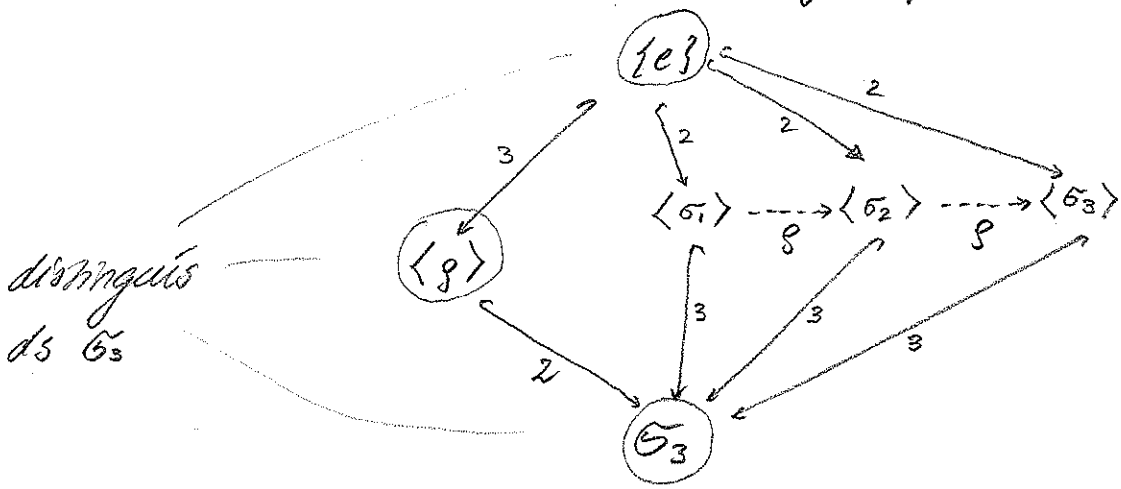
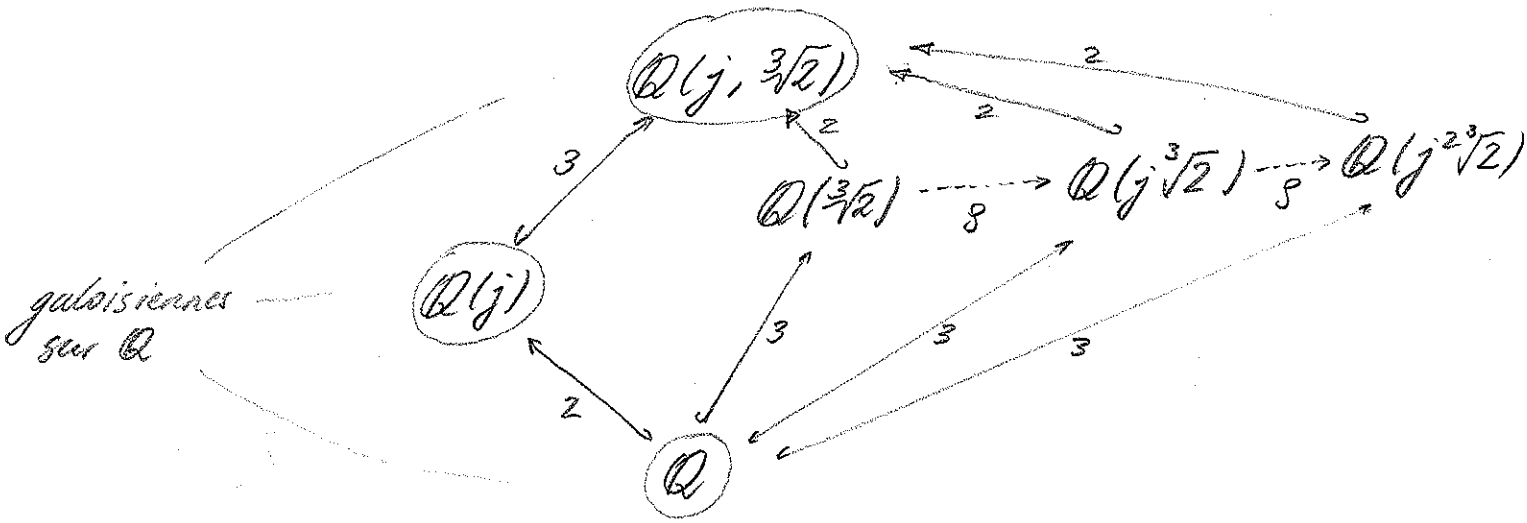
L'ensemble ordonné de ses sous-groupes est :



Dans l'isomorphisme $G \xrightarrow{\sim} \mathfrak{S}_3$, σ_1 correspond à la conjugaison complexe et S à la permutation cyclique des racines. Nous obtenons l'ens. ordonné des ss-corps :



2.5 Extensions cyclotomiques

Soient K un corps et n un entier ≥ 1. On suppose que n n'est pas multiple de $\mathrm{car}(K)$.

Notation : $\mu_n(K) = \{x \in K \mid x^n = 1\}$.

Rque : $\mu_n(K)$ est un groupe cyclique. Son ordre divise n et n'est pas multiple de $\mathrm{car}(K)$.

Déf: Un <u>corps cyclotomique de niveau n</u> sur K est un corps de décomposition de $X^n - 1$.

<u>Prop. 1</u>: Soit $L \supseteq K$ un corps cyclotomique de niveau n.

a) L contient exactement n racines n-ièmes de 1.

b) L'extension $L \supseteq K$ est galoisienne et on a un plongement $Gal(L/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$.

c) On a $[L:K] \leq \varphi(n)$.

Dém.: Le polynôme $X^n - 1$ est séparable car premier avec sa dérivée. Cela donne c) et le caractère galoisien de $L \supseteq K$. Tout $\sigma \in Gal(L/K)$ induit un automorphisme de $\mu_n(L)$ et cet autom. détermine σ. D'où un plongement

$$Gal(L/K) \hookrightarrow Aut(\mu_n(L)).$$

On a $Aut(\mu_n(L)) \cong Aut((\mathbb{Z}/n\mathbb{Z}, +)) \simeq (\mathbb{Z}/n\mathbb{Z})^*$, ce qui donne b). Puisque $Gal(L/K)$ est d'ordre $[L:K]$, on obtient c). ✓

<u>Prop 2</u>: Si L est une extension cyclotomique de niveau n de $\mathbb{Q}$, alors $Gal(L/\mathbb{Q})$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$.

Dém.: L est engendré sur $\mathbb{Q}$ par une racine primitive n-ième de 1. Donc L est le corps de rupture du polynôme cyclotomique Φ_n. Or Φ_n est de degré $\varphi(n)$. Donc L est de degré $\varphi(n)$ sur $\mathbb{Q}$, et $Gal(L/K)$ d'ordre $\varphi(n)$. D'où l'affirmation grâce à la prop. 1. ✓

2.6 Extensions cycliques

Soient K un corps et n un entier ≥ 2.

Hypothèse : Le groupe $\mu_n(K) = \{x \in K / x^n = 1\}$ est d'ordre n. (*)

Rques : 1) Par abus, on dit parfois "K contient toutes les racines n-ièmes de 1" au lieu de (*).

2) Pour que (*) soit vraie, il est nécessaire (mais non suffisant) que n ne soit pas multiple de $\mathrm{car}(K)$.

Lemme 1 : Soit $a \in K$. Si une extension $L \supseteq K$ est engendrée par une racine x de $X^n - a$, alors $L \supseteq K$ est galoisienne et on a un plongement can. $\mathrm{Gal}(L/K) \hookrightarrow \mu_n(K)$. En particulier, $\mathrm{Gal}(L/K)$ est cyclique.

Déf : Un extension cyclique de K est une extension galoisienne de groupe de Galois cyclique.

Dém. du lemme : Les σx, $\sigma \in \mu_n(K)$, forment l'ens. des racines de $X^n - a$. Donc $L \supseteq K$ est galoisienne en tant que corps de décomposition d'un polynôme séparable. Tout $\sigma \in \mathrm{Gal}(L/K)$ permute les racines de $X^n - a$ et est déterminé par l'image de x. D'où le plongement

$$\mathrm{Gal}(L/K) \hookrightarrow \mu_n(K), \quad \sigma \longmapsto \sigma(x)/x. \quad \checkmark$$

Prop 2 : Soit $a \in K$. Supposons que a n'est pas une puissance d-ième, pour tout diviseur $d > 1$ de n. Alors $P = X^n - a$ est irréductible et son corps de rupture $L \supseteq K$ est une ext. galoisienne de gr. de Galois $\mu_n(K)$.

Dém.: Soit L un corps de décomposition de P et $x \in L$ une racine de P. On a

$$P = \prod_{\zeta \in \mu_n(K)} (X - \zeta x)$$

dans $L[X]$. Soit $Q \in K[X]$ un facteur irréd. unitaire de P. Alors son coeff. constant est produit de e de P. Alors son coeff. constant est produit de e facteurs ζx, $\zeta \in \mu_n(K)$. Comme les ζ sont dans K, il s'ensuit que x^e est dans K. Par le thm. de Bézout, il s'ensuit que x^δ est dans K, où $\delta = \mathrm{PGCD}(n, e)$. Mais alors, on a $a = x^n = (x^\delta)^{\delta/n}$. Par l'hypothèse sur a, on a $\delta/n = 1$. Donc $e = n$ et $Q = P$. Comme L est engendré par x, L est le corps de rupture de P et $|\mathrm{Gal}(L|K)| = [L:K] = n = \mu_n(K)$. Le lemme 1 donne l'affirmation. ✓

Thm 3 (Kummer[1]): Soit $L \supseteq K$ une extension cyclique d'ordre n (i.e. de groupe de Galois cyclique d'ordre n). Alors il existe $a \in K$ tq. L soit un corps de décomposition de $X^n - a$.

Dém.: Soit g un générateur de $\mathrm{Gal}(L|K)$. On considère g comme un endomorphisme K-linéaire de L. On a $g^n = \mathbb{1}_L$ et $X^n - 1$ est scindé à racines simples dans K. Donc g est diagonalisable. Les valeurs propres de g forment un SS-groupe de $\mu_n(K)$ comme le montre la formule $g(xy^{-1}) = g(x)\,g(y)^{-1}$, $x, y \in L^\times$. Ce SS-groupe est cyclique d'ordre d pour un

[1] Eduard Kummer, 1810 (Sorau) – 1893 (Berlin)

diviseur d de n. On a $g^d = 1_L$ et donc $d=n$ (car g est d'ordre n). Donc il existe un vecteur propre $x \in L \setminus \{0\}$ de valeur propre une racine primitive n-ième ζ. Comme L est galoisienne sur K, le polynôme minimal de x est

$$\prod_{i=0}^{n-1} (X - g^i x) = \prod_{i=0}^{n-1} (X - \zeta^i x) = X^n - a$$

pour un certain $a = x^n$ dans K. ✓

2.7 Polynômes symétriques, discriminant

Soient A un anneau commutatif et n un entier ≥ 1.
Le groupe symétrique $\mathfrak{S}_n$ agit sur $A[X_1, \dots, X_n]$ par

$$(\sigma P)(X_1, \dots, X_n) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$$

où $P \in A[X_1, \dots, X_n]$ et $\sigma \in \mathfrak{S}_n$.

Déf : Un polynôme $P \in A[X_1, \dots, X_n]$ est <u>symétrique</u> si $\sigma P = P$, $\forall \sigma \in \mathfrak{S}_n$.
Les <u>polynômes symétriques élémentaires</u> sont les coeff. σ_i dans

$$\prod_{i=1}^{n} (T - X_i) = T^n - \sigma_1 T^{n-1} + \dots + (-1)^n \sigma_n$$

Rques : 1) On a $\sigma_1 = X_1 + \dots + X_n$, $\sigma_k = \sum_{i_1 < \dots < i_k} X_{i_1} \cdots X_{i_k}$, $\sigma_n = X_1 \cdots X_n$.

2) Les polynômes sym. forment une ss-alg. $A[X_1, \dots, X_n]^{\mathfrak{S}_n}$ de $A[X_1, \dots, X_n]$.

<u>Thm 1</u> : Pour tout polynôme sym. P, il existe un unique polynôme $S \in A[Y_1, \dots, Y_n]$ t.q. $P = S(\sigma_1, \dots, \sigma_n)$.

<u>Rque</u> : On a donc un isom. de A-algèbres

$$A[Y_1, \dots, Y_n] \xrightarrow{\sim} A[X_1, \dots, X_n]^{\mathfrak{S}_n}, \quad Y_i \longmapsto \sigma_i .$$

Dém. : Soit d le degré total de P. On procède par récurrence sur les couples (n,d) ordonnés lexicographiquement. L'affirmation est claire pour $n=1$ ou $d=0$. Supposons $n \geq 2$ et $d \geq 1$.

Soit

$$P_0(X_1, \dots, X_{n-1}) := P(X_1, \dots, X_{n-1}, 0).$$

Alors P_0 est symétrique en $n-1$ variables. Donc

$$P_0(X_1, \dots, X_{n-1}) = Q(\sigma_1^{(n-1)}, \dots, \sigma_{n-1}^{(n-1)})$$

pour un unique $Q \in A[Y_1, \dots, Y_{n-1}]$, où les $\sigma_k^{(n-1)}$ sont les polynômes sym. élém. en $n-1$ variables. On a

$$\sigma_k^{(n-1)} = \sigma_k(X_1, \dots, X_{n-1}, 0).$$

Il s'ensuit que

$$P - Q(\sigma_1, \dots, \sigma_{n-1})$$

s'annule pour $X_n = 0$. Par symétrie, il s'annule pour $X_k = 0$, pour tout $1 \leq k \leq n$. Donc tout monôme qui apparaît dans $P - Q(\sigma_1, \dots, \sigma_{n-1})$ avec un coefficient non nul est multiple de $\sigma_n = X_1 \cdots X_n$. Par conséquent, on a

$$P - Q(\sigma_1, \dots, \sigma_{n-1}) = \sigma_n \cdot R$$

pour un polynôme $R \in A[X_1, \dots, X_n]$, qui est symétrique (!). Puisque R est de degré total $< d$, l'hypothèse de récurrence s'applique et il existe un unique $T \in A[Y_1, \dots, Y_n]$ t.q. $R = T(\sigma_1, \dots, \sigma_n)$. Ainsi, on a

$$P = Q(\sigma_1, \dots, \sigma_{n-1}) + \sigma_n \cdot T(\sigma_1, \dots, \sigma_n).$$

et

$$S = Q(Y_1, \dots, Y_{n-1}) + Y_n T(Y_1, \dots, Y_n) \qquad (*)$$

convient. Cela montre l'existence. Pour l'unicité, supposons que

Si $S \in A[Y_1, \dots, Y_n]$ vérifie $S(\sigma_1, \dots, \sigma_n) = 0$. Ecrivons S sous la forme $(*)$. En prenant $Y_n = 0$, on voit que $Q(\sigma_1^{(n-1)}, \dots, \sigma_{n-1}^{(n-1)}) = 0$ donc $Q = 0$ (par l'hyp. de réc.) et $T(\sigma_1, \dots, \sigma_n) = 0$ ce qui donne $T = 0$ (par l'hyp. de réc. car T est de degré plus petit que S). ✓

Soit K un corps.

Cor. 2 : L'extension $K(\sigma_1, \dots, \sigma_n) \subseteq K(X_1, \dots, X_n)$ est galoisienne de groupe de Galois $\mathfrak{S}_n$ (agissant par permutation des variables).

Dém. : Par le lemme d'Artin, il suffit de montrer que $K(\sigma_1, \dots, \sigma_n)$ est le corps des points fixes de $\mathfrak{S}_n$ agissant dans $K(X_1, \dots, X_n)$.

Clairement, on a $K(\sigma_1, \dots, \sigma_n) \subseteq K(X_1, \dots, X_n)^{\mathfrak{S}_n}$.

Réciproquement, soit $f \in K(X_1, \dots, X_n)$. Ecrivons $f = P/Q$, où $P, Q \in K[X_1, \dots, X_n]$ et $Q \neq 0$. On a

$$f \cdot \prod_{\sigma \in \mathfrak{S}_n} \sigma Q \in K[X_1, \dots, X_n]^{\mathfrak{S}_n}.$$

Donc

$$f \cdot \prod_{\sigma \in \mathfrak{S}_n} \sigma Q = R(\sigma_1, \dots, \sigma_n)$$

pour un unique $R \in K[Y_1, \dots, Y_n]$ et on a

$$f = \frac{R(\sigma_1, \dots, \sigma_n)}{\prod_{\sigma \in \mathfrak{S}_n} \sigma Q} \in K(\sigma_1, \dots, \sigma_n). \quad ✓$$

Soit

$$D := \prod_{i<j} (X_i - X_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (X_i - X_j)$$

Clairement, on a $D \in \mathbb{Z}[X_1, \dots, X_n]^{\mathfrak{S}_n}$.