Université Claude Bernard Lyon I — 2nd semestre 2012/2013
Master I — Théorie de Galois

Partiel, 27 mars 2013, 14h-16h

Les règles du jeu :

1. Vous pouvez utiliser tout résultat du cours... sauf si la question est de démontrer un tel résultat.

2. Les documents, sauf les notes de cours de M. Tchoudjem sur sa page web, ainsi que la communication avec les autres étudiants ne sont pas autorisés.

3. Les questions à l'enseignant sont encouragées.

4. Il y a 4 exercices (25 points à gagner) qui attendent vos réponses. Bon travail...

Exercice 1 (Rappels élémentaires).
(2 pts) *Soient L et K deux corps. On suppose que L est le corps de décomposition d'un polynôme séparable $P \in K[X]$. Montrer que l'action de* $\mathrm{Gal}(L/K)$ *sur les racines de P est transitive si, et seulement si, P est irréductible sur K.*

Réponse : On admet d'abord que $\mathrm{Gal}(L/K)$ agit transitivement sur les racines de P. Supposons par l'absurde que P soit réductible. Comme nous travaillons dans un anneau factoriel, P se factorise en un nombre fini de facteurs irréductibles, disons $P_1, \ldots, P_k$ avec $k > 1$. D'après l'hypothèse de séparabilité, les facteurs sont deux à deux premiers entre eux. Considérons maintenant P_1 et P_2. Si α_1 et α_2 sont racines de P_1 et de P_2 respectivement, alors, d'après l'hypothèse de réductibilité, il existe un automorphisme $\sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma(\alpha_1) = \alpha_2$. Par conséquent, P_1 est égal à P_2 à multiple constant près, en d'autres termes, il existe $k \in K^*$ tel que $P_1 = kP_2$. Ceci contredit l'hypothèse.

Maintenant, on suppose P irréductible sur K. Le polynôme P est de la forme $a\prod_{i=1}^{d}(X - \alpha_i)$, avec $a \in K^*$. Si α_i et α_j sont deux racines de P, alors, P étant irréductible, $K(\alpha_i)$ et $K(\alpha_j)$ sont isomorphes par un K-isomorphisme (le théorème 1.7 du cours du 6/2/13). Par le théorème 1.8 de même cours, cet isomorphisme s'étend à un automorphisme L. La transitivité en découle.

Exercice 2 (Groupes de Galois, léger).
I. (3 pts) *On considère le polynôme $P(X) = (X^2 - p_1)(X^2 - p_2)$ dans $\mathbb{Q}[X]$ où les p_i sont des nombres premiers distincts. On déterminera son groupe de Galois. Voici une recette :*

1. *Déterminer le corps L de décomposition de P.*
2. *Vérifier que $X^2 - p_2$ est irréductible sur le corps de décomposition L_1 de $X^2 - p_1$ sur $\mathbb{Q}$. En déduire le degré $[L : \mathbb{Q}]$.*
3. *Expliciter des automorphismes des L/L_1.*
4. *Conclure.*

Réponse : Suivons la recette.
1. Les racines de P étant $\pm\sqrt{p_1}$ et $\pm\sqrt{p_2}$, $L = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$.
2. Comme p_1 est un nombre premier, il découle de l'unique factorisation des nombres naturels que $X^2 - p_1$ est irréductible dans $\mathbb{Q}[X]$. On définit $L_1 = \mathbb{Q}(\sqrt{p_1})$. L'extension $L_1/\mathbb{Q}$ est un $\mathbb{Q}$-espace vectoriel de dimension 2 dont une base est $(1, \sqrt{p_1})$. Par conséquent, tout élément de L_1 est de la forme $a + b\sqrt{p_1}$ avec $a, b \in \mathbb{Q}$. En particulier, si $\sqrt{p_2} \in L_1$ alors il existe $a, b \in \mathbb{Q}$ tels que $a + b\sqrt{p_1} = \sqrt{p_2}$. En élevant au carré, on obtient $p_2 = a^2 + p_1 b^2 + 2ab\sqrt{p_1}$. Le dernier terme du deuxième membre ne peut que s'annuler. Ainsi $a = 0$ ou $b = 0$. Si $a = 0$, alors $p_2 = p_1 b^2$. Or p_2 étant premier la seule posssibilité qui s'ensuit est $p_2 = p_1$, exclue par hypothèse. Si $b = 0$, alors $p_2 = a^2$, clairement impossible. Il en découle que $[L : \mathbb{Q}] = [L : L_1][L_1 : \mathbb{Q}] = 2.2 = 4$.
3. Tout automorphisme de L_1-espace vectoriel qui permute l'ensemble $\{\pm\sqrt{p_2}\}$ et s'étend par linéarité à L est un automorphisme de L/L_1. Ceci fournit deux possibilités, l'identité et $\sigma : \sqrt{p_2} \longrightarrow -\sqrt{p_2}$. Notons que σ est d'ordre 2.
4. Par symétrie du raisonnement, on obtient un automorphisme d'ordre 2, τ qui envoie $\sqrt{p_1}$ à $-\sqrt{p_1}$ et fixe $L_2 = \mathbb{Q}(\sqrt{p_2})$. Par ailleurs, tout automorphisme de $L = \mathbb{Q}1 \oplus \mathbb{Q}\sqrt{p_1} \oplus \sqrt{p_2} \oplus \sqrt{p_1 p_2}$ stabilise les ensembles $\{\pm\sqrt{p_1}\}$ et $\{\pm\sqrt{p_2}\}$. En d'autres termes, tout automorphisme de L est déterminé par son action sur $\{\sqrt{p_1}, \sqrt{p_2}\}$. Par conséquent $\mathrm{Gal}(L/K)$ est engendré par σ et τ, deux automorphismes qui commutent et qui sont d'ordre 2. Ainsi,

$$\mathrm{Gal}(L/K) \;=\; \{1, \sigma, \tau, \sigma\tau\} \;\equiv\; \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \quad .$$

II. *Soit $P[X]$ un polynôme séparable sur un corps K. On suppose que $P(X) = P_1(X) \dots P_k(X)$, où chaque P_i est irréductible dans $K[X]$ de degré n_i, et que son groupe de Galois G soit cyclique.*

1. (0,5 pt) *Montrer que le groupe de Galois de P agit transitivement sur les racines de chaque P_i.*

   Réponse : C'est une extension du premier exercice. Tous les polynômes en vue sont séparables puisque P l'est. Le corps de décomposition L de P est le composé de ceux des P_i qu'on notera L_i ($1 \leq i \leq k$). D'après l'exercice 1, chaque groupe de Galois $\mathrm{Gal}(L_i/K)$ agit transitivement sur les racines de P_i. Le théorème 1.8 du cours du 6/2/13 permet d'étendre ces automorphismes à L.

2. (1 pt) *Déduire que, quitte à réindexer les racines, G est engendré par un produit de k cycles de la forme*

$$(1\ 2\ \dots\ n_1)(n_1+1\ \dots\ n_1+n_2)\ \dots\ (n_1+\dots+n_{k-1}+1\ \dots\ n_1+\dots+n_k) \quad .$$

   Réponse : Soit σ un générateur de $G = \mathrm{Gal}(L/K)$. On commence avec quelques remarques :

   (i) Si x est une racine de P, alors $\sigma(x) = x$ si et seulement si $x \in K$, si et seulement si le facteur P_i dont x est racine, est linéaire. En effet, $\sigma(x) = x$ si et seulement si $\sigma^i(x) = x$ pour tout $i \in \mathbb{N}$, si et seulement si G fixe x. Cette dernière conclusion équivaut à ce que $x \in K$ puisque L/K est galoisienne.

   (ii) Comme P est séparable, pour toute racine x de P, x est racine de P_i si et seulement si $\sigma(x)$ est racine de P_i.

(iii) Comme chaque P_i est irréductible et que σ engendre G, d'après la remarque (i), si on fixe une racine de x_{i1} de P_i pour chaque $1 \leq i \leq k$, alors les autres racines de P_i sont de la forme $\sigma^j(x_{i1})$ ($j \in \mathbb{N}$).

Il découle de ces remarques que l'ensemble des racines se répartit en k parties $\{x_{i1}, \sigma(x_{i1}), \ldots, \sigma^{n_i-1}(x_{i1})\}$ ($1 \leq i \leq k$). Sur chaque ensemble σ induit un n_i-cycle respectivement. En particulier, chacune de ces classes est une orbite sous l'action de G. On définit alors le morphisme $G \longrightarrow S_{\sum_{i=1}^{k} n_i}$ qui associe à sigma la permutation de l'énoncé. C'est un isomorphisme entre G est le sous-groupe de permutations engendré par la permutation de l'énoncé.

Exercice 3 (Corps finis).
On étudie le corps à 8 éléments.

1. (0,5 pt) *Montrer, en les explicitant, qu'il existe deux polynômes irréductibles de degré 3 sur $\mathbb{F}_2$.*

   Réponse : Evidemment, un polynôme irréductible dans $\mathbb{F}_2[X]$, et d'ordre 3 doit avoir la forme générale $1 + a_1X + a_2X^2 + X^3$. Il suffit ensuite de trouver les combinaisons de a_1 et de a_2 convenables. Le polynôme étant de degré 3, cette recherche se réduit à la détermination des polynômes qui n'ont pas de racine dans $\mathbb{F}_2$, en d'autres termes qui ont un nombre impair de termes non nuls. Les deux possibilités sont $P_1 = 1 + X + X^3$ et $P_2 = 1 + X + X^2$.

2. (3 pts) *Expliciter tous les isomorphismes possibles entre les deux présentations du corps à 8 éléments, fournies par les deux polynômes du point précédent.*

   Réponse : Chacun des deux polynômes déterminés dans le premier point fournit une présentation du corps à 8 éléments, $\mathbb{F}_2[X]/(P_1)$ et $\mathbb{F}_2[X]/(P_2)$ respectivement. On définit $\alpha = X + (P_1)$ et $\beta = X + (P_2)$. Alors, α est une racine du polynôme P_1 et β en est une de P_2. Notons au passage que α et β engendrent le groupe multiplicatif. En effet, comme ce groupe a 7 éléments, tout membre non nul en est un générateur.

   En calculant modulo l'identité $\alpha^3+\alpha+1 = 0$, on détermine que α^2 et α^4 présentent les autres racines du polynôme P_1. Par conséquent, les racines de P_2 sont présentées par $\{\alpha^2, \alpha^5, \alpha^7\}$. Dans la présentation avec le polynôme P_2, des calculs modulo l'identité $\beta^3 + \beta^2 + 1 = 0$ montrent que les racines de P_2 sont $\{\beta, \beta^2, \beta^4\}$. Par conséquent, $\{\beta^3, \beta^5, \beta^7\}$ sont les racines de P_1.

   Le fait que le groupe multiplicatif soit cyclique engendré par α dans la présentation modulo P_1, montre qu'il suffit de déterminer les images de α pour déterminer les isomorphismes possibles de la présentation qui utilise P_1 vers la présentation qui utilise P_2. Avec les données du paragraphe précédent, il y a trois possibilités : $\alpha \longmapsto \beta^3$ $\alpha \longmapsto \beta^5$, $\alpha \longmapsto \beta^6$.

Exercice 4 (Groupes de Galois, gastronomique).
On étudie des extensions de $\mathbb{Q}$. On commence avec le polynôme suivant dans $\mathbb{Q}[X]$.

$$P(X) \;=\; X^3 - 3X - 1 \;.$$

1. (1.5 pts) *Montrer que ce polynôme est irréductible sur $\mathbb{Q}$.* (*Changement de variable.*)
   Réponse : Quand on remplace X par $X+1$, le polynôme P devient X^3+3X^2-3, auquel on peut appliquer Eisenstein en utilisant le nombre premier 3.

   On admettra que P a trois racines $\alpha_1, \alpha_2, \alpha_3$ telles que

   $$\alpha_3 < \alpha_2 < 0 < \alpha_1 \quad .$$

2. (1.5 pts) *Montrer que si α est racine de P, alors il en est de même pour $-1 - \frac{1}{\alpha}$. En déduire que $K = \mathbb{Q}(\alpha_1)$ est une extension galoisienne de $\mathbb{Q}$, et le cardinal de* $\mathrm{Gal}(K/\mathbb{Q})$.
   Réponse : Pour répondre à la première question il suffit de faire le calcul en utilisant l'identité rationnelle $\alpha^3 - 3\alpha - 1 = 0$. Comme la trace de P (la somme des trois racines) est nulle et que α_1 est une racine de P, la réponse à la première question implique que α_1, $-1 - \frac{1}{\alpha_1}$ et $1 + \frac{1}{\alpha_1} - \alpha_1$ sont les trois racines de P. Il en découle que toutes les racines sont contenues dans $\mathbb{Q}(\alpha_1)$. Ainsi, $\mathbb{Q}(\alpha_1)$ est aussi le corps de décomposition de P, et $\mathbb{Q}(\alpha_1)/\mathbb{Q}$ est une extensions galoisienne. Il s'ensuit que $\mathrm{Gal}(\mathbb{Q}(\alpha_1)/\mathbb{Q}) = [\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 3$.
3. (1 pt) *On définit $\beta_1, \beta_2, \beta_3 \in \mathbb{C}$ tels que $\beta_i^2 = \alpha_i$. Montrer qu'on peut choisir les β_i telles que $\beta_1\beta_2\beta_3 = 1$. On définit $L = K(\beta_1, \beta_2, \beta_3)$. Montrer que $L/\mathbb{Q}$ est une extension galoisienne en explicitant un polynôme séparable dont L est le corps de décomposition sur $\mathbb{Q}$.*
   Réponse : Par définition, $\beta_i^2 = \alpha_i$ pour chaque $i = 1, 2, 3$. Comme, par ailleurs $\alpha_1\alpha_2\alpha_3 = 1$, $(\beta_1\beta_2\beta_3)^2 = 1$. Par conséquent $\beta_1\beta_2\beta_3 = \pm 1$. Une fois un choix donnant $\beta_1\beta_2\beta_3 = 1$ est fait, on définit $L = K(\beta_1, \beta_2, \beta_3)$, qui est une extension galoisienne, le polynôme étant $Q = X^6 - 3X^2 - 1$, un polynôme séparable dont L est le corps de décomposition.
4. (2 pts) *Montrer que $[K(\beta_1) : K] = 2$.* (*Vous pouvez utiliser les images possibles de β_1 sous l'action des extensions des éléments de* $\mathrm{Gal}(K/\mathbb{Q})$ *à L.*)
   Réponse : Par définition, $\beta_1^2 = \alpha_1$, ce dernier appartient à K. Ainsi, $[K(\beta_1) : K] \leq 2$. La question est si $[K(\beta_1) : K] = 2$. Ceci équivaut à vérifier si $X^2 - \alpha_1$ est irréductible dans $K[X]$.
   Soit maintenant σ un générateur de $\mathrm{Gal}(\mathbb{Q}(\alpha_1)/\mathbb{Q})$. Le groupe $\mathrm{Gal}(\mathbb{Q}(\alpha_1)/\mathbb{Q})$ agit sur $\{\alpha_1, \alpha_2, \alpha_3\}$, et $\sigma(\alpha) \in \{\alpha_2, \alpha_3\}$. On note que σ s'étend à un automorphisme puisque L est le corps de décomposition de Q non seulement sur $\mathbb{Q}$ mais aussi sur K (le théorème 1.8 du cours du 6/2/13). Ce prolongement sera noté σ aussi. Comme α_2 et α_3 sont négatifs, $\sigma(\beta_1)$, qui est racine carrée de α_2 ou α_3, est complexe. Or $\sigma(K) = K \subset \mathbb{R}$. Ainsi, $\sigma(\beta_1) \notin K$ et $\beta_1 \notin K$.

5. (1 pt) *Montrer que* $L = \mathbb{Q}(\beta_1, \beta_2)$. *Déterminer* $[L : K]$, *et en déduire* $[L : \mathbb{Q}]$.

   Réponse : Par définition $L = K(\beta_1, \beta_2, \beta_3) = \mathbb{Q}(\beta_1, \beta_2, \beta_3, \alpha_1) = \mathbb{Q}(\beta_1, \beta_2, \beta_3)$. Or, $\beta_1\beta_2\beta_3 = 1$. Par conséquent, $\beta_3 \in \mathbb{Q}(\beta_1, \beta_2)$.

   D'un côté $\mathbb{Q}(\beta_1) \subset \mathbb{R}$ tandis que $\beta_2 \in \mathbb{C} \setminus \mathbb{R}$, d'un autre côté $\beta_2^2 = \alpha_2 \in K$. Par conséquent, $[L : K(\beta_1)] = 2$ et $[L : K] = 4$. Ainsi $[L : \mathbb{Q}] = 12$.

6. (i) (2 pts) *On définit* $G = \mathrm{Gal}(L/\mathbb{Q})$ *et* $H = \mathrm{Gal}(L/K)$. *Le sous-groupe* H *est-il distingué dans* G *? Quelle est sa structure ?*

   Réponse : Nous avons déjà vérifié que $K/\mathbb{Q}$ est galoisienne. La correspondance de Galois entraîne alors que $H \lhd G$. Par ailleurs, $L/\mathbb{Q}$ étant galoisienne, il découle toujours de ladite correspondance que $|H| = [L : K] = 4$.

   Décrivons la structure de H. Si $\theta \in H \setminus \{1\}$, alors forcément, $\theta(\beta_1)$ est racine de $X^2 - \alpha_1$. Par conséquent, $\theta(\beta_1) = \pm\beta_1$. Par un raisonnement similaire, θ permute les racines de $X^2 - \alpha_2$. Par conséquent, θ est d'ordre au plus 2. Ainsi $H \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

   (ii) (2 pts) *Montrer que* G *n'est pas abélien. En déduire que les* 3*-Sylow de* G *ne sont pas distingués.*

   Réponse : L'automorphisme σ du point 4 ne stabilise pas $K(\beta_1)$. Par conséquent, $K(\beta_1)/\mathbb{Q}$ n'est pas galoisienne, et $\mathrm{Gal}(L/K(\beta_1))$ n'est pas distingué dans G. Ceci implique en particulier que G n'est pas abélien. La non-commutativité de G force les 3-Sylow à ne pas être distingués, parce que dans le cas contraire G, étant d'ordre 12 avec un sous-groupe distingué d'ordre 4, serait abelien.

7. (4 pts) *On définit* $\theta = \beta_1 + \beta_2 + \beta_3$. *Montrer en les explicitant que* θ *a quatre images possibles sous l'action de* G. *En déduire* $[\mathbb{Q}(\theta) : \mathbb{Q}]$. *Cette extension est-elle galoisienne ?*

   Réponse : Soit $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Comme $\sigma(\beta_i)^2 = \alpha_j$ pour chaque $i, j = 1, 2, 3$, $\sigma(\beta_i) = \pm\beta_j$ pour les valeurs correspondantes de i et j. Par ailleurs, $\sigma(\beta_1\beta_2\beta_3) = \sigma(1) = 1$. On aboutit alors aux possibilités suivantes :

   (i) σ fixe β_1 : alors soit σ échange β_2 et β_3, soit il échange β_2 et $-\beta_3$, soit il échange β_2 avec $-\beta_2$ et β_3 avec $-\beta_3$, soit il est neutre. Dans tous les cas, soit θ reste fixe, soit il devient $\beta_1 - \beta_2 - \beta_3$.

   (ii) σ échange β_1 avec $-\beta_1$: alors soit σ échange β_2 avec $-\beta_2$ et fixe β_3, soit il échange β_3 avec $-\beta_3$ et fixe β_2. Les images possible pour θ dans ce cas sont $-\beta_1 \pm \beta_2 \mp \beta_3$.

   (iii) soit σ envoie β_1 à β_2, β_2 à β_3, β_3 à β_1, soit β_1 à β_2, β_2 à $-\beta_3$, β_3 à $-\beta_1$, soit β_1 à $-\beta_2$, β_2 à β_3, β_3 à $-\beta_1$, soit β_1 à $-\beta_2$, β_2 à $-\beta_3$, β_3 à β_1. On retrouve les possibilités déjà découvertes pour les images de θ.

   (iv) le cas (iii) est repris après avoir echangés les rôles de β_2 et β_3.

   Au total, on trouve 4 images possibles pour θ. L'extension L/K étant séparable, le polynôme minimal de θ sur $\mathbb{Q}$ est de degré 4 (le théorème 3.6 du cours du 20/2/13). Par conséquent $\mathrm{Gal}(L/\mathbb{Q}(\theta))$ est d'ordre 3, donc un 3-Sylow de G. Nous avons déjà vérifié que les 3-Sylow ne sont pas distingués dans g, ce qui a comme conséquence que $\mathbb{Q}(\theta)/\mathbb{Q}$ n'est pas galoisienne.