Université Denis Diderot Paris 7, Semestre Septembre 2005 -janvier 2006

M1 (Maîtrise) "Math-Info", cours d'algèbre

(M. Hindry et D. Mauger)

Corrigé (avec commentaires) de l'examen du 4 janvier 2006.

Les trois exercices étudient divers groupes de Galois d'équations de degré 5 mais sont largement indépendants.

On rappelle les points suivants:
- si $P \in K[X]$ se scinde sur une extension en $P = (X-\alpha_1)\dots(X-\alpha_n)$, l'extension $L := K(\alpha_1, \dots, \alpha_n)$ est galoisienne sur K, le groupe de Galois $\mathrm{Gal}(L/K)$ *s'appelle le groupe de Galois du polynôme P (sur le corps K) et peut naturellement être vu comme un sous-groupe de $\mathcal{S}_n$. Si de plus le polynôme P est irréductible, l'action du groupe de Galois sur les racines est transitive (voir par exemple le cours).*
- Un groupe de cardinal 15 est cyclique; un groupe de cardinal 30 contient un sous-groupe de cardinal 15 (voir par exemple le partiel).

Exercice A.

Soit G un sous-groupe de $\mathcal{S}_5$ agissant transitivement sur l'ensemble $X = \{1,2,3,4,5\}$.

A.1) *Montrer que le groupe G contient un 5-cycle.*

L'action possède une seule orbite donc, si l'on note G_1 le stabilisateur de $1 \in X$, la formule des classes donne une bijection entre G/G_1 et X donc $|G| = 5|G_1|$ est divisible par 5. Le groupe G contient donc un élément d'ordre 5 qui ne peut être qu'un 5-cycle dans $\mathcal{S}_5$.

A.2) *Rappeler pourquoi, si G contient une transposition, alors $G = \mathcal{S}_5$.*

On a vu en cours et TD que, si n est premier, un n-cycle σ et une transposition τ engendre $\mathcal{S}_n$; en effet (brièvement) quitte à renuméroter les éléments on a $\tau = (1,2)$, et, quitte à remplacer σ par une puissance σ^r (avec $0 < r < n$), on peut supposer $\sigma(1) = 2$ et comme n premier σ^r est encore un n-cycle. Quitte à rechanger la numérotation, on peut donc supposer $\tau = (1,2)$ et $\sigma = (1,2,3,\dots,n)$; alors $\sigma^r \tau \sigma^{-r} = (r+1, r+2)$ et ces transpositions engendrent $\mathcal{S}_n$.

Noter que l'argument ne marche pas si n n'est pas premier: par exemple si $n = 4$ et $\sigma = (1,2,3,4)$ et $\tau = (1,3)$ alors, comme $\tau\sigma\tau^{-1} = \sigma^{-1}$, les éléments σ et τ engendre un sous-groupe isomorphe à D_4. Par contre σ et $\tau' := (1,2)$ engendrent bien $\mathcal{S}_4$.

A.3) *Montrer que G ne peut pas avoir pour cardinal* 15 *ou* 30.

Si $|G| = 15$ alors G est cyclique et contient donc un élément d'ordre 15, mais $\mathcal{S}_5$ ne contient aucun élément d'ordre 15. Si $|G| = 30$ il contient un sous-groupe de cardinal 15, ce qui est impossible.

A.4) *Soit K un 2-sous-groupe de Sylow de $\mathcal{S}_5$, montrer qu'il contient une transposition. En déduire que G ne peut pas être de cardinal 40.*

Une transposition de $\mathcal{S}_5$ (disons $\tau = (1,2)$) est un élément d'ordre 2 donc est contenu dans un 2-sous-groupe de Sylow P_0. Un 2-sous-groupe de Sylow P est conjugué de P_0, i.e. $P = gP_0g^{-1}$ donc la transposition $g\tau g^{-1} = (g(1), g(2))$ appartient à P. Si on avait $|G| = 40$, il contiendrait un sous-groupe de cardinal 8, donc un 2 sous-groupe de Sylow de $\mathcal{S}_5$ et donc une transposition; d'après la question A.2) on aurait $G = \mathcal{S}_5$.

A.5) *Montrer que, si G contient une double transposition, alors $G = \mathcal{S}_5$ ou $\mathcal{A}_5$ ou est de cardinal* 10 *ou* 20.

Une double transposition est d'ordre 2 donc 5 et 2 divise $|G|$ qui divise $|\mathcal{S}_5| = 120$. Donc *a priori* $|G| = 10m$ avec $m \in \{1, 2, 3, 4, 6, 12\}$. On a vu que $m = 3$ (voir A.3) ou 4 (voir A.4) était exclu; si $m = 6$ alors $|G| = 60$ et G est distingué dans $\mathcal{S}_5$ donc $G = \mathcal{A}_5$, si $m = 12$, alors $G = \mathcal{S}_5$.

A.6) *Décrire un sous-groupe de cardinal 10 (resp. 20) dans $\mathcal{S}_5$. [Indication : on pourra poser $\sigma = (1,2,3,4,5)$, $\tau = (1,4)(2,3)$ et $\rho = (1,2,4,3)$ et considérer les sous-groupes engendrés par σ, τ puis par σ, ρ.]*

L'élément σ est d'ordre 5, engendrant $H \cong \mathbf{Z}/5\mathbf{Z}$, l'élément τ est d'ordre 2, engendrant $K \cong \mathbf{Z}/2\mathbf{Z}$, l'élément ρ est d'ordre 4, engendrant $L \cong \mathbf{Z}/4\mathbf{Z}$. Les ensembles $H \cdot K$ et $H \cdot L$ sont de cardinal 10 et 20 respectivement, car $H \cap K = H \cap L = \{id\}$. On a $\tau\sigma\tau^{-1} = \sigma^{-1}$ donc τ (et K) normalise H et $H \cdot K$ est bien un sous-groupe. On a $\rho\sigma\rho^{-1} = \sigma^2$ donc ρ (et L) normalise H et $H \cdot L$ est bien un sous-groupe.

Remarque. On pouvait construire les sous-groupes en invoquant d'autres arguments. Par exemple, le groupe dièdral D_n agit fidèlement sur les n sommets d'un polygone donc peut être vu comme un sous-groupe de S_n, ainsi $D_5 \subset \mathcal{S}_5$ et on peut montrer que son normalisateur dans $\mathcal{S}_5$ est un sous-groupe de cardinal 20.

A.7) *Soient les polynômes $P = X^5 + 6X + 3$ et $R = X^5 - 6X + 3$. Montrer qu'ils sont irréductibles. En considérant la conjugaison complexe, que pouvez-vous dire du groupe de Galois de P (resp. R)?*

Le critère d'Eisenstein (appliqué avec $p = 3$) montre que P et R sont irréductibles sur $\mathbf{Q}$. Le polynôme P possède une unique racine réelle et donc deux paires de racines complexes conjuguées. La conjugaison complexe induit donc une permutation des 5 racines de P qui est une double transposition; d'après la question A.5, on a $G = \mathcal{S}_5$ ou $\mathcal{A}_5$ ou est de cardinal 10 ou 20. Le polynôme R possède trois racines réelles et donc une paire de racines complexes conjuguées. La conjugaison complexe induit donc une permutation des 5 racines de R qui est une transposition; d'après la question A.2, on a $G = \mathcal{S}_5$. [Note : on peut montrer – mais c'est plus difficile et cela n'était pas demandé – que le groupe de Galois de P est également $\mathcal{S}_5$.]

Exercice B.

Soit $\alpha = \sqrt[5]{3}$ et $\zeta := \exp(2\pi i/5)$ et $L = \mathbf{Q}(\alpha, \zeta)$.

B.1) *Donner le polynôme minimal de α et ζ sur $\mathbf{Q}$.*

Le polynôme $X^5 - 3$ est irréductible (d'après le critère d'Eisenstein avec $p = 3$) et annule α, c'est donc le polynôme minimal de α. Le polynôme minimal de ζ est le polynôme cyclotomique Φ_5 de degré $\phi(5) = 4$: explicitement $\Phi_5 = (X^5 - 1)/(X - 1) = X^4 + X^3 + X^2 + X + 1$.

B.2) *En déduire que* $[L : \mathbf{Q}] = 20$. *Montrer que* $L/\mathbf{Q}$ *est galoisienne; quel est le cardinal de* $G := \mathrm{Gal}(L/\mathbf{Q})$*?*

On a donc $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 5$ et $[\mathbf{Q}(\zeta) : \mathbf{Q}] = 4$, de plus $[\mathbf{Q}(\alpha, \zeta) : \mathbf{Q}(\zeta)] \leq 5$ puisque le degré du polynôme minimal de α sur $\mathbf{Q}(\zeta)$ est inférieur ou égal à 5. On a $[\mathbf{Q}(\alpha, \zeta) : \mathbf{Q}] = [\mathbf{Q}(\alpha, \zeta) : \mathbf{Q}(\zeta)][\mathbf{Q}(\zeta) : \mathbf{Q}] = 4[\mathbf{Q}(\alpha, \zeta) : \mathbf{Q}(\zeta)] \leq 20$ et $[\mathbf{Q}(\alpha, \zeta) : \mathbf{Q}] = [\mathbf{Q}(\alpha, \zeta) : \mathbf{Q}(\alpha)][\mathbf{Q}(\alpha) : \mathbf{Q}] = 5[\mathbf{Q}(\alpha, \zeta) : \mathbf{Q}(\alpha)]$. Ainsi $[\mathbf{Q}(\alpha, \zeta) : \mathbf{Q}]$ est inférieur à 20 et divisible par 4 et 5 donc par 20; il vaut donc 20. L'extension $L/\mathbf{Q}$ est galoisienne car L est le corps de décomposition du polynôme $X^5 - 3$. On a $|\mathrm{Gal}(L/K)| = [L : \mathbf{Q}] = 20$.

B.3) *On définit* σ *par* $\sigma(\alpha) = \zeta\alpha$ *et* $\sigma(\zeta) = \zeta$, *et* ρ *par* $\rho(\alpha) = \alpha$ *et* $\rho(\zeta) = \zeta^2$. *Vérifier que* σ *et* ρ *appartiennent à* G, *déterminer leurs ordres et en déduire qu'ils engendrent* G.

Montrons que σ est l'unique automorphisme de L tel que $\sigma(\alpha) = \zeta\alpha$ et $\sigma(\zeta) = \zeta$. D'après la question précédente, le polynôme $X^5 - 3$ reste irréductible sur $\mathbf{Q}(\zeta)$. Comme α et $\alpha' := \zeta\alpha$ sont deux racines de ce polynôme, l'application $\phi : \mathbf{Q}(\zeta)[X] \to \mathbf{Q}(\alpha\zeta) = L$ (resp. $\phi' : \mathbf{Q}(\zeta)[X] \to \mathbf{Q}(\alpha'\zeta) = L$) qui à P associe $P(\alpha)$ (resp. $P(\alpha')$) induit un isomorphisme noté encore ϕ de $\mathbf{Q}(\zeta)[X]/(P)$ vers L (resp. ϕ' de $\mathbf{Q}(\zeta)[X]/(P)$ vers L). L'automorphisme de L défini par $\phi' \circ \phi^{-1}$ laisse fixe $\mathbf{Q}(\zeta)$ et envoie α sur α', c'est donc σ. On peut procéder de manière analogue pour τ.

On voit aisément que $\sigma^r(\zeta) = \zeta$ et $\sigma^r(\alpha) = \zeta^r\alpha$ et donc σ est d'ordre 5; de même $\rho^r(\zeta) = \zeta^{2^r}$ et $\rho^r(\alpha) = \alpha$ et donc ρ est d'ordre 4. Soit H le sous-groupe engendré par σ et K le sous-groupe engendré par ρ, on a $|H \cdot K| = |H|\,|K| = 20$ donc $H \cdot K = G$ et σ et ρ sont bien générateurs.

B.4) *Démontrer la relation* $\rho\sigma\rho^{-1} = \sigma^2$. *Montrer que* G *contient un unique sous-groupe de cardinal 5; combien de sous-groupes de cardinal 4 le groupe* G *contient-il?*

On calcule $\rho\sigma\rho^{-1}(\alpha) = \rho\sigma(\alpha) = \rho(\zeta\alpha) = \zeta^2\alpha = \sigma^2(\alpha)$ et $\rho\sigma\rho^{-1}(\zeta) = \rho\sigma(\zeta^3) = \rho(\zeta^3) = \zeta = \sigma^2(\zeta)$. Ainsi on a bien $\rho\sigma\rho^{-1} = \sigma^2$. Les théorèmes de Sylow indiquent que le nombre n_5 de sous-groupes d'ordre 5 divise 4 et est congru à 1 modulo 5, donc il y a un unique tel sous-groupe (c'est d'ailleurs $H :=< \sigma >$). De même n_2 est impair et divise 5, il vaut donc 1 ou 5. cependant si on avait $n_2 = 1$ le groupe $K :=< \rho >$ serait distingué et $G = H \cdot K$ serait commutatif, ce qui est faux donc $n_2 = 5$.

B.5) *Décrire toutes les extensions* $\mathbf{Q} \subset F \subset L$ *telles que* $[F : \mathbf{Q}] = 4$ *puis* $[F : \mathbf{Q}] = 5$.

Par le théorème fondamental de Galois, les extensions $\mathbf{Q} \subset F \subset L$ avec $[L : F] = d$ correspondent aux sous-groupes de cardinal d de G et on a $[F : \mathbf{Q}] = 20/d$. Ainsi il y a une unique extension avec $[F : \mathbf{Q}] = 4$, elle correspond au sous-groupe $H :=< \sigma >$, c'est-à-dire $F = \mathbf{Q}(\zeta)$; de même il y a cinq extensions avec $[F : \mathbf{Q}] = 5$, elles correspondent aux sous-groupes de cardinal 4, ce sont donc les extensions $F_r = \mathbf{Q}(\zeta^r\alpha)$ pour $r = 0, 1, 2, 3, 4$.

B.6) *Existe-t-il une extension* $\mathbf{Q} \subset F \subset L$ *telle que* $[F : \mathbf{Q}] = 10$*? Est-elle galoisienne?*

Une telle extension correspond à un sous-groupe d'ordre 2, donc à un élément d'ordre 2 dans G qui existe bien puisque 2 divise $|G|$. Dans $K :=< \rho >$ il y a un seul élément d'ordre 2, c'est $\tau := \rho^2$ et les autres éléments d'ordre 2 dans G sont donc conjugués de τ. Cependant $\rho^2\sigma\rho^{-2} = \sigma^4 = \sigma^{-1}$ donc τ n'est pas centralisé par σ, le sous-groupe engendré par τ n'est pas distingué et l'extension correspondante n'est pas galoisienne sur $\mathbf{Q}$.

B.7) *Montrer qu'il existe une unique extension quadratique (i.e.* $[K_0 : \mathbf{Q}] = 2$*) telle que* $K_0 \subset \mathbf{Q}(\zeta)$*. Montrer que le groupe de Galois* $\mathrm{Gal}(L/K_0)$ *n'est pas abélien et est donc isomorphe au groupe dièdral* D_5*.*

Le groupe de galois $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ est isomorphe (canoniquement) à $(\mathbf{Z}/5\mathbf{Z})^*$ donc (non canoniquement) à $\mathbf{Z}/4\mathbf{Z}$; il contient donc un unique sous-groupe H_0 de cardinal 2 qui correspond donc à une unique extension quadratique $K_0 = \mathbf{Q}(\zeta)^{H_0}$. Le groupe de Galois $\mathrm{Gal}(L/K_0)$ est de cardinal $[L : K_0] = 20/[K_0 : \mathbf{Q}] = 10$ et il est donc isomorphe à $\mathbf{Z}/10\mathbf{Z}$ ou D_5 (Cf Cours). Cependant ce groupe doit contenir $H =< \sigma >$ (seul sous-groupe de cardinal 5) et un élément d'ordre 2 donc $\tau = \rho^2$ ou un conjugué, or cet élément ne commute pas avec σ donc $\mathrm{Gal}(L/K_0)$ n'est pas commutatif et est isomorphe à D_5.

Exercice C.

On pose dans cet exercice $\xi := \exp(2\pi i/11)$ *et* $\eta := \xi + \xi^{-1} = 2\cos(2\pi/11)$.

C.1) *Déterminer* $[\mathbf{Q}(\xi) : \mathbf{Q}]$ *et* $[\mathbf{Q}(\xi) : \mathbf{Q}(\eta)]$ *et en déduire* $[\mathbf{Q}(\eta) : \mathbf{Q}]$.

D'après le cours on sait que $[\mathbf{Q}(\xi) : \mathbf{Q}] = \phi(11) = 10$. L'élément ξ vérifie $\xi + \xi^{-1} = \eta$ ou encore $\xi^2 - \eta\xi + 1 = 0$ et est donc au plus quadratique sur $\mathbf{Q}(\eta)$; comme $\mathbf{Q}(\eta)$ est inclus dans les réels, on a $\xi \notin \mathbf{Q}(\eta)$ donc $[\mathbf{Q}(\xi) : \mathbf{Q}(\eta)] = 2$. On en tire $[\mathbf{Q}(\eta) : \mathbf{Q}] = [\mathbf{Q}(\xi) : \mathbf{Q}]/[\mathbf{Q}(\xi) : \mathbf{Q}(\eta)] = 5$.

C.2) *Montrer que l'extension* $\mathbf{Q}(\eta)/\mathbf{Q}$ *est galoisienne et décrire son groupe de Galois.*

Le groupe de Galois $\mathrm{Gal}(\mathbf{Q}(\xi)/\mathbf{Q})$ est isomorphe à $(\mathbf{Z}/11\mathbf{Z})^*$ et en particulier abélien donc tous ses sous-groupes sont distingués et donc toutes les sous-extension de $\mathbf{Q}(\xi)$ sont galoisiennes sur $\mathbf{Q}$. Le groupe $\mathrm{Gal}(\mathbf{Q}(\eta)/\mathbf{Q})$ est de cardinal 5 donc isomorphe à $\mathbf{Z}/5\mathbf{Z}$.

Remarque. Si on souhaite une description plus précise, on peut rajouter que

$$\mathrm{Gal}(\mathbf{Q}(\eta)/\mathbf{Q}) = \mathrm{Gal}(\mathbf{Q}(\xi)/\mathbf{Q})/\,\mathrm{Gal}(\mathbf{Q}(\xi)/\mathbf{Q}(\eta)).$$

Le groupe $\mathrm{Gal}(\mathbf{Q}(\xi)/\mathbf{Q})$ s'identifie à $(\mathbf{Z}/11\mathbf{Z})^*$ en identifiant m et σ_m donné par $\xi \mapsto \xi^m$ (Cf Cours). Ainsi $\sigma_m(2\cos(2\pi/11)) = 2\cos(2m\pi/11)$; par ailleurs le groupe de Galois de $\mathbf{Q}(\xi)/\mathbf{Q}(\eta)$ est engendré par la conjugaison complexe, c'est-à-dire par σ_{-1}. Ainsi, on a canoniquement

$$\mathrm{Gal}(\mathbf{Q}(\eta)/\mathbf{Q}) = (\mathbf{Z}/11\mathbf{Z})^*/\{\pm 1\}.$$

C.3) *Donner un polynôme de degré 5 dont le groupe de Galois sur* $\mathbf{Q}$ *est isomorphe à* $\mathbf{Z}/5\mathbf{Z}$.

D'après ce qui précède, le polynôme minimal de η sur $\mathbf{Q}$ répond à la question.

[Note: Ce polynôme est égal à $X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1$.]