Une extension L de K comme dans le théorème est un *corps de rupture de P sur K.*

En particulier $1, \alpha, ..., \alpha^{\deg P - 1}$ *est une $K-$base de α.*

Exemple : $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(j\sqrt[3]{2}), \mathbb{Q}(j^2\sqrt[3]{2})$ sont des corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$.

Corollaire 1.6.1 *Si $P \in K[X]$ est irréductible, il existe toujours un corps de rupture de P sur K, unique à isomorphisme près.*

Réalisation du corps de rupture

Si $P(X) = X^n + a_1 X^{n-1} + ... + a_n \in K[X]$ est irréductible, alors $K[X]/(P) \simeq K[A]$ où A est la matrice :

$$\begin{pmatrix} 0 & & 0 & -a_n \\ 1 & \ddots & & \vdots \\ 0 & & 0 & \\ \vdots & \ddots & & \\ 0 & 0 & 1 & -a_1 \end{pmatrix} \in \mathscr{M}_n(\mathbb{K})$$

Par exemple : $\mathbb{C} \simeq \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$ et $\mathbb{F}_{25} \simeq \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} : a, b \in \mathbb{F}_5 \right\}$

1.5 Corps de décomposition

Soit $0 \neq P \in K[X]$. On suppose que $E \geq K$ est un corps où P est scindé : $P = c(X - x_1)...(X - x_n)$, $c \in K^\times$. On dit que $K(x_1, ..., x_n)$ est le *corps de décomposition* de P dans E.

Proposition 1.7 *Un cops de décomposition existe toujours.*

Démonstration : Par récurrence sur $\deg P$ en utilisant l'existence de corps de rupture. **Q.e.d.**

Nous allons voir qu'il y a unicité à isomorphisme près.

Théorème 1.8 (prolongement d'isomorphisme) *Soit $\sigma : K \to K'$ un isomorphisme de corps. Soit $P \in K[X]$ un polynôme irréductible. Alors $P^\sigma \in K'[X]$ est irréductible. Si α, α' sont des racines de P et P^σ dans des extensions de K, K', alors σ se prolonge en un isomorphisme $K(\alpha) \simeq K'(\alpha')$ qui envoie α sur α'.*

Théorème 1.9 (unicité du corps de décomposition) *Soit $\sigma : K \to K'$ un isomorphisme de corps. Soit $P \in K[X]$. Soit $E \geq K$ un corps où P est scindé :$P = c(X - x_1)...(X - x_n)$. Soit $E' \geq K'$ un corps où P^σ est scindé : $P^\sigma = c'(X - x'_1)....(X - x'_n)$. Soient $B := K(x_1, ..., x_n), B' := K'(x'_1, ..., x'_n)$. Alors σ se prolonge en un isomorphisme $B \simeq B'$.*

Corollaire 1.9.1 *Soient L, L' deux corps de décomposition de P sur K. Alors il existe un $K-$isomorphisme $L \simeq L'$.*

Exemples : soient q une puissance d'un nombre premier p ; le corps $\mathbb{F}_q$ est un corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$ et on a donc l'unicité à isomorphisme près des corps finis de cardinaux donnés.

Définition 2 *On dit qu'un corps K est algébriquement clos si tout polynôme non constant est scindé sur K.*

Théorème 1.10 *Soit K un corps. Il existe une extension algébrique $\overline{K}$ de K qui est un corps algébriquement clos. C'est une clôture algébrique de K. L'extension $\overline{K}$ est unique à $K-$isomorphisme près.*

Démonstration :
Existence : soit $\mathscr{P}$ l'ensemble des polynômes irréductibles unitaires de $K[X]$. Pour tout $p \in \mathscr{P}$, on choisit une variable X_p. Soit $A := K[X_p : p \in \mathscr{P}]$. Soit I l'idéal de A engendré par les polynômes $p(X_p)$, $p \in \mathscr{P}$. Alors I est propre donc contenu dans un idéal maximal M. Le corps A/M est une extension algébrique de K et tout polynôme p irréductible sur K a une racine $(X_p \bmod M)$ dans A/M. Cela suffit pour dire que A/M est algébriquement clos (comme nous le verrons plus tard) ...
Unicité : on utilise le lemme de Zorn ... **Q.e.d.**

Exemples : $\mathbb{C}$ (*resp.*$\overline{\mathbb{Q}}$ (*resp.*$\cup_{n\geq 1}\mathbb{C}((t^{1/n}))$)) est une clôture algébrique de $\mathbb{R}$ (*resp.*de $\mathbb{Q}$ (*resp.*de $\mathbb{C}((t))$)).

2 Théorème d'indépendance des caractères d'Artin

Si G est un groupe et K un corps, un caractère de G dans K est un morphisme de groupes $G \to K^\times$. L'ensemble des caractères est une partie du $K-$espace vectoriel des fonctions $G \to K$.

Exemple : $G = \mathbb{Z}/n\mathbb{Z}$, $K = \mathbb{C}$, les caractères de G dans $\mathbb{C}$ sont les $k \mapsto \zeta^k$ où $\zeta = \exp(2i\pi/n)$.

2.1 Indépendance

Théorème 2.1 (Artin) *Soient $\sigma_1, ..., \sigma_n$ n caractères distincts de G dans K. Alors les σ_i sont $K-$linéairement indépendants.*

Corollaire 2.1.1 *Soient E, E' deux corps. Si $\sigma_1, ..., \sigma_n$ sont n morphismes distincts de corps $E \to E'$. Alors les σ_i sont $E'-$linéairement indépendants.*

Exercice : si G abélien, on pose $G^\vee$ le groupe des caractères de G dans $\mathbb{C}$. Montrer que $G^\vee \simeq G$ *(non canonique).*

Exercice : si G fini, $|\mathrm{Hom}(G, K^\times)| \leq |G|$.

2.2 Corps des invariants

Théorème 2.2 *Soient $\sigma_1, ..., \sigma_m$ m morphismes distincts $E \to E'$. Alors si $F := E^{\{\sigma_1,...,\sigma_m\}} := \{x \in E \ : \ \sigma_1(x) = ... = \sigma_n(x)\}$, $[E : F] \geq m$.*

Démonstration : Si $e_1, ..., e_n$ est une famille génératrice de E comme $F-$espace vectoriel, alors les lignes de la matrice $(\sigma_i(e_j))_{\substack{1\leq i\leq m \\ 1\leq j\leq n}} \in \mathscr{M}_{m,n}(E')$ sont indépendantes. Donc $m \leq n$. **Q.e.d.**

Corollaire 2.2.1 *Si G est un sous-groupe fini de $\mathrm{Aut}(E)$, alors $[E : E^G] \geq |G|$.*

Remarque : comme G contient l'identité, $E^G = \{x \in E \ : \ \forall g \in G, \ g(x) = x\}$.

Exemple : $E = \mathbb{C}$, $G = \{1, \sigma\}$ où σ est la conjugaison complexe, $[\mathbb{C} : \mathbb{R}] = 2$.

3 Correspondance de Galois

3.1 Extensions galoisiennes

Définition 3 *Soit E un corps. Soit $G \leq \mathrm{Aut}(E)$ fini. On dit que E/E^G est une extension galoisienne de groupe de Galois G.*

Exemples : $\mathbb{C}/\mathbb{R}$, $\mathbb{F}_{q^n}/\mathbb{F}_q$, $\mathbb{Q}(\zeta)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{C}(X)/\mathbb{C}(X^3)$; *contre-exemple :* $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, $\mathbb{F}_p(X)/\mathbb{F}_p(X^p)$, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$.

Exemple : $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$.

Théorème 3.1 *Soit E un corps. Soit $G \leq \mathrm{Aut}(E)$ un groupe fini. Alors $[E : E^G] = |G|$.*

Démonstration : On utilise la forme $F-$linéaire $\mathrm{Tr} : E \to F$, $x \mapsto \sigma_1(x) + ... + \sigma_n(x)$ où $F = E^G$, $G = \{\sigma_1, ..., \sigma_n\}$. Soient $g_1, ..., g_n$ les éléments de G. Si $e_1, ..., e_{n+1}$ sont des éléments de E, alors les colonnes de la matrices $(g_i(e_j))_{\substack{1\leq i\leq n \\ 1\leq j\leq n+1}} \in \mathscr{M}_{n,n+1}$ sont liées. Donc $\forall\, i$, $\sum_j x_j g_i(e_j) = 0$ pour certains $x_j \in E$. D'où :

$$\forall\, i, \ \sum_j g_i^{-1}(x_j) e_j = 0$$

et $\sum_i \sum_j g_i^{-1}(x_j)e_j = 0 \Rightarrow \sum_j \mathrm{Tr}(x_j)e_j = 0$. C'est encore vrai si on remplace x_j par xx_j, $x \in E$. Donc on peut choisir les x_j tels que $x_1 \in E$ et $\mathrm{Tr}(x_1) \neq 0$ par exemple. Mais alors, les e_j sont liés sur E^G. **Q.e.d.**

Corollaire 3.1.1 (Maximalité du groupe de Galois) *Soit E/F galoisienne de groupe G. Alors si $E' \geq E$ et si $\sigma : E \to E'$ est un $F-$morphisme de corps, $\sigma \in G$. En particulier, $G = \mathrm{Aut}_F(E)$, groupe des automorphismes $F-$linéaires de E.*

Notation : si $F = E^G$, $G =: \mathrm{Gal}(E/F)$.

Corollaire 3.1.2 (Injectivité) *Si E/F est galoisienne de groupe G si $H_1, H_2 \leq G$, alors $E^{H_1} = E^{H_2} \Leftrightarrow H_1 = H_2$.*

Exemples :

a) $k(x_1, ..., x_n)^{\mathfrak{S}_n} = k(s_1, ..., s_n)$ (où k est un corps),

b) $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ est galoisienne de groupe de Galois $G := \langle s, t\rangle \simeq \mathfrak{S}_3$ où s est le $\mathbb{Q}(j)-$automorphisme qui envoie $\sqrt[3]{2}$ sur $j\sqrt[3]{2}$ et t le $\mathbb{Q}(\sqrt[3]{2})-$automorphisme qui envoie j sur j^2 ;

c) soit G le sous-groupe des automorphismes de $\mathbb{C}(t)$ engendré par les changements de variables $t \mapsto t^{-1}$ et $t \mapsto 1 - t$. Montrer que G laisse stable l'ensemble des 3 fonctions :

$$f_1 := t + t^{-1},\ f_2 := 1 - t + (1 - t)^{-1},\ f_3 := 1 - t^{-1} + (1 - t^{-1})^{-1}\ .$$

En déduire que G est isomorphe au groupe S_3.
Soit K le sous-corps des fractions rationnelles $f \in \mathbb{C}(t)$ invariantes par les changements de variables

$$t \mapsto 1 - t \text{ et } t \mapsto t^{-1}\ .$$

Montrer que $K = \mathbb{C}\left(\frac{(t^2-t+1)^3}{t^2(t-1)^2}\right)$.
En déduire que l'extension :

$$\mathbb{C}\left(\frac{(t^2 - t + 1)^3}{t^2(t - 1)^2}\right) \subset \mathbb{C}(t)$$

est galoisienne de groupe de Galois S_3.

Exercice : on pose $y_1 := x_1 + jx_2 + j^2x_3$, $y_2 := x_1 + j^2x_2 + jx_3$. Montrer que $\mathbb{C}(x_1, x_2, x_3)^{A_3} = \mathbb{C}(y_1^2/y_2, y_2^2/y_1, \sigma_1)$.

Proposition 3.2 *On pose $L := k(s_1, ..., s_n)$ et $L_i := L(x_{i+1}, ..., x_n)$, $0 \leq i \leq n$ ($L_n = L$).*

a) $[L_{i-1} : L_i] = i$ et $1, ..., x_i^{i-1}$ est une base de L_{i-1}/L_i.

b) $\{x_1^{a_1}...x_n^{a_n}\ :\ \forall\, i,\ a_i \leq i - 1\}$ est une base de $k(x_1, ..., x_n)/L$.

c) tout $g \in k[x_1, ..., x_n]$ est une combinaison $k[s_1, ..., s_n]-$linéaire de monômes $x_1^{a_1}...x_n^{a_n}\ :\ \forall\, i,\ a_i \leq i - 1$.

d) On retrouve que $k[x_1, ..., x_n]^{\mathfrak{S}_n} = k[s_1, ..., s_n]$.

3.2 Surjectivité

Théorème 3.3 *Soit E/F une extension galoisienne de groupe de Galois G. Si $F \leq B \leq E$, alors il existe $H \leq G$ tel que $E^H = B$.*

Démonstration : Soit $H := \mathrm{Aut}_B(E)$. On a : $B \leq E^H$. Soit $s_1, ..., s_r$ un système de représentants de G/H. On a $B^{\{s_1,...,s_r\}} = F$ donc $[B : F] \geq r$ et $[E : B] \leq [E : F]/r = |H| = [E : E^H]$ d'où $B = E^H$. **Q.e.d.**

Exercice : donner la liste des sous-corps de $\mathbb{Q}(\sqrt[3]{2}, j)$.
(*réponse :* $\mathbb{Q}(\sqrt[3]{2}, j) \geq \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(j\sqrt[3]{2}), \mathbb{Q}(j^2\sqrt[3]{2}), \mathbb{Q}(j) \geq \mathbb{Q}$).

Cours du mercredi 5 février 2014

3.3 Théorème fondamental

Théorème 3.4 *Soit E/F une extension galoisienne de groupe G.*

i) On a 2 bijections réciproques :

$$\{H \leq G\} \overset{1:1}{\longleftrightarrow} \{F \leq B \leq E\}$$
$$H \mapsto E^H$$
$$\mathrm{Gal}(E/B) \leftarrow B \ .$$

ii) L'extension E/B est galoisienne et $[E : B] = |\mathrm{Gal}(E/B)|$;

iii) $[B : F] = |G/\mathrm{Gal}(E/B)|$;

iv) l'extension B/F est galoisienne si et seulement si $\mathrm{Gal}(E/B) \triangleleft G$. Dans ce cas, $\mathrm{Gal}(B/F) \simeq G/\mathrm{Gal}(E/B)$.

Démonstration : Si $\mathrm{Gal}(E/B) \triangleleft G$, si $\sigma \in G$, alors $\sigma(B) = B$: en effet, $\mathrm{Gal}(E/\sigma(B)) = \sigma\mathrm{Gal}(E/B)\sigma^{-1} = \mathrm{Gal}(E/B) \Rightarrow \sigma(B) = B$. Notons G' l'image du morphisme $\sigma \mapsto \sigma|_B$. On a : $B^{G'} = F$. Réciproquement si B/F est galoisienne, alors pour tout $\sigma \in G$, $\sigma|_B \in \mathrm{Gal}(B/F)$ (*cf.* le corollaire 3.1.1). On a alors $\mathrm{Gal}(E/B) = \ker(G \to \mathrm{Gal}(B/F), \sigma \mapsto \sigma|_B)$ qui est un noyau donc distingué. **Q.e.d.**

Proposition 3.5 *Soit E/K une extension galoisienne. On suppose que $K \leq B \leq B' \leq E$. On note $U := \mathrm{Gal}(E/B)$, $U' := \mathrm{Gal}E/B'$. Alors B'/B est galoisienne $\Leftrightarrow U' \triangleleft U$. Et dans ce cas, $\mathrm{Gal}(B'/B) \simeq U/U'$.*

3.4 Caractérisation des extensions galoisiennes

Théorème 3.6 *Soit E/K une extension finie. On a toujours : $|\mathrm{Aut}(E/K)| \leq [E : K]$. L'extension E/K est galoisienne $\Leftrightarrow |\mathrm{Aut}(E/K)| = [E : K]$. Dans ce cas, $\mathrm{Gal}(E/K) = \mathrm{Aut}(E/K)$.*

Exemple : si $E = \mathbb{Q}(\sqrt[4]{2})$, alors $|\mathrm{Aut}(E/\mathbb{Q})| = 2 < 4 = [E : \mathbb{Q}]$.

3.5 Séparabilité

Soit $P \in K[X]$. Alors : P est premier avec P' si et seulement s'il n'existe pas d'extension où P a une racine multiple (*i.e.* d'ordre > 1). Dans ce cas, on dit que P est un *polynôme séparable*

Définition 4 (séparable) *Si E/K est une extension. On dit que $\alpha \in E$ est algébrique séparable si $P(\alpha) = 0$ pour un polynôme séparable $P \in K[X]$ $\Leftrightarrow$ le polynôme minimal de α est séparable.*

Une extension est *séparable* si tous ses éléments le sont.

Proposition 3.7 *Si $P \in K[X]$ est irréductible, alors P est séparable si $P' \neq 0$. En particulier, en caractéristique nulle ou sur un corps fini, tout polynôme irréductible est séparable.*

Contre-exemple : $X^p - t$ est irréductible non séparable sur $\mathbb{F}_p(t)$.

Théorème 3.8 *Soit E/F une extension galoisienne de groupe G. Soit $x \in E$. Soient $x_1, ..., x_r$, $r \leq n$ les images distinctes de x par les $\sigma \in G$. Le polynôme $(X - x_1)....(X - x_r)$ est le polynôme minimal de x sur F. En particulier, E/F est séparable.*

Théorème 3.9 *Une extension finie E/K est galoisienne $\Leftrightarrow$ E est le corps de décomposition sur K d'un polynôme $P \in K[X]$ séparable. Dans ce cas, on dit que $\mathrm{Gal}(E/K)$ est le groupe de Galois de P sur K, noté $\mathrm{Gal}_K(P)$. De plus $\mathrm{Gal}_K(P)$ s'identifie à un sous-groupe de $\mathfrak{S}_r$ où $r = \deg P$.*

3.6 Normalité

On dit qu'une extension E/F est *normale* si pour toute extension Ω de F, et pour tous $F-$morphismes $\sigma, \tau : E \to \Omega$, $\sigma(E) = \tau(E)$.

Exercice : Cela revient à dire que $\sigma(E) = E$ si ci-dessus $\Omega \geq E$.

Proposition 3.10 *Si E/F est un corps de décomposition, E/F est normale.*

Exemple : $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$, *contre-exemple :* $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

Théorème 3.11 *Soit E/F une extension finie. Alors l'extension E/F est galoisienne si et seulement si elle est normale et séparable.*

Cours du mercredi 12 février 2014

Exercice : vérifier que $\mathrm{Gal}_K(P)$ agit transitivement sur les racines si et seulement si P est irréductible sur K.

Remarques :

i) Si M/L et L/K sont normales, M/K ne l'est pas forcément. Par exemple : $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, $M = \mathbb{Q}(\sqrt[4]{2})$.

ii) Si M/L et L/K sont séparables, alors M/K est aussi séparable.

3.7 Composée de corps

section non faite en cours

Soit L/K une extension. Soient $K \leq E, E' \leq L$. On note EE' le sous-corps de L engendré par E et E'.

Proposition 3.12 *Soient L/K une extension galoisienne de groupe G, $K \leq E, E' \leq L$, $H := \mathrm{Gal}(L/E)$, $H' := \mathrm{Gal}(L/E')$. On a :*

i) $\mathrm{Gal}(L/EE') = H \cap H'$, $\mathrm{Gal}(L/E \cap E') = \langle H, H' \rangle$.

ii) *Si E'/K est galoisienne, alors EE'/E aussi et* $\mathrm{Gal}(EE'/E) \simeq \mathrm{Gal}(E/E \cap E')$, $s \mapsto s|_E$.

iii) *Si E/K et E'/K sont galoisiennes, alors EE'/K aussi et* $\mathrm{Gal}(EE'/K)$ *est isomorphe à un sous-groupe de* $\mathrm{Gal}(E/K) \times \mathrm{Gal}(E'/K)$ *via* $s \mapsto (s|_E, s|_{E'})$. *Si de plus,* $E \cap E' = K$, $\mathrm{Gal}(EE'/K) \simeq \mathrm{Gal}(E/K) \times \mathrm{Gal}(E'/K)$.

Exercice : Soient $L := k(X_1, X_2, X_3, X_4)$, $K := L^{\mathfrak{S}_4} = k(s_1, s_2, s_3, s_4)$, $E := k(x_4) = L^{\mathfrak{S}_3}$, $E' := L^{K_4}$ où $K_4 = \{1, (12)(34), (13)(24), (14)(23)\}$.

On a $H = \mathfrak{S}_3$, $H' = K_4$, $[E : K] = |\mathfrak{S}_4/\mathfrak{S}_3| = 4$, $[E' : K] = |\mathfrak{S}_4/K_4| = 6$, $EE' = L = L^{H \cap H'}$, $E \cap E' = L^{\langle H, H' \rangle} = K$. Comme H n'est pas distingué dans $\mathfrak{S}_4$, E/K n'est pas galoisienne. En revanche E'/K est galoisienne de groupe de Galois $\simeq \mathfrak{S}_4/K_4 \simeq \mathfrak{S}_3$. Vérifier que $E' = K(\beta)$ où $\beta = \sum_{\sigma \in K_4} \sigma\alpha$ où $\alpha := x_1 x_2^2 x_3^3 x_4^4$.

4 Corps finis

4.1 Sous-groupes finis de $K^\times$

Soit G un groupe fini. On note $\omega(G)$ l'*exposant de G* : c'est le ppcm des ordres des éléments de G.

Exemple : $\omega(\mathfrak{S}_3) = 6$

Lemme 4.1 *Soient $a, b \in G$ tels que $ab = ba$. Si a, b sont d'ordres finis m, n premiers antre eux, alors ab est d'ordre mn.*

Corollaire 4.1.1 *Dans un groupe abélien fini, l'ensemble des ordres des éléments est stable par ppcm.*

Proposition 4.2 *Soit G un sous-groupe fini de $K^\times$, alors G est cyclique.*

Exemple : les $\mathbb{F}_q^\times$ sont cycliques ; les sous-groupes finis de $\mathbb{C}^\times$ sont cycliques : ce sont les $\boldsymbol{\mu_n}$.

Contre-exemple : $\mathbb{Q}_8 := \{\pm 1, \pm i, \pm j, \pm k\} \leq \mathbb{H}^\times$ n'est pas cyclique.

Exercice : déterminer les sous-groupes *d'indice fini* de $\mathbb{C}^\times$, de $\mathbb{R}^\times$.