, X_n)$ où les Σ_i sont les polynômes symétriques élémentaires en les indéterminées X_i. On montre facilement que son groupe de Galois est $\mathfrak{S}_n$.

4.6.4 L'équation "générale" de degré n à coefficients rationnels

C'est plus difficile. Là encore, son groupe de Galois est $\mathfrak{S}_n$ mais il faut utiliser le théorème d'irréductibilité de Hilbert :

4.6.1 Théorème. *Soit $P_T(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polynôme à coefficients dans $K = \mathbf{Q}(T_1, \ldots, T_r)$. On suppose P_T irréductible sur K. Alors, il existe une infinité de r-uplets $(t_1, \ldots, t_r) \in \mathbf{Q}^r$, tels que le polynôme $P_t(X)$ obtenu en remplaçant T_i par t_i soit irréductible sur $\mathbf{Q}$ et que $Gal_{\mathbf{Q}}(P_t)$ soit égal à $Gal_K(P_T)$.*

TER numéro 5

Le paradoxe de Hausdorff-Banach-Tarski

5.1 Problématique

Le point de départ est le (difficile) théorème de Banach dans le plan qui montre l'existence d'une mesure "universelle" des parties (bornées) du plan :

5.1.1 Théorème. *Il existe une application non nulle μ simplement additive et invariante par déplacement, définie sur l'ensemble de toutes les parties bornées du plan euclidien et à valeurs dans $\mathbf{R}^+$.*

Simplement additive signifie que si l'on a deux parties disjointes X et Y on a $\mu(X \cup Y) = \mu(X) + \mu(Y)$; invariant par déplacement signifie que si g est un déplacement on a $\mu(g(X)) = \mu(X)$.

Le but du TER est de montrer le paradoxe de Hausdorff-Banach-Tarski c'est-à-dire le théorème suivant :

5.1.2 Théorème. *Soient A et B deux parties bornées d'intérieur non vide de $\mathbf{R}^3$. Alors, il existe une partition de A (resp. B) en $A_1, \ldots, A_n$ (resp. $B_1, \ldots, B_n$) et, pour chaque i, un déplacement g_i tel que $B_i = g_i(A_i)$.*

Une conséquence de ce paradoxe est que l'analogue du théorème de Banach est faux dans $\mathbf{R}^3$ (pourquoi ?).

Références principales :

[B] Banach S., Tarski A., *Sur la décomposition des ensembles de points en parties respectivement congruentes*, Fundamenta Mathematica 6 (1924), p. 244-277.

[G] Guinot M., *Le paradoxe de Banach-Tarski*, Aleas, Lyon (1991).
[H] Hausdorff F. *Bemerkung über den Inhalt von Punktmengen*, Mathematische Annalen LXXV, (1914).
[P] Perrin D., *Cours d'algèbre*, Ellipses (1991).

5.2 Hausdorff ou le paradoxe de la sphère

On se place dans $\mathbf{R}^3$ muni de la métrique euclidienne usuelle pour laquelle la base canonique e_1, e_2, e_3 est orthonormée. On note $O^+(3, \mathbf{R})$ le groupe orthogonal direct (groupes des matrices orthogonales de déterminant 1, isomorphe au groupe des rotations, cf. [P]). On note I l'identité.

5.2.1 Théorème. *Soit S la* **sphère**[1] *unité de $\mathbf{R}^3$. Il existe deux rotations a et b fixant 0, d'angles respectifs π et $2\pi/3$ et une partition de S en quatre ensembles X, Y, Z, T tels que :*
1) T est dénombrable,
2) on a $Y = b(X)$, $Z = b(Y) = b^2(X)$ et $X = a(Y \cup Z)$.

Autrement dit X est à la fois isométrique à Y, à Z et à $Y \cup Z$, donc à son double !
Démonstration. Elle comporte plusieurs étapes.

5.2.1 Les rotations

Voilà les a et b proposés par Hausdorff :

$$a = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \qquad b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ 0 & -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.$$

(On précisera leurs éléments géométriques et leur ordre.)

5.2.2 Le groupe

On considère le sous-groupe $G \subset O^+(3, \mathbf{R})$ engendré par a et b. On montrera le lemme crucial suivant :

[1] Attention, pas la boule.

5.2.2 Lemme. *Tout élément r de G, distinct de I et de a s'écrit, de manière unique, sous la forme suivante (on parle d'un* **mot***) :*

$$r = a^{\epsilon_1} b^{n_1} a b^{n_2} a \cdots a b^{n_{k-1}} a b^{n_k} a^{\epsilon_2}$$

avec $k \in \mathbf{N}^*$, $\epsilon_i = 0$ ou 1 et $n_i = 1$ ou 2. En particulier, le groupe G est dénombrable.

Ce n'est pas facile. L'existence ça va. Pour l'unicité il faut montrer par récurrence sur k qu'un produit du type $c = b^{n_1} a \cdots b^{n_k} a$ est de la forme ci-dessous :

$$\frac{1}{2^k} \begin{pmatrix} p_1 & p_2 & p_3\sqrt{3} \\ q_1 & p_4 & q_2\sqrt{3} \\ q_3\sqrt{3} & p_5\sqrt{3} & q_4 \end{pmatrix}$$

avec $p_i, q_i \in \mathbf{Z}$, p_i pair et q_i impair. On en déduit que c ne peut être égal à I ou a.

5.2.3 Le découpage du groupe

Notre objectif est de partager G en trois parties **disjointes** : $G = A \cup B \cup C$ vérifiant $B = bA$, $C = bB = b^2A$ et $A = a(B \cup C)$.

Pour cela, on écrit G comme union **disjointe** : $G = A_0 \cup B_0 \cup C_0 \cup \{I\}$ où A_0 est la partie formée par les mots commençant par a, B_0 celle formée par les mots commençant par b et C_0 celle formée par les mots commençant par b^2.

5.2.3 Lemme. *On a les formules suivantes : $C_0 = bB_0$, $B_0 = b^2C_0$, $bA_0 = B_0 - \{b\}$, $b^2A_0 = C_0 - \{b^2\}$, $a(B_0 \cup C_0) = A_0 - \{a\}$.*

Cela ressemble beaucoup à ce qu'on cherche, mais il y a quelques éléments récalcitrants : a, b, b^2, I qu'il faut faire rentrer dans le rang. L'idée fondamentale pour cela : le fait que $\mathbf{N}$ est en bijection avec $\mathbf{N} - \{0\}$ par $n \mapsto n + 1$. Pour trouver un ensemble qui ressemble à $\mathbf{N}$ on prend un élément d'ordre infini de G, par exemple b^2a (pourquoi est-il d'ordre infini ?) et on appelle N le "monoïde" engendré :

$$N = \{I, b^2a, (b^2a)^2, (b^2a)^3, \ldots, (b^2a)^n, \ldots\}$$

On note que $N - \{I\}$ est contenu dans C_0, aN dans A_0 et baN dans B_0. De plus, on notera que l'on a $bN = aN \cup \{b\}$: voilà comment rajouter l'élément b !

Maintenant, on modifie A_0, B_0, C_0 comme suit : on leur retranche aN, baN et $N - \{I\}$ et l'on redistribue autrement les ensembles N, aN, baN pour obtenir A, B, C comme annoncé.

5.2.4 Le découpage de la sphère

C'est maintenant facile. On fait opérer le groupe G sur S. Il y a deux sortes de points $x \in S$. Ceux (disons de type 1) qui sont sur les axes des éléments $g \in G$. Ils sont en nombre dénombrable (car G est dénombrable) : c'est l'ensemble T. Les autres (de type 2) vérifient $g(x) \neq x$ pour tout $g \in G$. L'orbite de x, $\omega(x)$ est donc en bijection avec G. Les orbites des points de type 2 forment une partition de $S - T$. Dans chacune des orbites des points de type 2 on choisit un point (c'est possible grâce à **l'axiome du choix**). On obtient ainsi un ensemble E et si on pose $X = AE = \{g(x) \mid g \in A \text{ et } x \in E\}$, $Y = BE$, $Z = CE$, on obtient le découpage cherché.

5.3 Banach-Tarski, suite et fin

5.3.1 Généralités sur le découpage

5.3.1 Définition. *Soient X, Y deux parties de $\mathbf{R}^d$. On dit que X et Y sont* **équidécomposables** *(ou encore équivalentes par découpage et recollement) s'il existe des* **partitions** *$X = X_1 \cup X_2 \cup \cdots \cup X_n$ et $Y = Y_1 \cup Y_2 \cup \cdots \cup Y_n$ telles que, pour tout $i = 1, \ldots, n$, il existe un déplacement f_i de $\mathbf{R}^d$ qui vérifie $f_i(X_i) = Y_i$. On note alors $X \sim Y$.*

Ce qu'affirme Banach-Tarski c'est que deux parties bornées d'intérieur non vide de $\mathbf{R}^3$ sont équivalentes.

On réfléchira sur l'astuce suivante (l'une des astuces fondamentales dans ce genre de choses, toujours le fait que $\mathbf{N}$ et $\mathbf{N} - \{0\}$ c'est pareil). Il s'agit de montrer que, dans le plan, le disque unité D est équivalent à $D - A$ où A est un rayon. Pour cela, on choisit une rotation ρ, de centre 0 et d'angle irrationnel par rapport à π, on regarde $E = \bigcup_{n \in \mathbf{N}} \rho^n(A)$ et on écrit $D = (D - E) \cup E$ et, par un tour de magie, on fait disparaître A.

On montrera les trois points suivants :

• La relation $\sim$ est une relation d'équivalence (pour la transitivité, il faut découper les découpages).

• Si on a $X \sim X'$ et $Y \sim Y'$ avec X, Y (resp. X', Y') disjoints, on a $X \cup Y \sim X' \cup Y'$.

• On a un théorème du type de Cantor-Bernstein :

5.3.2 Proposition. *Si on a $X' \subset X$ et $Y' \subset Y$ avec $X \sim Y'$ et $Y \sim X'$, on a aussi $X \sim Y$.*

Démonstration. Le mieux est de comprendre d'abord le Cantor-Bernstein ordinaire. On a des bijections $f : X \to Y' \subset Y$ et $g : Y \to X' \subset X$, d'où

$f^{-1} : Y' \to X$ et $g^{-1} : X' \to Y$ et il s'agit de construire une bijection Φ de X sur Y. On part de $x \in X$ et on applique, tant qu'on peut, g^{-1}, puis f^{-1}, puis g^{-1}, etc. On partage alors X en trois sortes de points suivant que le processus s'arrête sur X, sur Y, ou ne s'arrête pas. On définit Φ sur cette partition. (On formalisera ces idées, bien entendu.)

5.3.2 Trois sphères ou presque

5.3.3 Corollaire. *Soient S, S', S'' trois sphères de rayon 1 disjointes. Il existe des parties dénombrables T, T', T'' respectivement contenues dans S, S', S'' telles que l'on ait $S - T \sim (S' - T') \cup (S'' - T'')$.*

Démonstration. On utilise Hausdorff, bien sûr.

5.3.3 Élimination des dénombrables

5.3.4 Corollaire. *Avec les notations du corollaire 7, on a $S \sim S' \cup S''$.*

Démonstration. Il suffit de montrer qu'on a $S \sim S - T$. Pour cela, on trouve une rotation r telle que l'on ait, pour $x, y \in T$, distincts et $n \in \mathbf{N}^*$, $r^n x \neq y$ (ça existe !). On utilise alors l'astuce $\mathbf{N} \sim \mathbf{N} - \{0\}$ vue plus haut avec la réunion des $r^n(T)$.

5.3.4 On a les boules !

5.3.5 Corollaire. *Soient B, B', B'' trois boules disjointes de rayon 1. On a $B \sim B' \cup B''$.*

Démonstration. Il suffit d'utiliser les sphères. Attention tout de même à l'origine !

5.3.5 Conclusion

On finira de prouver le théorème 5.1.2. Il suffit de montrer que si B est une boule fermée de rayon R contenue dans X on a $B \sim X$. Pour cela on recouvre X par un nombre fini de boules de rayon R et on utilise Cantor-Bernstein.

TER numéro 6

Constructions à la règle et au compas

6.1 Introduction

Le but du TER est de comprendre quelles constructions sont possibles à la règle et au compas et de résoudre en particulier un certain nombre de problèmes laissés en suspens par les grecs.

Références principales :

[C] Carréga, *Théorie des corps, la règle et le compas*, Hermann.

[ST] Stewart, *Galois theory*, Chapmann-Hall,

[P] Perrin, *Cours d'algèbre*, Ellipses.

[P'] Perrin D, *Mathématiques d'école*, Cassini.

Sur ce type de problème, une introduction historique s'impose. Il faut présenter les problèmes des grecs, dire ce qu'ils savaient faire et ne pas faire. Voir la bibliographie de [C] et notamment :

[De] Descartes R. *La géométrie*, nouvelle édition, Hermann, 1886.

Pour voir qu'il y a des gens qui n'ont toujours pas compris :

[Du] Dudley Underwood, *A budget of trisections*, Springer Verlag, 1987.

6.2 Nombres réels constructibles

6.2.1 La partie facile

Rappeler quelles constructions élémentaires on sait faire. Donner quelques exemples un peu amusants.

Préciser les définitions : points constructibles (à partir de points donnés, en général deux points), réels constructibles.

Montrer que l'ensemble $\mathcal{K}$ des constructibles est un corps, qui contient $\mathbf{Q}$ et qui est stable par racine carrée. Caractérisation des constructibles :

6.2.1 Théorème. *Soit x un nombre réel. Alors x est constructible si et seulement si il existe une suite $K_0, K_1, \cdots, K_r$ de sous-corps de $\mathbf{R}$ vérifiant les conditions suivantes :*
1) on a $K_0 = \mathbf{Q}$,
2) on a $K_0 \subset K_1 \subset \cdots \subset K_n$, plus précisément, pour chaque $i = 1, 2, \cdots, r$, il existe $d_i \in K_{i-1}$ tel que $K_i = K_{i-1}(\sqrt{d_i})$,
3) on a $x \in K_r$.

On en déduit qu'un constructible est algébrique sur $\mathbf{Q}$ et de degré une puissance de 2. Attention, la réciproque est fausse.

6.2.2 La partie difficile

On utilise la théorie de Galois (dont il faut comprendre les rudiments, cf. [S]) pour obtenir le théorème suivant.

6.2.2 Théorème. *Soit x un nombre réel algébrique de polynôme minimal P. Alors x est constructible si et seulement si le corps de décomposition de P est de degré une puissance de 2.*

Contre-exemple avec $X^4 - X - 1$ sinon.

6.3 Applications

6.3.1 Duplication, trisection

Montrer que la duplication est impossible, préciser quels angles sont trisectables.

6.3.2 Quadrature du cercle

C'est la transcendance de π, voir les références.

6.3.3 Les polygones réguliers

Le résultat est le suivant :

6.3.1 Théorème. *Soit n un entier ≥ 3. Le polygone régulier à n côtés est constructible si et seulement si n est de la forme $n = 2^\alpha p_1 \cdots p_r$ avec $\alpha \geq 0$, $r \geq 0$, les p_i premiers, distincts et de la forme $2^{2^m} + 1$ (nombres de Fermat).*

Seuls exemples de nombres de Fermat connus : 3,5,17,257, 65537.

Construction effective dans le cas du pentagone et du polygone à 17 côtés (cf. [S]).

6.4 Compléments

Selon l'intérêt on pourra étudier des problèmes voisins : le compas seul, la règle seule, la règle à glissière et d'autres amusettes (le compas bloqué, la règle ou la feuille trop petites, etc.).

TER numéro 7

Quaternions

7.1 Introduction

Le but du TER, après avoir revu la définition et les propriétés algébriques du corps des quaternions, est d'étudier l'isomorphisme du quotient $G\{\pm 1\}$ du groupe des quaternions de norme 1 par son centre et le groupe euclidien $O^+(3, \mathbf{R})$ et d'en tirer les conséquences topologiques sur le groupe $O^+(3, \mathbf{R})$ en particulier, le fait qu'il n'est pas simplement connexe.

Références

[DP] Perrin Daniel, *Cours d'algèbre*, Ellipses.

[Gramain] Gramain André, *Topologie des surfaces*, PUF, 1971.

7.2 Définitions et propriétés algébriques

Définir l'ensemble $\mathbf{H}$ des quaternions et montrer que c'est un corps non commutatif. Définir conjugué et norme. Voir [DP].

7.3 Les quaternions et le groupe orthogonal

Montrer l'isomorphisme entre le quotient $G/\{\pm 1\}$ du groupe des quaternions de norme 1 par son centre et le groupe euclidien $O^+(3, \mathbf{R})$. Relation du groupe $O^+(4, \mathbf{R})$ avec $G \times G$. Voir [DP].

7.4 Topologie : préliminaires

7.4.1 Définitions

On travaille sur un espace topologique X dont on se donne un point a. On note I le segment $[0,1]$.

7.4.1 Définition.
1) Un chemin est une application continue $\gamma : I \to X$. Un **lacet** *de base a est un chemin qui vérifie $\gamma(0) = \gamma(1) = a$. Le lacet trivial (ou nul) est le lacet constant donné par $\gamma(t) = a$ pour tout t. L'opération de* **concaténation** *(ou somme) de deux lacets (notée $\gamma \wedge \delta$) consiste à parcourir l'un puis l'autre.*
2) Deux lacets γ et δ sont **homotopes** *s'il existe une application continue $H : I^2 \to X$ qui à (t,u) associe $H(t,u)$ et vérifie :*
a) $H(0,u) = H(1,u) = a$ pour tout u.
b) $H(t,0) = \gamma(t)$ et $H(t,1) = \delta(t)$ pour tout t.

7.4.2 Définition. *L'espace X est dit* **simplement connexe** *s'il est connexe par arcs et si tout lacet est homotope au lacet trivial (on dit encore homotope à un point, voire à 0).*

7.4.3 *Exemples.* L'espace $\mathbf{R}^d$ est simplement connexe. Le plan privé d'un point, le cercle ne sont pas simplement connexes.

7.4.4 Lemme. *Si des lacets γ et δ sont homotopes à 0 il en est de même de $\gamma \wedge \delta$.*

7.4.2 La sphère

7.4.5 Proposition. *On suppose $d \geq 2$. La sphère unité euclidienne de $\mathbf{R}^{d+1}$:*

$$\mathbf{S}^d = \{(x_0, x_1, \ldots, x_d) \in \mathbf{R}^{d+1} \ \mid \ \sum_{i=0}^{d} x_i^2 = 1 \ \}$$

est simplement connexe.

Démonstration. La démonstration se fait en plusieurs étapes (voir [Gramain] si besoin est).

7.4.6 Lemme. *La sphère $\mathbf{S}^d$ privée d'un point est homéomorphe à $\mathbf{R}^d$.*

La preuve utilise la projection stéréographique. On enlève le pôle nord n et on projette la sphère sur l'équateur P en associant à un point $x \in \mathbf{S}^d$ le point où la droite (nx) coupe P.

Une fois ce résultat établi, le principe de la preuve de 7.4.5 est simple. On recouvre la sphère par deux ouverts U_1 et U_2 homéomorphes à $\mathbf{R}^d$ (obtenus en enlevant les pôles n et s) et on considère un lacet γ de base $a \neq n, s$. On va montrer qu'il est homotope à 0 en montrant qu'il est homotope au concaténé de lacets tracés successivement dans U_1 et U_2. En fait, le lemme général est le suivant :

7.4.7 Lemme. *On suppose que X est réunion de deux ouverts simplement connexes U_1 et U_2 et que l'intersection $U_1 \cap U_2$ est connexe par arcs. Alors X est simplement connexe.*

Le lemme suivant sera utile ici et dans la suite :

7.4.8 Lemme. *Soit X un espace métrique compact et $(U_i)_{i\in I}$ un recouvrement ouvert de X. Il existe un nombre $r > 0$ (appelé nombre de Lebesgue du recouvrement) tel que toute boule de rayon $< r$ est contenue dans un ouvert du recouvrement au moins.*

La conséquence de ce qui précède c'est que le groupe topologique G des quaternions de norme 1, qui est homéomorphe à $\mathbf{S}^3$ est simplement connexe.

7.5 Revêtements et homotopie

7.5.1 La situation

On reprend l'homomorphisme p du groupe G des quaternions de norme 1 sur le groupe $\overline{G} = O^+(3, \mathbf{R})$. La situation est donc la suivante : on a deux groupes topologiques compacts G et $\overline{G}$ et un homomorphisme $p : G \to \overline{G}$, continu, surjectif, de noyau[1] $\{1, -1\}$. On pose $-g = (-1)g$ pour $g \in G$.

7.5.1 Lemme.
L'application p est fermée et ouverte.

Démonstration. C'est évident pour fermé. Pour ouvert, il faut utiliser la notion de partie saturée, i.e. stable par l'application $g \mapsto -g$.

7.5.2 Revêtements

L'application p est ce qu'on appelle un **revêtement**. C'est ce que dit la proposition suivante :

[1] Dans le cas général, -1 est un élément d'ordre 2 central de G.

7.5.2 Proposition. *Soit $\overline{g} \in \overline{G}$ et et soient g et $-g$ ses antécédents dans G. Il existe un ouvert U de G contenant g vérifiant les conditions suivantes :*
1) $\overline{U} = p(U)$ est un ouvert de $\overline{G}$,
2) $p^{-1}(\overline{U}) = U \cup (-U)$ et $U \cap (-U) = \emptyset$,
3) les restrictions de p à U et $-U$ sont des homéomorphismes sur $\overline{U}$.

7.5.3 Définition. *Un ouvert $\overline{U}$ de $\overline{G}$ du type de 7.5.2 est appelé ouvert de trivialisation.*

Sur un ouvert de trivialisation on dispose donc d'un homéomorphisme qui "remonte" p.

7.5.3 Relèvement d'applications : unicité

7.5.4 Théorème. *Soit T un espace topologique connexe et soit $h : T \to \overline{G}$ une application continue. Soit $t_0 \in T$, $y_0 = h(t_0)$ et $x_0 \in G$ tel que $p(x_0) = y_0$. Alors il existe au plus une application continue $k : T \to G$ telle que $pk = h$ et $k(t_0) = x_0$.*

Démonstration. Si on a deux applications k et k' vérifiant les conditions du théorème, on pose : $X = \{t \in T \mid k(t) = k'(t)\}$ et on utilise la connexité.

7.5.4 Relèvement des chemins

La propriété principale des revêtements est le relèvement des chemins :

7.5.5 Théorème. *Soit x_0 un point de G, $y_0 = p(x_0)$ son image et soit $\gamma : [0,1] \to \overline{G}$ un chemin (continu) d'origine $\gamma(0) = y_0$. Alors, il existe un unique chemin (continu) $\delta : [0,1] \to G$ qui relève γ (ce qui signifie qu'on a $p\delta(t) = \gamma(t)$ pour tout t) et qui vérifie $\delta(0) = x_0$.*

Démonstration. (Pas facile, me consulter au besoin.) Grâce aux ouverts de trivialisation on sait faire le relèvement localement au voisinage de chaque point $\gamma(t)$ du chemin. On va recouvrir le chemin par un nombre fini d'ouverts de trivialisation (par compacité) et on obtiendra ainsi des chemins définis sur des intervalles J_k recouvrant I. Le lemme suivant sera alors utile :

7.5.6 Lemme. *Soient $J_1, J_2, \cdots, J_n$ des intervalles, ouverts dans $[0,1]$, recouvrant $[0,1]$ et sans inclusions mutuelles. Quitte à à réordonner les J_i, on peut supposer que J_1 contient 0 et que, pour $i = 1, \cdots, n-1$, $J_i \cap J_{i+1}$ contient un point τ_i, avec $0 < \tau_1 < \tau_2 < \cdots < \tau_{n-1}$.*

7.5.5 Relèvement des homotopies

C'est l'autre propriété essentielle des revêtements :

7.5.7 Théorème. *Posons $I = [0,1]$. Soit $H : I^2 \to \overline{G}$ une application continue. On pose $H(0,0) = \overline{g}$. Soit $g \in G$ tel que $p(g) = \overline{g}$. Alors, il existe $K : I^2 \to G$, continue, unique, telle que l'on ait $pK = H$ et $K(0,0) = g$.*

Démonstration. (Me consulter) La technique est analogue au cas des lacets. On utilisera des relèvements définis sur des pavés P_{ij} de la forme $[\frac{i}{n}, \frac{i+1}{n}] \times [\frac{j}{n}, \frac{j+1}{n}]$, avec $i, j \in \{0, \ldots, n-1\}$ et on raisonnera par récurrence sur les couples (i,j) ordonnés par ordre lexicographique.

7.5.8 Corollaire. *Avec les notations précédentes, on suppose qu'on a, pour tout $u \in I$, $H(0,u) = H(1,u) = \overline{g} \in \overline{G}$. Soit $g \in G$ tel que $p(g) = \overline{g}$. Alors, il existe $K : I^2 \to G$, continue, unique, telle que l'on ait $pK = H$ et $K(0,u) = g$ pour tout u.*

7.5.6 Groupe d'homotopie

On suppose désormais que G est simplement connexe (c'est le cas de la sphère). On a le résultat suivant :

7.5.9 Théorème. *Soit γ un lacet de $\overline{G}$ d'origine et d'extrémité $\overline{1}$ et soit δ son unique relevé dans G vérifiant $\delta(0) = 1$ (cf. 7.5.5). On a $\delta(1) = \pm 1$.*
1) Si $\delta(1)$ est égal à 1, i.e. si δ est un lacet, γ est homotope à zéro.
2) Si $\delta(1)$ est égal à -1, γ n'est pas homotope à zéro, tous les lacets de ce type sont homotopes entre eux et leur double est homotope à 0.
Le groupe fondamental de $\overline{G}$ est le groupe $\mathbf{Z}/2\mathbf{Z}$.

Conlure avec le "truc de l'assiette à soupe", comme dit Berger.

TER numéro 8

Le théorème de Minkowski

8.1 Introduction

Le but du TER est de montrer quelques résultats concernant les réseaux et notamment le théorème de Minkowski et ses applications arithmétiques.

Références principales :

[C] Cox, *Primes of the forme* $x^2 + ny^2$, Wiley.
[P] Perrin, *Cours d'algèbre*, Ellipses.
[PR] Perrin-Riou, *Algèbre, arithmétique et maple*, Cassini.
[S] Samuel, *Théorie algébrique des nombres*, Hermann.
[SO] Scharlau-Opolka, *From Fermat to Minkowski*, Springer.
[ST] Stewart-Tall, *Algebraic number theory*, Chapmann-Hall.
[T] Tauvel, *Mathématiques générales pour l'agrégation*, Masson.

Voir aussi, plus généralement, les livres de théorie des nombres.

Un sous-réseau L de $\mathbf{R}^n$ est un sous-groupe additif qui admet une $\mathbf{Z}$-base $e_1, \cdots, e_r$ c'est-à-dire une famille libre telle que tout élément de L soit combinaison linéaire des e_i à coefficients entiers relatifs. Un réseau est un sous-réseau de rang $r = n$.

8.2 Propriétés des réseaux

8.2.1 Sous-groupes discrets

8.2.1 Théorème. *Un sous-groupe de* $\mathbf{R}^n$ *est un sous-réseau si et seulement si il est discret.*

8.2.2 Corollaire. *Un sous-groupe d'un sous-réseau est un sous-réseau.*

8.2.2 Volume et domaine fondamental

On munit $\mathbf{R}^n$ d'une structure euclidienne. Le volume d'un réseau est le déterminant d'une $\mathbf{Z}$-base sur une base orthonormée (c'est indépendant du choix de ces bases). Interprétation géométrique avec le parallélotope bâti sur la $\mathbf{Z}$-base.

8.3 Minkowski

8.3.1 Théorème. *(Minkowski) Soit L un réseau de $\mathbf{R}^n$ et C un convexe, symétrique par rapport à l'origine et tel que $\mu(C) > 2^n \, vol\,(L)$. Alors C contient un point non nul de L.*

Variantes diverses. (cf. [S, ST, etc])

8.4 Application 1 : les deux carrés

Référence [ST]

8.4.1 Théorème. *Tout nombre premier p congru à 1 modulo 4 est somme de deux carrés.*

8.4.2 Corollaire. *Description des entiers sommes de deux carrés. (cf. [ST] ou [P])*

Pour un algorithme, cf. [PR].

8.5 Les quatre carrés

8.5.1 Théorème. *Tout entier est somme de quatre carrés.*

Voir [ST] et me consulter.

8.6 Les entiers de la forme $x^2 + 5y^2$

Problème : déterminer exactement les entiers de la forme $x^2 + 5y^2$. Voilà le résultat. Soit P l'ensemble des nombres premiers. On distingue trois parties de P :

$$P_1 = \{\ p \in P \ \mid\ p = 5 \quad \text{ou} \quad \big(\ p \equiv \pm 1 \pmod 5 \quad \text{et} \quad p \equiv 1 \pmod 4\ \big)\ \},$$

$P_2 = \{\, p \in P \mid p = 2 \quad \text{ou} \quad \big(p \equiv \pm 2 \pmod 5 \quad \text{et} \quad p \equiv -1 \pmod 4 \big) \,\}$,

et enfin $P_3 = P - P_1 - P_2$. On a alors :

8.6.1 Théorème. *Soit $n \in \mathbf{N}$. On pose $n = \prod_{p \in P} p^{v_p(n)}$. Alors, n est de la forme $x^2 + 5y^2$ si et seulement si on a les deux conditions suivantes :*
1) $\forall p \in P_3$, $v_p(n)$ est pair,
2) $\sum_{p \in P_2} v_p(n)$ est pair.

TER numéro 9

Pavages du plan

9.1 Introduction

Le but du TER est, dans un premier temps, de classifier les pavages réguliers du plan, mais aussi les ornements linéaires (ou frises), puis d'étudier les pavages irréguliers.

Références principales :

[B] Berger, *Géométrie*, Nathan ou Cassini.

[FT] Fejes-Toth, *Regular figures*, Pergamon Press, 1964.

Le livre de Fejes-Toth est très intéressant, notamment par les dessins, les notes historiques, etc.

[HCV] Hilbert et Cohn-Vossen, *Geometry and the Imagination*, Chelsea publishing, 1952.

Voir aussi, pour les dessins Escher ou le magazine Tangente.

9.2 Sous-groupes discrets du groupe des isométries planes

9.2.1 Définitions

On désigne par X le plan affine euclidien.

Déterminer les sous-groupes discrets (expliquer ce mot, lien avec fermé discret) de $(\mathbf{R}^2, +)$, lien avec les réseaux, caractérisations. Déterminer les isométries vectorielles conservant un sous-groupe de la forme $\mathbf{Z}$ ou $\mathbf{Z}^2$. (On ramènera un réseau à une forme particulière.)

Sous-groupes discrets G de $\mathrm{Is}\,(X)$, groupe des isométries affines du plan, caractérisation. On montrera que, si G est infini, G est discret si et seulement si le groupe des translations T de G est isomorphe à $\mathbf{Z}$ ou $\mathbf{Z}^2$ et on précisera le quotient G/T.

9.2.2 Ornements et pavages

9.2.1 Définition. *On appelle ornement linéaire (resp. ornement plan) une partie A de X telle que le groupe des translations qui conservent A soit isomorphe à $\mathbf{Z}$ (resp. à $\mathbf{Z}^2$).*

9.2.2 Définition. *On appelle pavage du plan la donnée d'un compact P de X, d'intérieur non vide et d'un sous-groupe G de $\mathrm{Is}\,(X)$ vérifiant :*
1) $\bigcup_{g\in G} g(P) = X$,
2) $g(P^\circ) \cap h(P^\circ) \neq \emptyset \Longrightarrow g(P) = h(P)$.

Montrer que le groupe d'un ornement (linéaire ou plan) et d'un pavage sont des sous-groupes discrets de $\mathrm{Is}\,(X)$.

9.3 Ornements linéaires

9.3.1 Détermination

Soit A un ornement linéaire, G le groupe des isométries qui conservent A, T son sous-groupe de translations.

Rappeler les quotients G/T possibles.

Montrer l'existence d'une droite D invariante par G.

Répertorier les transformations possibles dans G.

Décrire tous les ornements possibles (i.e. les G possibles) en précisant la structure de G. Donner un dessin pour chacun. (Il y en a 7).

9.3.2 Classification

Classifier les groupes des ornements linéaires vis-à-vis des 5 relations d'équivalence suivantes :

1) $G\ \mathcal{R}_1\ G' \iff G$ et G' isomorphes.

2) $G\ \mathcal{R}_1\ G' \iff T$ et T' isomorphes, G/T et G/T' isomorphes, les extensions isomorphes.

3) $G\ \mathcal{R}_1\ G' \iff G$ et G' conjugués dans le groupe affine $A(X)$.

4) $G \mathcal{R}_1 G' \iff G$ et G' conjugués dans le groupe des similitudes $\mathrm{Sim}(X)$.

5) $G \mathcal{R}_1 G' \iff G$ et G' conjugués dans le groupe des isométries $\mathrm{Is}(X)$.

9.4 Pavages et ornements plans

9.4.1 Détermination

Soit A un ornement plan (ou un pavage), G le groupe des isométries qui conservent A, T son sous-groupe de translations.

Rappeler les possibilités pour le groupe G/T.

Répertorier les transformations possibles dans G.

Décrire tous les ornements possibles (i.e. les G possibles) en précisant la structure de G. Donner un dessin pour chacun. (Il y en a 17). Préciser les invariants géométriques (axes et centres de symétrie, distances des axes, des centres, rotations, angles, symétries glissées, etc.)

9.4.2 Classification

En quel sens (i.e. pour quelles $\mathcal{R}_i$) y-a-t'il 17 groupes ?

9.4.3 Réalisation

Comment réaliser un pavé qui permet de recouvrir le plan (cf. Escher, Kangourou, etc.)

9.5 Pavages irréguliers

9.5.1 Pavages de la droite

Fibonacci et consorts. Quelle régularité ? Réalisation par projection.

9.5.2 Pavages du plan

Les pavages archimédiens (par des polygones réguliers, pas tous du même type, mais tels qu'en chaque point on ait la même configuration, cf. Fejes-Toth).

TER numéro 10

Polyèdres

10.1 Introduction

Le but du TER est, d'étudier les polyèdres (convexes) de $\mathbf{R}^3$.

Références principales :

[B] Berger, *Géométrie*, Nathan ou Cassini.

[FT] Fejes-Toth, *Regular figures*, Pergamon Press, 1964.

Le livre de Fejes-Toth est très intéressant, notamment par les dessins, les notes historiques, etc.

[H] Hadamard, Jacques, *Géométrie*, tome 2.

[HCV] Hilbert et Cohn-Vossen, *Geometry and the Imagination*, Chelsea publishing, 1952.

[P] Perrin, *Mathématiques d'école*, Cassini.

Voir aussi, Boursin-Larose pour les pliages.

Les parties peuvent être traitées dans un ordre arbitraire

10.2 Polyèdres convexes

10.2.1 Définitions

Le point principal est de montrer l'équivalence entre les deux définitions suivantes :

10.2.1 Définition. *Un polyèdre convexe est une intersection finie P de demi-espaces fermés vérifiant deux conditions :*
1) P est borné,
2) P est d'intérieur non vide.

10.2.2 Définition. *Un polyèdre convexe est l'enveloppe convexe d'un nombre fini de points de l'espace, non contenus dans un plan.*

Il s'agit ensuite de définir, dans chaque cas, ce que sont les faces, les arêtes, les sommets.

10.2.2 Dualité

Définir le dual P^* d'un polyèdre convexe P et montrer que c'est un polyèdre convexe. Quels rapports entre faces, arêtes, sommets de P et de P^* ?

10.3 Formule d'Euler

10.3.1 La formule des angles

Il s'agit de montrer que la somme des angles en un sommet d'un polyèdre convexe est $< 2\pi$.

10.3.2 La formule de Girard

Si T est un triangle sphérique (limité par des grands cercles) sur la sphère unité la somme des angles de T est égale à π plus l'aire de T.

10.3.3 La formule d'Euler

Si P est un polygone convexe (?) on a $s - a + f = 2$ où s (resp. a, resp. f) est le nombre de sommets (resp. d'arêtes, resp. de faces) de P.

10.4 Polyèdres réguliers

10.4.1 Classification combinatoire

Montrer qu'il y a cinq polyèdres réguliers au plus. Les décrire.

10.4.2 Des démonstrations

Existence des polyèdres en question.

Équivalence des définitions de régulier.

Unicité à similitude près.

10.4.3 Les groupes d'isométrie

Déterminer les groupes d'isométries du tétraèdre, du cube, du dodécaèdre. Comportement par dualité. Identrification à des groupes symétriques ou alternés.

10.5 Polyèdres archimédiens, deltaèdres et autres bêtes

Voir [ME].

TER numéro 11

Décomposition de Cartan

11.1 La décomposition de Cartan de $GL(n, \mathbf{R})$

11.1.1 Le résultat algébrique

11.1.1 Proposition. *Soit $A \in GL(n, \mathbf{R})$ une matrice inversible. Il existe un unique couple (B, C) avec $B \in O(n, \mathbf{R})$ et C symétrique définie positive, tel que $A = BC$.*

Indication : si on a une telle décomposition on a ${}^tAA = C^2$. Or, ${}^tAA$ est une matrice symétrique définie positive. Il s'agit de montrer qu'on peut extraire une racine d'une telle matrice (de manière unique) ce qui se fait par diagonalisation. Attention à l'unicité.

11.1.2 Les homéomorphismes

On note $\mathcal{S}$ (resp. $\mathcal{S}^+$) l'ensemble des matrices $n \times n$ réelles symétriques (resp. symétriques définies positives).

11.1.2 Théorème. *L'application $(B, C) \mapsto BC$ est un homéomorphisme de $O(n, \mathbf{R}) \times \mathcal{S}^+ \to GL(n, \mathbf{R})$.*

Indication : il y a plusieurs voies. On peut montrer que $A \mapsto A^2$ est un homéomorphisme de $\mathcal{S}^+$ sur lui-même en montrant que c'est un C^1-difféomorphisme (inversion locale). On peut aussi montrer directement l'homéo par un argument de compacité ($O(n, \mathbf{R})$ est compact) en utilisant le fait qu'une suite de points d'un compact qui n'a qu'une valeur d'adhérence converge vers cette valeur.

11.1.3 Proposition. *L'exponentielle est un homéomorphisme de $\mathcal{S}$ sur $\mathcal{S}^+$.*

Indication : plusieurs voies encore. Soit on montre que c'est un difféomorphisme, mais le calcul de la différentielle est plus ardu, soit on utilise un argument de compacité (ou plutôt de propreté) comme pour le th. 2.

On note aussi que $\mathcal{S}$ est homéomorphe à l'espace numérique $\mathbf{R}^{n(n+1)/2}$, donc aussi $\mathcal{S}^+$.

11.1.3 Conséquences

11.1.4 Proposition. *Le groupe $GL(n,\mathbf{R})$ est homéomorphe au produit de $O(n,\mathbf{R})$ par un espace numérique.*

11.1.5 Corollaire. *Le groupe $GL(n,\mathbf{R})$ a deux composantes connexes. Le groupe $SL(n,\mathbf{R})$ est connexe par arcs.*

(Il y a des preuves directes de ce fait).

Notons que $O(n,\mathbf{R})$ est un sous-groupe compact maximal de $GL(n,\mathbf{R})$. On montre en effet que tout sous-groupe compact de GL est contenu dans un $O(q)$ pour une forme q définie positive, donc dans un conjugué de $O(n,\mathbf{R})$.

Prolongements possibles : étudier le cas de $GL(n,\mathbf{C})$, étudier la connexité de $PGL(n,\mathbf{R})$, lien avec l'orientabilité de l'espace projectif.

11.2 La décomposition de Cartan de $O(q)$

On étudie le groupe $O(q)$ pour une forme q non dégénérée de rang n (mais pas définie positive). Attention, ce groupe n'est plus compact (pourquoi ?). On sait, par Sylvester qu'on peut supposer que la forme q admet pour matrice $J = \begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix}$ où I_k est la matrice identité d'ordre k et où l'on a $p+q=n$. On note aussi $O(J)$ le groupe orthogonal.

11.2.1 Théorème. *Soit $A \in O(J)$ et soit $A = BC$ sa décomposition de Cartan. Alors, on a $B, C \in O(J)$.*

Indication : écrire $C = \exp(S/2)$ et montrer que si $\exp(S)$ est dans $O(J)$ il en est de même de $\exp(\lambda S)$ pour $\lambda \in \mathbf{R}$.

11.2.2 Proposition. *Le groupe $O(J) \cap O(n,\mathbf{R})$ est isomorphe au produit direct $O(p,\mathbf{R}) \times O(q,\mathbf{R})$.*

Indication : écrire les matrices par blocs.

11.2.3 Proposition. *Soit S une matrice symétrique. Alors, $\exp(S)$ est dans $O(J)$ si et seulement si on a $SJ + JS = 0$.*

11.2.4 Corollaire. *L'espace $\mathcal{S}^+ \cap O(J)$ est homéomorphe à un espace numérique.*

11.2.5 Corollaire. *Le groupe $O(J)$ est homéomorphe au produit de $O(p) \times O(q)$ par un espace numérique. Il a donc quatre composantes connexes.*

(On peut donner une preuve directe de ce dernier fait en utilisant une écriture par blocs).

Prolongements : montrer que la composante connexe de l'élément neutre d'un groupe topologique est un sous-groupe distingué. Montrer que dans le cas de $O(J)$ c'est le groupe des commutateurs. Comprendre la condition $SJ + JS = 0$ en termes d'espace tangent et d'algèbre de Lie.

TER numéro 12

Le théorème de Pascal

12.1 Introduction

Le but du TER est de prouver le théorème de Pascal sur une conique. :

12.1.1 Théorème. *Soit C une conique et soient a, b, c, a', b', c' six points distincts de C. On appelle respectivement u, v, w les points d'intersections de (bc') et $(b'c)$, (ca') et $(c'a)$, (ab') et $(a'b)$. Alors, u, v, w sont alignés.*

La référence principale est le texte sur le sujet, sur ma page web :
`http://www.math.u-psud.fr/ perrin/conferences.html`
qu'il s'agira de comprendre et de compléter.

12.2 La preuve dans l'esprit d'Erlangen

Elle consiste à prouver d'abord le résultat dans le cas d'un cercle, puis à montrer que, du point de vue projectif, cercle et conique (propre) sont équivalents, soit en utilisant les sections de cône (comme Pascal), soit la transitivité des homographies.

12.3 La preuve par le birapport

On prouvera d'abord la conservation du birapport par perspective, puis l'existence du birapport sur un cercle ou une conique. On terminera en montrant que Pappus ou Pascal sont conséquences des points précédents.

12.4 La preuve avec les relations

On définira crochets et produits extérieurs. On établira la formule qui donne Pappus et Pascal :

(1) $$[(b \wedge c') \wedge (b' \wedge c), (c \wedge a') \wedge (c' \wedge a), (a \wedge b') \wedge (a' \wedge b)] =$$

$$[a, a', b][b, b', c][c, c', a][a', b', c'] - [a, a', c'][b, b', a'][c, c', b'][a, b, c]$$

et on en déduira le théorème.

12.5 La preuve par le théorème de Noether

Elle fait appel à des notions de géométrie algébrique. Voir la Partie III de mon livre :
`http://www.math.u-psud.fr/ perrin/Livre_de_geometrie_projective.html`

TER numéro 13

La géométrie projective linéaire

Ce TER a été proposé par Marie-Claude David, à partir de la Partie I de mon projet de livre de géométrie projective. Voir :

`http://www.math.u-psud.fr/ perrin/Livre_de_geometrie_projective.html`