Solutions of exercise sheet 2

1. Let k be a field with $\mathrm{char}(k) \neq 2$.

1. Let $a, b \in k$ be such that a is a square in $k(\beta)$, where β is an element algebraic over k such that $\beta^2 = b$. Prove that either a or ab is a square in k. [*Hint:* Distinguish the cases $\beta \in k$ and $\beta \notin k$. For the second case, expand $(c + d\beta)^2$, for $c, d \in k$.]
2. Now consider $K = k(u, v)$, where $u, v \notin k$ are elements in an algebraic extension of k such that $u^2, v^2 \in k$. Set $\gamma = u(v + 1)$. Prove: $K = k(\gamma)$.

Solution:

1. If $\beta \in k$, then $k(\beta) = k$, so that a is a square in k. Else, β is algebraic of order 2 over k, and any element in $k(\beta)$ can be expressed as $c + d\beta$, with $c, d \in k$. In particular, for some c and d in k we have
$$a = (c + d\beta)^2 = (c^2 + bd^2) + 2cd\beta,$$
which gives, since 1 and β are two k-linear independent elements,
$$a = c^2 + bd^2,\ 2cd = 0.$$
Then, since $\mathrm{char}(k) \neq 2$, we get $cd = 0$, implying that $c = 0$ or $d = 0$. If $d = 0$, then $a = c^2$ is a square in k. Else $c = 0$, and $a = bd^2$, so that $ab = b^2d^2 = (bd)^2$ is a square in k.
2. The inclusion $K \supseteq k(\gamma)$ is clear, since $\gamma = u(v + 1) \in k(u, v) = K$. To prove the other inclusion, we need to show that $u, v \in k(\gamma)$. We have
$$k(\gamma) \ni \gamma^2 = u^2(v^2 + 2v + 1),$$
which implies, since $u^2, v^2 \in k \subseteq k(\gamma)$ and $\mathrm{char}(k) \neq 2$, that
$$v = \frac{1}{2}\left(\frac{\gamma^2}{u^2} - v^2 - 1\right) \in k(\gamma).$$
Then $v + 1 \in k(\gamma)$ as well, so that $u = \gamma(v + 1)^{-1} \in k(\gamma)$ and we are done. Notice that it makes sense to quotient by u and $v + 1$ because they cannot be zero as they lie outside k.

2.
1. Prove that if $[K : k] = 2$, then $k \subseteq K$ is a normal extension.
2. Show that $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ is normal.

Please turn over!

3. Show that $\mathbb{Q}(\sqrt[4]{2}(1+i))/\mathbb{Q}$ is not normal over $\mathbb{Q}$.
4. Deduce that given a tower $L/K/k$ of field extensions, L/k needs not to be normal even if L/K and K/k are normal.

Solution:

1. Since $[K:k]=2$, there is an element $\xi \in K \setminus k$. Then $k(\xi)/k$ is a proper intermediate extension of K/k, and the only possibility is that $K = k(\xi)$, so that ξ has a degree-2 minimal polynomial $f(X) = X^2 - sX + t \in k[X]$. Then $s - \xi \in k(\xi) = K$ and
$$f(s-\xi) = s^2 - 2s\xi + \xi^2 - s^2 + s\xi + t = -s\xi + \xi^2 + t = f(\xi) = 0.$$
Hence K is the splitting field of f, implying that K/k is a normal extension.
2. Let us prove that $\mathbb{Q}(\sqrt[4]{2}, i)$ is the splitting field of the polynomial $X^4 - 2 \in \mathbb{Q}[X]$ (which is irreducible by Eisenstein's criterion). This is quite straightforward: this splitting field must contain all the roots of the polynomials, i.e. $\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$, implying that it must contain $i\sqrt[4]{2}/\sqrt[4]{2} = i$, so that it must contain $\mathbb{Q}(sqrt[4]2, i)$. Clearly all the roots of X^4-2 lie $\mathbb{Q}(\sqrt[4]{2}, i)$ which is then the splitting field of $X^4 - 2$, so that it is a normal extension of $\mathbb{Q}$.
3. Since $i \notin \mathbb{R} \supseteq \mathbb{Q}(\sqrt[4]{2})$ satisfies the polynomial $X^2+1 \in \mathbb{Q}(\sqrt[4]{2})$, we have $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$. Moreover, $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ (as $X^4 - 2$ is irreducible by Eisenstein's criterion), so that
$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8.$$
Let $\gamma = \sqrt[4]{2}(1+i)$. It is enough to prove that the minimal polynomial of γ over $\mathbb{Q}$ does not split in $\mathbb{Q}(\gamma)$ to conclude that $\mathbb{Q}(\gamma)/\mathbb{Q}$ is not a normal extension.
Notice that $\gamma^2 = \sqrt{2}(1-1+2i)$, so that $\gamma^4 = -8$, and γ satisfies the polynomial $g(X) = X^4 + 8 \in \mathbb{Q}[X]$. Hence $[\mathbb{Q}(\gamma) : \mathbb{Q}] \leq 4$. On the other hand,
$$\mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\sqrt[4]{2}(1+i), i) = \mathbb{Q}(\gamma)(i),$$
with $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\gamma)] \leq 2$ since i satisfies $X^2 + 1 \in \mathbb{Q}(\gamma)[X]$. Then
$$8 = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\gamma)(i) : \mathbb{Q}(\gamma)][\mathbb{Q}(\gamma) : \mathbb{Q}],$$
and the only possibility is that $[\mathbb{Q}(\gamma)(i) : \mathbb{Q}(\gamma)] = 2$ and $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 4$. In particular, $g(X)$ is the minimal polynomial of γ over $\mathbb{Q}$, and $i \notin \mathbb{Q}(\gamma)$. But the roots of $g(X)$ are easily seen to be $u\gamma$, for $u \in \{\pm 1, \pm i\}$, so that the root $i\gamma$ of g does not lie in $\mathbb{Q}(\gamma)$ (as $i \notin \mathbb{Q}(\gamma)$).
4. Let $k = \mathbb{Q}$, $L = \mathbb{Q}(\gamma)$ and $K = \mathbb{Q}(\gamma^2)$. Then $\gamma^2 = 2\sqrt{2}i \notin \mathbb{Q}$ satisfies the degree-2 polynomial $Y^2 + 8 \in \mathbb{Q}[Y]$, so that $[K:k] = 2$. Since $[L:k] = 4$, we have $[L:K] = 2$. Then by point 1 the extensions L/K and K/k are normal, while L/k is not by previous point.

3. Let K be a field, and $L = K(X)$ its field of rational functions.

See next page!

1. Show that, for any $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$, the map

$$\sigma_A(f) = f\left(\frac{aX+b}{cX+d}\right)$$

defines a K-automorphism of L, and we obtain a group homomorphism

$$i : \mathrm{GL}_2(K) \longrightarrow \mathrm{Aut}(L/K).$$

2. Compute $\ker(i)$.
3. For $f \in K(X)$, write $f = \frac{p(X)}{q(X)}$, with $p(X), q(X) \in K[X]$ coprime polynomials. Prove that $p(X) - q(X)Y$ is an irreducible polynomial in $K[X,Y]$, and deduce that X is algebraic of degree $\max\{\deg(p), \deg(q)\}$ over $K(f)$.
4. Conclude that i is surjective [*Hint:* For $\sigma \in \mathrm{Aut}(L/K)$, apply previous point with $f = \sigma(X)$].
5. Is an endomorphism of the field $K(X)$ which fixes K always an automorphism?

Solution:

1. Since σ_A operates on $f \in K(X)$ just by substituting X with $\sigma_A(X)$, it is clear that σ_A is a field endomorphism fixing K. Define the map $i : \mathrm{GL}_2(K) \longrightarrow \mathrm{End}_K(L)$ sending $A \mapsto \sigma_A$. If we prove that it is a map of monoids (i.e., it respects multiplication), then its image will clearly lie in the submonoid of invertible elements of the codomain $\mathrm{Aut}(L/K) \subseteq End_K(L)$ because the domain is a group (explicitly, σ_A will have inverse $\sigma_{A^{-1}}$).
   We are then only left to prove that $\sigma_{AB} = \sigma_A\sigma_B$. Notice that we can write, for $f \in L = K(X)$, the equality $\sigma_A(f(X)) = f(\sigma_A(X))$ because σ_A is a field homomorphism. Then

$$(\sigma_A\sigma_B)(f(X)) = \sigma_A(\sigma_B(f(X))) = \sigma_A(\sigma_B(f(X))) = f(\sigma_A\sigma_B(X)),$$

   so that we only need to prove that $\sigma_{AB}(X) = \sigma_A\sigma_B(X)$. This just an easy computation, which was already done (for $K = \mathbb{R}$) in Algebra I (HS14), Exercise sheet 2, Exercise 4. Hence i is multiplicative.
2. The kernel of i consists of matrix A such that $\sigma_A(f) = f$ for every $f \in K(X)$. Since σ_A is a K-automorphism of $L = K(X)$, this condition is equivalent to $\sigma_A(X) = X$, i.e., $\frac{aX+b}{cX+d} = X$, which is equivalent to $aX + b = cX^2 + dX$, i.e. $a = d$ and $c = b = 0$. Hence

$$\ker(i) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in \mathrm{GL}_2(K) \right\}.$$

3. As K is a field, $K[X]$ is an integral domain, so that for $t, u \in K[X,Y]$ we have $\deg_Y(tu) = \deg_Y(t) + \deg_Y(u)$, and each decomposition of $r(X,Y) = p(X) + Yq(X)$ is of the type $r(X,Y) = t(X)u(X,Y)$, with $u(X,Y) = u_0(X) + Yu_1(X)$.

Please turn over!

Then $t(X)$ needs to be a common factor of $p(X)$ and $q(X)$, which are coprime, so that $t(X)$ is constant. This proves that $r(X,Y) = p(X) + Yq(X)$ is irreducible in $K[X,Y]$.

We now prove that $r(X,Y)$ is also irreducible in $K(Y)[X]$: suppose that $K[X,Y] \ni r(X,Y) = r_1(X,Y)r_2(X,Y)$, with $r_i(X,Y) \in K(Y)[X]$. Then we can write $r_i(X,Y) = \frac{1}{R_i(Y)} s_i$, with $s_i \in K[Y][X]$ a primitive polynomial in X, that is, a polynomial in X whose coefficients are coprime polynomials in Y, and $R_i(Y) \in K[Y]$. It is easily seen that the product of two primitive polynomials is again primitive, so that from $r(X,Y) \in K[X,Y]$ we get that $R_1(Y)$ and $R_2(Y)$ are constant polynomials, and the factorization of r is a factorization in $K[X,Y]$.

Now X is a root of the irreducible polynomial $s(T) := r(T,f) \in K(f)[T]$, so that $[K(X) : K(f)] = \deg(s) = \max\{\deg(p), \deg(q)\}$ as desired.

4. For every $\sigma \in \mathrm{Aut}(L/K)$ and $f \in L$, we have

$$\sigma(f(X)) = f(\sigma(X)),$$

so that we just need to prove that $\sigma(X)$ is a quotient of degree-1 polynomials. Clearly, the image of L via σ is $K(\sigma(X))$, and we have seen in the previous point that $K(\sigma(X))$ is a subfield of $K(X)$. Then surjectivity of σ is attained only when $\max\{\deg(p), \deg(q)\} = 1$, so that any K-automorphism of L comes is of the form σ_A for some $A \in \mathrm{GL}_2(K)$. In conclusion, i is surjective.

5. No. Indeed, one can send $X \mapsto X^2$ to define a K-endomorphism τ of L. Then the image $K(X^2)$ of this field endomorphism is a subfield of $K(X)$, and $[K(X^2) : K(X)] = 2$ by what we have seen in the previous points, so that τ is not surjective.

4.

1. Let K be field containing $\mathbb{Q}$. Show that any automorphism of K is a $\mathbb{Q}$-automorphism.
2. From now on, let $\sigma : \mathbb{R} \longrightarrow \mathbb{R}$ be a field automorphism. Show that σ is increasing:

$$x \leq y \Longrightarrow \sigma(x) \leq \sigma(y).$$

3. Deduce that σ is continuous.
4. Deduce that $\sigma = \mathrm{Id}_{\mathbb{R}}$.

Solution:

1. Let $\sigma : K \longrightarrow K$ a field automorphism, and suppose that $\mathbb{Q} \subseteq K$. Then $\mathbb{Z} \subseteq K$, and for every $n \in \mathbb{Z}$ one has $\sigma(n) = \sigma(n \cdot 1) = n\sigma(1)$, by writing n as a sum of 1's or -1's and using additivity of σ. Hence $\sigma|_{\mathbb{Z}} = \mathrm{Id}_{\mathbb{Z}}$. Now suppose $f \in \mathbb{Q}$, and write $f = mn^{-1}$ with $n \in \mathbb{Z}$. Then by multiplicativity of σ we obtain $\sigma(f) = \sigma(m)\sigma(n^{-1}) = mn^{-1} = f$, so that $\sigma|_{\mathbb{Q}} = \mathrm{Id}_{\mathbb{Q}}$ and σ is a $\mathbb{Q}$-isomorphism.
2. Let $x, y \in \mathbb{R}$ such that $x \leq y$. Then $y - x \geq 0$, so that there exist $z \in \mathbb{R}$ such that $y - x = z^2$. Then

$$\sigma(y) - \sigma(x) = \sigma(y - x) = \sigma(z^2) = \sigma(z)^2 \geq 0,$$

so that $\sigma(y) \geq \sigma(x)$ and σ is increasing.

See next page!

3. To prove continuity, it is enough to check that counterimages of intervals are open. For $I = (a, b) \subseteq \mathbb{R}$ an interval with $a \neq b$, by surjectivity of σ there exist $\alpha, \beta \in \mathbb{R}$ such that $\sigma(\alpha) = a$ and $\sigma(\beta) = b$, and since σ is injective and increasing we need $\alpha < \beta$. Then $\sigma^{-1}(I) = \{x \in \mathbb{R} : a < \sigma(x) < b\} = \{x \in \mathbb{R} : \sigma(\alpha) < \sigma(x) < \sigma(\beta)\} = (\alpha, \beta)$, which is an open interval in $\mathbb{R}$. Hence σ is continuous.
4. Now σ is continuous and so is $\mathrm{Id}_{\mathbb{R}}$. By point 1, those two maps coincide on $\mathbb{Q}$, which is a dense subset of $\mathbb{R}$. Then they must coincide on the whole $\mathbb{R}$, so that $\sigma = \mathrm{Id}_{\mathbb{R}}$.