Inledning till Galoisteori

En enkel beskrivning av Galoisteorin är att den handlar om automorfismer av kroppar. En automorfism av ett algebraiskt objekt, t ex en grupp eller en kropp, är en bijektiv avildning av objektet på sig själv som respekterar den algebraiska strukturen. Om K/k är en kroppsutvidgning, så kan kunskap om de automorfismer av K som fixerar k elementvis ge information om strukturen av utvidgningen själv.

1. Homomorfismer och inbäddningar. En *kropphomomorfism* är en avbildning $\sigma\colon K \to F$ mellan två kroppar sådan att

$$\sigma(x+y) = \sigma(x) + \sigma(y) \quad \text{och} \quad \sigma(xy) = \sigma(x)\sigma(y)$$

för alla $x, y \in K$. Det finns alltid minst en homomorfism $K \to F$, nämligen nollavbildningen. Om $\sigma(1) = 0$, så måste σ vara nollavbildningen, ty $\sigma(a) = \sigma(a \cdot 1) = \sigma(a)\sigma(1) = 0$. Antag att $\sigma \neq 0$. Av $\sigma(1)^2 = \sigma(1)$ följer att $\sigma(1) = 1$, ty $\sigma(1) \neq 0$. Härav följer att $\sigma(x^{-1}) = \sigma(x)^{-1}$ om $x \neq 0$.

Sats 1 *En kropphomomorfism som inte är 0 är injektiv.*

Bevis. Antag att $\sigma\colon K \to F$ inte är nollavbildningen och att $x \neq y$. Då finns $(x-y)^{-1}$ och $\sigma((x-y)^{-1}) = (\sigma(x-y))^{-1} = (\sigma(x) - \sigma(y))^{-1}$. Alltså måste $\sigma(x) \neq \sigma(y)$.

En injektiv homomorfism kallas en *inbäddning* (embedding på engelska), notera nämligen att om $\sigma\colon K \to F$ är injektiv, så innehåller F en kopia av K. Härav följer att om K och F har olika karaktäristik, så är nollavbildningen den enda homomorfismen $K \to F$. I fortsättningen antar vi att alla homomorfismer är skilda från 0 och att alla kroppar är delkroppar till $\mathbf{C}$. Låt K/k vara en utvidgning. En inbäddning $\sigma\colon K \to \mathbf{C}$ säges vara *över* k om den fixerar alla element i k, dvs om $\sigma(a) = a$ för alla $a \in k$. Alla delkroppar till $\mathbf{C}$ innehåller $\mathbf{Q}$ och alla inbäddningar är över de rationella talen. Ty om p är ett positivt heltal så har vi $\sigma(p) = \sigma(1+1+\ldots+1) = p \cdot \sigma(1) = p$. Om $p, q > 0$ så följer härav att $\sigma(p/q) = \sigma(pq^{-1}) = \sigma(p)\sigma(q)^{-1} = p/q$. Vi har $\sigma(-1)^2 = \sigma((-1)^2) = \sigma(1) = 1$, så $\sigma(-1) = -1$ eftersom σ är injektiv. Alltså är $\sigma(-r) = -\sigma(r) = -r$ om r är ett positivt rationellt tal.

När $\sigma\colon K \to F$ är en kropphomomorfism, så får vi en ringhomomorfism $\sigma\colon K[x] \to F[x]$ (vi använder samma beteckning) genom

$$\sigma(a_0 + a_1x + \ldots + a_nx^n) = \sigma(a_0) + \sigma(a_1)x + \ldots + \sigma(a_n)x^n.$$

2. Utvidgningar av homomorfismer. Låt K/k vara en utvidgning och σ en inbäddning av k (i $\mathbf{C}$). En *utvidgning* av σ till K är en inbäddning τ av K sådan att restriktionen $\tau|_k = \sigma$. Vi skall diskutera om och på hur många sätt σ kan utvidgas till K. Vi antar först att $K = k(\alpha)$, där α är algebraiskt över k med minimalpolynom $f(x) = a_0 + a_1x + \ldots + a_nx^n \in k[x]$. Låt alltså σ vara en

inbäddning av k och sätt $k' = \sigma(k)$; då är σ en isomorfism av k och k'. Antag att σ kan utvidgas till $k(\alpha)$. Vad kan då $\sigma(\alpha)$ vara? Vi har ju

$$a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$$

så att

$$0 = \sigma(a_0 + a_1\alpha + \ldots + a_n\alpha^n) = \sigma(a_0) + \sigma(a_1)\sigma(\alpha) + \ldots + \sigma(a_n)\sigma(\alpha)^n$$

dvs $(\sigma f)(\sigma(\alpha)) = 0$. Alltså måste $\sigma(\alpha)$ vara en av rötterna till polynomet $\sigma f \in k'[x]$. Ett viktigt specialfall är då σ är identitetsavbildningen på k; då måste $\sigma\alpha$ vara en av de andra rötterna till minimalpolynomet f. Rötterna till f brukar f ö kallas de *algebraiska konjugaten* till α (över k).

Låt α' vara en rot till σf. Intuitivt är det väl ganska klart att man kan utvidga σ till en isomorfism $k(\alpha) \to k'(\alpha')$ genom $\sigma(\alpha) = \alpha'$ eftersom α och α' uppfyller samma ekvation, så när som på beteckningen på koefficienterna, så utvidgningen måste vara väldefinierad. Antalet utvidgningar till $k(\alpha)$ borde alltså vara lika med deg $f = [k(\alpha) : k]$. Beviset för detta är något abstrakt, men inte svårt (hoppa över det om du tror på resultatet!).

Lemma 1 *Låt α vara algebraiskt över k med minimalpolynom $f(x) \in k[x]$. Då är $k[x]/(f(x)) \cong k(\alpha)$ och en isomorfism ges av $g(x) + (f(x)) \mapsto g(\alpha)$.*

Bevis. Definiera $\phi\colon k[x] \to k(\alpha)$ genom $\phi(g(x)) = g(\alpha)$. Man kontrollerar lätt att kärnan är precis idealet som genereras av $f(x)$ och då $k(\alpha)$ består av polynom i α, så följer påståendet ur homomorfismsatsen.

Lemma 2 *Med beteckningar som ovan, låt $\sigma\colon k \to k'$ vara en isomorfism. Låt α' vara en rot till σf. Då kan σ utvidgas till en isomorfism $k(\alpha) \to k'(\alpha')$ sådan att $\sigma\alpha = \alpha'$.*

Bevis. Definiera $\phi\colon k[x] \to k'(\alpha')$ genom $\phi(g(x)) = (\sigma g)(\alpha')$. Man kontrollerar lätt att kärnan är idealet $(f(x))$, så att

$$k(\alpha) \cong k[x]/(f(x)) \cong k'(\alpha').$$

Sammansättningen avbildar α på α'.

Sats 2 *Låt K/k vara en utvidgning av grad n. Då finns precis n inbäddningar av K i $\mathbf{C}$ över k.*

Bevis. Satsen är sann då $K = k(\alpha)$ enligt Lemma 2 (tag σ lika med identiteten på k) eftersom minimalpolynomet bara har enkla rötter (dvs de är alla olika). I det allmänna fallet tar vi ett $\alpha \in K$ och betraktar kedjan $k \subset k(\alpha) \subset K$. Identiteten på k kan utvidgas på $[k(\alpha) : k]$ sätt till $k(\alpha)$. Med induktion över utvidgningens grad ser vi att en inbäddning av $k(\alpha)$ i sin tur kan utvidgas på $[K : k(\alpha)]$ sätt till K. Totalt finns det alltså

$$[K : k(\alpha)][k(\alpha) : k] = n$$

inbäddningar av K över k.

Anmärkning: Lägg märke till att vi på ett väsentligt sätt använde att karaktäristiken är 0, nämligen för att dra slutsatsen att minimalpolynomets rötter är enkla. Detta är inte sant i allmänhet i karaktäristik $p > 0$, vilket gör teorin lite trassligare där, även om det mesta kan räddas.

Exempel: Låt $k = \mathbf{Q}, K = \mathbf{Q}(\sqrt{2})$. En inbäddning σ av K måste avbilda $\sqrt{2}$ på någon av rötterna till $x^2 - 2$, dvs på $\pm\sqrt{2}$. Inbäddningarna ges alltså av

$$a + b\sqrt{2} \mapsto a + b\sqrt{2} \quad \text{resp.} \quad a + b\sqrt{2} \mapsto a - b\sqrt{2}.$$

Lägg märke till att båda avbildar K på sig själv, m a o att de är *automorfismer* av K.

Exempel: Låt nu k vara som ovan, men tag $K = \mathbf{Q}(\alpha)$, där $\alpha = \sqrt[3]{2}$. Minimalpolynomet är $x^3 - 2$ med rötterna $\alpha, \omega\alpha, \omega^2\alpha$, där $\omega = -1/2 + i\sqrt{3}/2$ är en primitiv 3:e enhetsrot. Inbäddningarna i det här fallet ges således av

$$\alpha \mapsto \alpha, \ \alpha \mapsto \omega\alpha \text{ samt } \alpha \mapsto \omega^2\alpha.$$

Här är det bara identiteten som är en automorfism av K.

Exempel: Låt k vara som förut och $K = \mathbf{Q}(\beta)$, där $\beta = \sqrt{2} + \sqrt{3}$. Vi har $\beta^3 = 11\sqrt{2} + 9\sqrt{3}$, så $\sqrt{2} = (\beta^3 - 9\beta)/2 \in K$ och det följer också att K innehåller $\sqrt{3}$. Men då måste $K = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. Elementen i K är alltså linjärkombinationer av $1, \sqrt{2}, \sqrt{3}$ och $\sqrt{2} \cdot \sqrt{3} = \sqrt{6}$ med rationella koefficienter. Läsaren kan själv verifiera att inbäddningarna av K ges av

$$\begin{aligned}
a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} &\mapsto a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \\
a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} &\mapsto a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} \\
a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} &\mapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \\
a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} &\mapsto a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}.
\end{aligned}$$

Även i det här fallet är inbäddningarna automorfismer av K.

Definition: En utvidgning K/k sådan att alla inbäddningar av K över k är automorfismer av K kallas en *Galoisutvidgning*.

Exempel på Galoisutvidgningar är tydligen $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ och $\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q}$, medan $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ inte är Galois. Mängden av automorfismer av K över k är alltid en grupp, men den är intressant bara då K/k är Galois. I det fallet kallas den för *Galoisgruppen* för K/k och betecknas $G(K/k)$ (ofta även $\mathrm{Gal}(K/k)$). Enligt Sats 2 har den ordning $n = [K : k]$. Galoisgruppen $G(\mathbf{Q}(\sqrt{2})/\mathbf{Q})$ är gruppen med 2 element. Gruppen $G(\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q})$ har ordning 4. Det finns två grupper med 4 element, dels den cykliska och dels Kleins fyrgrupp i vilken alla element utom identiteten har ordning 2. Det är lätt att kontrollera att $G(\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q})$ är den senare.

En *kvadratisk talkropp* är en kropp av formen $\mathbf{Q}(\sqrt{d})$, där d är ett kvadratfritt heltal (positivt eller negativt). Som i fallet $d = 2$ ser man lätt att sådana är

Galois över $\mathbf{Q}$ och Galoisgruppen genereras av "konjugering" $\sqrt{d} \mapsto -\sqrt{d}$. Låt $\zeta_n = e^{2\pi i/n}$ vara en primitiv $n$te enhetsrot. En talkropp av formen $K_n = \mathbf{Q}(\zeta_n)$ kallas en *cyklotomisk* talkropp (cyklotomisk är grekiska och betyder ungefär cirkeldelning). Det är klart att K_n innehåller *alla* $n$te enhetsrötter. Men om σ är en inbäddning av K_n, så är $\sigma(\zeta_n)^n = 1$, varför $\sigma(\zeta_n) \in K_n$. Det följer att $K_n/\mathbf{Q}$ är Galois. I boken visas att

$$[\mathbf{Q}(\zeta_n) : \mathbf{Q}] = \varphi(n)$$

och att

$$G(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \cong U(\mathbf{Z}/n\mathbf{Z}).$$

Man kan ganska enkelt visa att K/k är Galois om och endast om K är sönderfallskropp över k till något polynom i $k[x]$. Vidare gäller att det alltid finns en ändlig utvidgning E av K sådan att E/k är Galois. Inuti E finns alla inbäddningar av K och $G(E/k)$ permuterar dessa. Den minsta Galoisutvidgningen av $\mathbf{Q}(\sqrt[3]{2})$ är $E = \mathbf{Q}(\sqrt[3]{2}, \omega)$ med ω som ovan. Det är en intressant övning att bevisa att $G(E/\mathbf{Q})$ är isomorf med S_3, den symmetriska gruppen av grad 3.

Galoisteori handlar om sambandet mellan strukturen hos utvidgningen K/k och Galoisgruppen $G(K/k)$. Exempelvis finns ett samband mellan delutvidgningar $k \subset F \subset K$ på följande sätt: Låt H vara en undergrupp till $G(K/k)$ och sätt $K^H = \{a \in K; \sigma(a) = a \text{ för alla } \sigma \in H\}$ (den s k fixkroppen till H). Man kontrollerar lätt att K^H är en kropp och att $k \subset K^H$. Då är avbildningen $H \mapsto K^H$ en bijektion mellan undergrupperna till Galoisgruppen och mängden av kroppar som ligger mellan k och K. Ett specialfall är att fixkroppen till hela gruppen $G(K/k)$ är grundkroppen k. Detta följer av Lemma 2.

Om $k \subset F \subset K$, så är K/F alltid Galois om K/k är det, men F/k behöver inte vara Galois. Galoisgruppen $G(K/F)$ är den undergrupp till $G(K/k)$ som fixerar alla element i F och Galoisteorins huvudsats säger att F/k är en Galoisutvidgning om och endast om $G(K/F)$ är en normal undergrupp till $G(K/F)$. I så fall gäller att

$$G(F/k) \cong G(K/k)/G(K/F).$$

Galoisteori är uppenbarligen av de vackraste algebraiska teorierna. Grunderna lades av Evariste Galois (1811-1832) i samband med undersökningar av algebraiska ekvationers lösbarhet medelst rotutdragningar.

Man kan bevisa att varje ändlig grupp är Galoisgrupp till någon utvidgning K/k, men det är ett olöst problem huruvida varje grupp är en Galoisgrupp till någon utvidgning av $\mathbf{Q}$. Detta är i själva verket ett av algebrans mest berömda olösta problem. Exempel på grupper som man vet är Galoisgrupper för utvidgningar av $\mathbf{Q}$ är alla abelska grupper och alla symmetriska grupper. Ifråga om abelska grupper så gäller följande vackra resultat, som brukar kallas Kroneckers Jugendtraum (ungdomsdröm): Om K är en Galoisutvidgning av $\mathbf{Q}$ sådan att $G(K/\mathbf{Q})$ är abelsk, så finns ett n sådant att $K \subset \mathbf{Q}(\zeta_n)$. Den här vackra satsen bevisades av Kronecker och Weber. Beviset är inte enkelt.

3. Norm och spår. Låt K/k vara en ändlig utvidgning som inte nödvändigtvis är Galois och $\alpha_1, \ldots, \alpha_n$ en bas. När $\alpha \in K$ så finns $a_{ij} \in k$ sådana att

$$\begin{aligned}
\alpha\alpha_1 &= a_{11}\alpha_1 + a_{21}\alpha_2 + \ldots + a_{n1}\alpha_n \\
\alpha\alpha_2 &= a_{12}\alpha_1 + a_{22}\alpha_2 + \ldots + a_{n2}\alpha_n \\
&\ldots \\
\alpha\alpha_n &= a_{1n}\alpha_1 + a_{2n}\alpha_2 + \ldots + a_{nn}\alpha_n.
\end{aligned}$$

Spåret av α relativt utvidgningen K/k definieras som

$$\mathrm{tr}_{K/k}\ (\alpha) = \sum_{i=1}^{n} a_{ii}$$

och *normen* som

$$N_{K/k}(\alpha) = \det(a_{ij})_{1 \le i,j \le n}.$$

Det är lätt att visa att $\mathrm{tr}\ (AB) = \mathrm{tr}\ (BA)$, varav följer att $\mathrm{tr}\ (C^{-1}AC) = \mathrm{tr}\ (A)$, vilket innebär att spåret inte beror på den valda basen. Detsamma gäller förstås för normen, eftersom $\det(AB) = \det(A)\det(B)$.

Låt L_α vara den k-linjära avbildningen $\beta \mapsto \alpha\beta$ på K. Det karaktäristiska polynomet är

$$\det(t \cdot 1_K - L_\alpha) = \det \begin{pmatrix} t - a_{11} & -a_{12} & \ldots & -a_{1n} \\ -a_{21} & t - a_{22} & \ldots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \ldots & t - a_{nn} \end{pmatrix}$$

(1_K är identitetsavbildningen på K) och en direkt räkning ger att

$$\det(t \cdot 1_K - L_\alpha) = t^n - \mathrm{tr}_{K/k}\ (\alpha)t^{n-1} + \ldots + (-1)^n N_{K/k}(\alpha).$$

Om F/K är en annan ändlig utvidgning, så kan man visa att

$$\mathrm{tr}_{F/k} = \mathrm{tr}_{K/k} \circ \mathrm{tr}_{F/K} \quad \text{och} \quad N_{F/k} = N_{K/k} \circ N_{F/K},$$

så spåret och normen beror på vilken utvidgning man arbetar i. Vi kommer inte att behöva detta i allmänhet, utan bara i ett specialfall. Låt $f(x) = a_0 + \ldots + a_m x^m \in k[x]$ vara minimalpolynomet till α. Vi skall beräkna normen och spåret från $k(\alpha)$ till k. En bas för $k(\alpha)$ är $1, \alpha, \ldots, \alpha^{m-1}$ och vi har

$$\begin{aligned}
\alpha \cdot 1 &= \alpha \\
\alpha \cdot \alpha &= \alpha^2 \\
&\ldots \\
\alpha \cdot \alpha^{m-2} &= \alpha^{m-1} \\
\alpha \cdot \alpha^{m-1} &= \alpha^m = -a_0 - a_1\alpha - \ldots - a_{m-1}\alpha^{m-1},
\end{aligned}$$

så i den här basen är

$$L_\alpha = \begin{pmatrix} 0 & 0 & \dots & -a_0 \\ 1 & 0 & \dots & -a_1 \\ 0 & 1 & \dots & -a_2 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & -a_{n-1} \end{pmatrix}.$$

Det är nu en trevlig övning i determinanträkning att visa att

$$\det(t \cdot 1_{k(\alpha)} - L_\alpha) = f(t).$$

Härav följer sedan att

$$\mathrm{tr}_{k(\alpha)/k}\,(\alpha) = -a_{m-1} \quad \text{och} \quad N_{k(\alpha)/k}(\alpha) = (-1)^m a_0.$$

Om samtliga rötter till minimalpolynomet är $\alpha = \alpha_1, \dots, \alpha_m$, så är

$$f(x) = \prod_{i=1}^{m} (x - \alpha_i)$$

och det följer att

$$\mathrm{tr}_{k(\alpha)/k}\,(\alpha) = -\sum_{i=1}^{m} \alpha_i, \;\; N_{k(\alpha)/k}(\alpha) = \prod_{i=1}^{m} \alpha_i.$$

Låt $\beta_1, \dots, \beta_l$ vara en bas för K över $k(\alpha)$. Informellt kan vi skriva $K = \sum_{j=1}^{l} k(\alpha)\beta_j$ och delrummen $\beta_j k(\alpha)$ är slutna under multiplikation med α. Det är klart att det karaktäristiska polynomet på alla dessa delrum är lika med $f(t)$, så det karaktäristiska polynomet för L_α på K är lika med $f(t)^l$. Alltså är

$$\mathrm{tr}_{K/k}(\alpha) = -l a_{m-1} \quad \text{och} \quad N_{K/k}(\alpha) = (-1)^{ml} a_0^l = (-1)^n a_0^l.$$

Till sist skall vi uttrycka normen och spåret med hjälp av inbäddningar. Låt Ω vara mängden av inbäddningar av K över k (K/k behöver således inte vara Galois). Låt $\alpha \in K$ ha minimalpolynomet $f(x)$ över k och låt $\alpha = \alpha_1, \dots, \alpha_m$ vara dess rötter (konjugaten till α). När $\sigma \in \Omega$, så är $\sigma(\alpha) = \alpha_i$ för något i. Enligt vad vi har sett tidigare, så finns för varje i en inbäddning τ av $k(\alpha)$ sådan att $\tau(\alpha) = \alpha_i$ och τ har precis $l = n/m$ utvidgningar till K. Alltså gäller $\sigma(\alpha) = \alpha_i$ för precis l stycken $\sigma \in \Omega$. Härav och av vad vi sade ovan om spåret och normen från $k(\alpha)$, så följer

$$\mathrm{tr}_{K/k}\,(\alpha) = \sum_{\sigma \in \Omega} \sigma(\alpha), \;\; N_{K/k}(\alpha) = \prod_{\sigma \in \Omega} \sigma(\alpha).$$