Solutions of exercise sheet 9

1. Let G be a solvable group, and H a subgroup of G, not necessarily normal. Prove that H is solvable.

Solution: We first prove that whenever $K \trianglelefteq G$ is a normal subgroup such that G/K is abelian, then for any subgroup $H \leq G$ we get that $H \cap K \trianglelefteq H$ and $H/H \cap K$ is abelian.

Indeed, we are in position of applying Exercise 2 from Exercise sheet 4 of last semester's Algebra I course, as $hK = Kh$ for each $h \in H$ by normality of K in G. This exercise tells us immediately that $H \cap K \trianglelefteq H$. Moreover, $HK \leq G$ and

$$H/H \cap K \cong HK/K \leq G/K,$$

so that $H/H \cap K$ is abelian since it is embeddable in an abelian group.

Now take a normal sequence with abelian quotients

$$\{1\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = G.$$

Then, applying what we found above at each step, we easily see that

$$\{1\} = H_n \trianglelefteq H_{n-1} \trianglelefteq \cdots \trianglelefteq H_1 \trianglelefteq H_0 = H,$$

where $H_i := G_i \cap H$ is a normal sequence with abelian quotients for H. Hence H is solvable.

2. The aim of this exercise is to explain Cardan's formula for solutions of a degree-3 polynomial equation.

Let K be a field of characteristic 0 and $P \in K[X]$ be an irreducible degree 3 polynomial. Denote by L the splitting field of P, and assume that $\mathrm{Gal}(L/K) = S_3$. Up to a change of variable, we can assume that $P(X) = X^3 + pX + q$. Then one can find that the discriminant of P is $\Delta = -4p^3 - 27q^2$.

1. Show that Δ is not a square in K, and that $[L : K(\Delta)] = 3$.
2. Let μ_3 be the group of cubic roots of 1 in $\bar{K}$. Show that $L(\mu_3)/K(\sqrt{\Delta}, \mu_3)$ is a Galois extension of degree 3. Deduce that $\mathrm{Gal}(L(\mu_3)/K(\sqrt{\Delta}, \mu_3)) \cong \mathbb{Z}/3\mathbb{Z}$. [*Hint:* $[K(\sqrt{\Delta}, \mu_3) : K(\sqrt{\Delta})] \leq 2$.]
3. Let σ be a generator of $\mathrm{Gal}(L(\mu_3)/K(\sqrt{\Delta}, \mu_3)) \cong \mathbb{Z}/3\mathbb{Z}$, and x a root of P in L. Prove that the set of roots of P in L is $\{x, \sigma(x), \sigma^2(x)\}$.

Please turn over!

4. Let $\xi \in \bar{K}$ be a primitive cubic root of unity, and consider the Lagrange resolvents

$$\alpha := x + \xi\sigma(x) + \xi^2\sigma^2(x)$$
$$\beta := x + \xi^2\sigma(x) + \xi\sigma^2(x).$$

   Prove that $x, \sigma(x), \sigma^2(x)$ can be expressed in terms of α and β. [*Hint:* $x + \sigma(x) + \sigma^2(x) = 0$. Use linear systems.]

5. Explain why α^3 and β^3 belong to $K(\sqrt{\Delta}, \mu_3)$. Why does this allow to solve the cubic in principle?

6. From now on denote the three roots of P as x_1, x_2 and x_3. Consider $D = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$, so that $D^2 = \Delta$. Define also

$$A := x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1$$
$$B := x_1 x_2^2 + x_2 x_3^2 + x_3 x_1^2.$$

   Prove the following equalities

$$\alpha^3 = -9q + 3\xi A + 3\xi^2 B, \quad \beta^3 = -9q + 3\xi^2 A + 3\xi B$$

   Find A, B in terms of D and use this to find α and β. [*Hint:* See Chambert-Loir, *A field guide to algebra*, page 121, for further hints.]

Solution:

1. Since $\mathrm{char}(K) \neq 2$ we know that Δ is a square if and only if $\mathrm{Gal}(L/K)$ is a subgroup of A_3, which is not the case by hypothesis. Hence Δ is not a square in K and $[K(\sqrt{\Delta}) : K] = 2$. Recall that $\sqrt{\Delta}$ can be chosen to be equal to $\pm D$ (where D is taken as in Point 6), so that it is clearly an element of L. Moreover, $[L : K] = |\mathrm{Gal}(L/K)| = |S_3| = 6$, so that

$$[L : K(\sqrt{\Delta})] = [L : K]/[K(\sqrt{\Delta}) : K] = 3.$$

2. $L(\mu_3)$ is the splitting field of the polynomial P viewed as $P \in K(\sqrt{\Delta}, \mu_3)$, and as such it is a Galois extension of $K(\sqrt{\Delta}, \mu_3)$. Comparing the degrees in the two towers $L(\mu_3)/K(\sqrt{\Delta}, \mu_3)/K(\sqrt{\Delta})$ and $L(\mu_3)/L/K(\sqrt{\Delta})$ we see that

$$[L(\mu_3) : K(\sqrt{\Delta}, \mu_3)][K(\sqrt{\Delta}, \mu_3) : K(\sqrt{\Delta})] = [L(\mu_3) : L] \cdot 3$$

   the only possibility is that $[L(\mu_3) : K(\sqrt{\Delta}, \mu_3)] = 3$, because adjoining the cube roots of unity one only gets extensions of degree 1 or 2, so that $3 | [L(\mu_3) : K(\sqrt{\Delta}, \mu_3)]$, which cannot be 6 because that μ_3 would not be contained in L, and a fortiori neither in $K(\sqrt{\Delta})$.
   Since all groups of cardinality 3 are cyclic we get $\mathrm{Gal}(L(\mu_3)/K(\sqrt{\Delta}, \mu_3)) \cong \mathbb{Z}/3\mathbb{Z}$. Denote this Galois group by $G := \mathrm{Gal}(L(\mu_3)/K(\sqrt{\Delta}, \mu_3))$.

See next page!

3. Since $[K(y):K]=3$ for each root y of P, $K(\sqrt{\Delta},\mu_3)$ cannot contain any root of P, because $[K(\sqrt{\Delta},\mu_3):K]$ is either 2 or 4. Then P is irreducible in $K(\sqrt{\Delta},\mu_3)[X]$ and since $L(\mu_3)$ is its splitting field over $K(\sqrt{\Delta},\mu_3)$, G acts transitively on the roots of P, so that

$$\{x,\sigma(x),\sigma^2(x)\} = Z_P := \{y\in\bar{K} : P(y)=0\}.$$

4. $x+\sigma(x)+\sigma^2(x)=0$ because it is up to the sign equal to the coefficient of degree $3-1=2$ in P, which is 0. We can easily solve the following linear system in $x,\sigma(x),\sigma^2(x)$:

$$\begin{cases} x+\xi\sigma(x)+\xi^2\sigma^2(x)=\alpha \\ x+\xi^2\sigma(x)+\xi\sigma^2(x)=\beta \\ x+\sigma(x)+\sigma^2(x)=0 \end{cases}$$

to obtain

$$\begin{cases} x=\frac{1}{3}\alpha+\frac{1}{3}\beta \\ \sigma(x)=\frac{1}{3}\varrho^2\alpha+\frac{1}{3}\varrho\beta \\ \sigma^2(x)=\frac{1}{3}\varrho\alpha+\frac{1}{3}\varrho^2\beta. \end{cases}$$

5. Notice that $\sigma(\alpha)=\xi^{-1}\alpha$ and $\sigma(\beta)=\xi\beta$ (because $\xi^3=1$). Then by multiplicativity of σ we get

$$\sigma(\alpha^3)=\sigma(\alpha)^3=(\xi^{-1}\alpha)^3=\alpha^3$$
$$\sigma(\beta^3)=\sigma(\beta)^3=(\xi^{-2}\beta)^3=\beta^3,$$

and since σ generates G we obtain $\alpha^3,\beta^3\in L(\mu_3)^G=K(\sqrt{\Delta},\mu_3)$.
This allows to solve the equation by radicals, because it tells us that α and β are cubic roots of a rational expression of $\sqrt{\Delta}$ (which is a square root of $\Delta\in K$) and μ_3, so that in view of the previous point we can recover x, $\sigma(x)$ and $\sigma^2(x)$ as expressions containing radicals in terms of μ_3, which can be expressed in terms of $\sqrt{-3}$.

6. The equalities for α^3 and β^3 are obtained via an easy computation that is done in Chambert-Loir's book (see Hint).
Then one has $A-B=D$, while $A+B$ is a symmetric expression in x_1,x_2,x_3, so that it can be expressed in terms of elementary symmetric expressions in x_1,x_2,x_3, i.e., in terms of the coefficients of P. To do so, notice that

$$0=(x_1+x_2+x_3)(x_1x_2+x_1x_3+x_2x_3)=A+B+3x_1x_2x_3,$$

and we immediately deduce from $x_1x_2x_3=-q$ that $A+B=3q$.
This allows to find

$$A=\frac{3}{2}q+\frac{1}{2}\sqrt{\Delta} \text{ and } B=\frac{3}{2}q-\frac{1}{2}\sqrt{\Delta},$$

and obtain formulas by radicals for α and β and hence for the three roots of P. See Chambert-Loir, *A field guide to algebra*, page 121, for explicit formulas.