EXAMPLE SHEET 4 (LECTURES 19–23)
GALOIS THEORY MICHAELMAS 2009

Soluble groups / Radical extensions

1. (i) Let G be a finite group, and N its normal subgroup. Show that G is soluble if and only if N and G/N are soluble.

(ii) For a group G, the derived subgroup G^{der} is the subgroup generated by all the elements of the form $xyx^{-1}y^{-1}$ for $x, y \in G$. Show that G^{der} is normal, and that G/G^{der} is abelian (it is the **maximal abelian quotient** of G, i.e. every group homomorphism from G to an abelian group factors through G/G^{der}).

(iii) Let $G_0 = G,\ G_i = (G_{i-1})^{\mathrm{der}}$ for $i \in \mathbb{N}$. Show that G is soluble if and only if there is an i such that $G_i = 1$.

(iv) Let G be the group of invertible $n \times n$ upper triangular matrices with entries in a finite field K. Show that G is soluble.

2. Show that if $E/K, F/K$ are two soluble extensions, their composite field EF/K is also soluble.

3. Write $\cos(2\pi/17)$ explicitly in terms of radicals.

Discriminants, cubics and quartics

4. (i) Show that the discriminant of $X^4 + pX + q$ is $-27p^4 + 256q^3$. [Hint: It is a symmetric polynomial of degree 12, hence a linear combination of p^4 and q^3. By making good choices for p, q, determine the coefficients.]

(ii) Show that the discriminant of $X^5 + pX + q$ is $4^4p^5 + 5^5q^4$. (The discriminant of a general quintic will have 59 terms...)

5. (i) **(Vandermonde determinant)** Show that if $X_1, \ldots, X_n$ are indeterminates, then

$$\begin{vmatrix} X_1^{n-1} & X_2^{n-1} & \cdots & X_n^{n-1} \\ X_1^{n-2} & X_2^{n-2} & \cdots & X_n^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ X_1 & X_2 & \cdots & X_n \\ 1 & 1 & \cdots & 1 \end{vmatrix} = \prod_{1 \le i < j \le n} (X_i - X_j).$$

(First show that each $(X_i - X_j)$ is a factor of the determinant.)

(ii) For $P(X) = \prod_{i=1}^n (X - x_i)$, show that $P'(x_i) = \prod_{j \neq i} (x_i - x_j)$, and deduce that its discriminant is given by $\Delta_P = (-1)^{n(n-1)/2} \prod_{i=1}^n P'(x_i)$.

Date: January 27, 2010.

(iii) Now suppose $P(X) = X^n + pX + q = \prod_{i=1}^n (X - x_i)$, with $n \geq 2$. Show that

$$x_i P'(x_i) = (n-1)p\Big(\frac{-nq}{(n-1)p} - x_i\Big)$$

and deduce that

$$\Delta_P = (-1)^{n(n-1)/2}\left((1-n)^{n-1}p^n + n^n q^{n-1}\right).$$

6. Compute the discriminant of $X^{p^n} - 1$.

7. Let P be an irreducible cubic polynomial over K with $\operatorname{char} K \neq 2$, and let δ be a square root of the discriminant of P. Show that P remains irreducible over $K(\delta)$.

8. Let P be an irreducible quartic polynomial over K with $\operatorname{char} K \neq 2$, whose Galois group is A_4. Show that its splitting field can be written in the form $L(\sqrt{a}, \sqrt{b})$ where L/K is a Galois cubic extension and $a, b \in L$.

9. Let P be an irreducible separable quartic, and Q its resolvant cubic. Show that the discriminants of P and Q are equal.

10. Let $P(X) = X^4 + 8X + 12 \in \mathbb{Q}[X]$. Compute the discriminant and resolvant cubic Q of P. Show P and Q are both irreducible, and that the Galois group of P is A_4.

Galois groups over $\mathbb{Q}$

11. (i) Determine the Galois groups of the following cubics in $\mathbb{Q}[X]$:

$$X^3 + 3X,\ X^3 + 27X - 4,\ X^3 - 21X + 7,\ X^3 + X^2 - 2X - 1,\ X^3 + X^2 - 2X + 1.$$

(ii) Determine the Galois groups of the following quartics in $\mathbb{Q}[X]$:

$$X^4 + 4X^2 + 2,\ X^4 + 2X^2 + 4,\ X^4 + 4X^2 - 5,\ X^4 - 2,\ X^4 + 2,$$
$$X^4 + X + 1,\ X^4 + X^3 + X^2 + X + 1.$$

12. (i) Show that the Galois group of $X^5 - 4X + 2$ over $\mathbb{Q}$ is S_5, and determine its Galois group over $\mathbb{Q}(i)$.

(ii) Find the Galois group of $X^4 - 4X + 2$ over $\mathbb{Q}$ and over $\mathbb{Q}(i)$.

13. Determine whether the following nested radicals can be written in terms of unnested ones, and if so, find an expression: $\sqrt{2+\sqrt{11}},\ \sqrt{6+\sqrt{11}},\ \sqrt{11+6\sqrt{2}},\ \sqrt{11+\sqrt{6}}$.

14. Show that $\mathbb{Q}(\boldsymbol{\mu}_{21})$ has exactly three subfields of degree 6 over $\mathbb{Q}$. Show that one of them is $\mathbb{Q}(\boldsymbol{\mu}_7)$, one is real, and the other is a cyclic extension $K/\mathbb{Q}(\boldsymbol{\mu}_3)$. Use a suitable Lagrange resolvent to find $a \in \mathbb{Q}(\boldsymbol{\mu}_3)$ such that $K = \mathbb{Q}(\zeta_3, \sqrt[3]{a})$.

15. Let $\alpha = \sqrt[3]{a + b\sqrt{2}}$ for $a, b \in \mathbb{Q}$, and let F be the splitting field for the minimal polynomial of α over $\mathbb{Q}(\boldsymbol{\mu}_3)$. Determine the possible groups for $\operatorname{Gal}(F/\mathbb{Q}(\boldsymbol{\mu}_3))$.

Trace & norm

16. We saw that we can prove the fundamental theorem of Galois theory without using the primitive element theorem. Now deduce the primitive element theorem from the fundamental theorem. (Use Example Sheet 2, Problem 3.)

17. Let F/K be a cyclic extension of prime degree p, and σ a generator of $\mathrm{Gal}(F/K)$.

(i) Show that $T_{F/K}(\sigma(x)-x)=0$ for all $x \in F$. Deduce that if $y \in F$ then $T_{F/K}(y)=0$ if and only if $y=\sigma(x)-x$ for some $x \in F$.

(ii) **(Artin-Schreier theory)** Suppose that K has characteristic p. Use (i) to show that every element of K can be written in the form $\sigma(x)-x$ for some $x \in F$. Show also that if $\sigma(x)-x \in \mathbb{F}_p$ then $x^p-x \in K$. Deduce that F/K is an extension of the type described in the Example Sheet 2, Problem 1.

[This is the analogue of Kummer theory in characteristic $p>0$. The natural analogue of radical extensions in characteristic p is to consider the tower of abelian extensions which involve Kummer and Artin-Schreier extensions.]

18. (**Normal Basis Theorem**) In this example we show that if F/K if a finite Galois extension of infinite fields, then there exists $y \in F$ such that $\{\sigma(y) \mid \sigma \in \mathrm{Gal}(F/K)\}$ is a basis for F/K. (Such a basis $\{\sigma(y)\}$ is said to be a **normal basis** for F/K.)

(i) Let $P \in K[X]$ be a monic separable polynomial of degree n, with roots x_i in a splitting field F. Let

$$Q_i(X)=\frac{P(X)}{P'(x_i)(X-x_i)} \in F[X] \qquad (1 \le i \le n).$$

Show that, in $F[X]$:

$$Q_1+\cdots+Q_n=1 \tag{1}$$

$$Q_iQ_j \equiv \begin{cases} 0 \pmod{(P)} & \text{if } j \neq i \\ Q_i \pmod{(P)} & \text{if } j=i \end{cases} \tag{2}$$

(Equation (1) is the "partial fractions" decomposition of $1/P(X)$.)

(ii) Let F/K be a finite Galois extension and $\mathrm{Gal}(F/K)=\{\sigma_1,\ldots,\sigma_n\}$ with $\sigma_1=\mathrm{id}$. Let $x \in F$ be such that $F=K(x)$ and its minimal polynomial over K is $P \in K[X]$, and $x_i=\sigma_i(x)$. Let $A=(a_{ij})$ be the matrix with entries $a_{ij}:=\sigma_i\sigma_jQ_1 \in F[X]$. Use (1),(2) of (i) to show that $A^tA \equiv I_n \pmod{(P)}$.

(iii) Assume that K is infinite. Use (ii) to show that there exists $b \in K$ such that $\det(\sigma_i\sigma_jQ_1(b)) \neq 0$. Deduce that $\{\sigma_1(y),\ldots,\sigma_n(y)\}$ for $y=Q_1(b)$ is a K-basis of F.

E-mail address: t.yoshida@dpmms.cam.ac.uk