Warm-up (not to be handed in)

[DF], §13.1, exercises 1,3,4,5,7, §13.2, exercises 2,3,4,14.

1. Exercises to be handed in

Exercise 1. Do [DF], §13.1, 8.

Solution. If \( x^5 - ax - 1 \) is reducible, then it has a linear or an irreducible quadratic factor. Suppose that \( x^5 - ax - 1 \) has a linear factor. Then there exists an integer \( b \) such that \( b^5 - ab - 1 = 0 \). Clearly, \( b \) must divide 1 so \( b = 1 \) or \( b = -1 \). If \( b = 1 \) we get \( 1 - a - 1 = 0 \) so \( a = 0 \). If \( b = -1 \) then \( -1 + a - 1 = 0 \) so \( a = 2 \). Suppose that \( x^5 - ax - 1 \) has a quadratic factor. Such a quadratic factor \( q(x) \) has to be of the form \( x^2 + \lambda x + 1 \) or \( x^2 + \lambda x - 1 \).

Suppose that \( q(x) = x^2 + \lambda x + 1 \). If \( \alpha \) is a root of \( q(x) \) then so is \( 1/\alpha \). So \( \alpha \) is a solution of
\[
x^5 - ax - 1 = 0
\]
hence a solution of
\[
1 - ax^4 + x^5 = 0
\]
If we subtract \( x^5 - ax + 1 = 0 \) we get that \( \alpha \) is a solution of
\[
-ax^4 + ax = (-ax)(x + 1)(x^2 - x + 1).
\]
Since \( \alpha \neq 0, -1 \) we get that \( q(x) = x^2 - x + 1 \). Using division with remainder gives us \( a = -1 \).

Suppose \( q(x) = x^2 + \lambda x - 1 \). If \( \alpha \) is a root of \( q(x) \), then \( -1/\alpha \) is a root of \( q(x) \). So \( \alpha \) is a solution of
\[
-x^5 + ax^{-1} - 1 = 0
\]
hence a solution of
\[
-1 + ax^4 - x^5 = 0
\]
if we add \( x^5 - ax + 1 = 0 \) then we see that \( \alpha \) is a solution of
\[
a x^4 - ax = (ax)(x - 1)(x^2 + x + 1).
\]
From this follows that \( a = 0 \) or \( q(x) = x^2 + x + 1 \). The remainder of division of \( x^5 - ax - 1 \) by \( x^2 + x + 1 \) is \( (-a - 1)x - 2 \). There is no solution for \( a = 0 \) for which the remainder is equal to 0.

Solution. Clearly $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ so $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Conversely $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$, so $\sqrt{6} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Moreover $\sqrt{6}(\sqrt{2} + \sqrt{3}) = 3\sqrt{2} + 2\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, hence $\sqrt{2} = (3\sqrt{2} + 2\sqrt{3} - 2(\sqrt{2} + \sqrt{3}) \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ and $\sqrt{3} = (\sqrt{2} + \sqrt{3}) - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. This shows that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Exercise 3. Do [DF], §13.2, 16.

Solution. Suppose that $\alpha \in R$ and $\alpha \neq 0$. Then $\alpha$ is algebraic over $F$ because $\alpha \in K$. Suppose that $\alpha$ is a root an irreducible polynomial
\[ p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \]
where $a_0, a_1, \ldots, a_{n-1} \in F$. If $a_0 = 0$ then $n = 1$ because $p(x)$ is irreducible and $x$ is an irreducible factor of $p(x)$. But then $\alpha$ is a root of $p(x) = x$ and $\alpha = 0$. Contradiction. So $a_0 \neq 0$. We have
\[ p(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0 \]
so
\[ \alpha(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1) = -a_0 \]
It follows that
\[ \alpha^{-1} = (-a_0)^{-1}(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1) \in R. \]
So $R$ is closed under inverses of nonzero elements, and $R$ must be a subfield of $K$.


Solution. Suppose that $h(x)$ is an irreducible factor of $f(g(x))$. Consider the field $K = F[x]/(h(x))$ and set $\alpha = x + (h(x))$. Since $h(\alpha) = 0$, we have $f(\alpha) = 0$. Let $L = F(\alpha)$. Then $L \cong F[x]/(f(x))$. In particular, $[L : F] = n$ where $n$ is the degree of $f(x)$. Since $K$ contains $L$, we have that $[K : F]$ is divisible by $n = [L : F]$. On the other hand $[K : F]$ is the degree of $h(x)$.


Solution. (a) Suppose that $P(X) - tQ(X)$ is irreducible as a polynomial in $k(t)[X]$. By Gauss’ Lemma, it is irreducible if and only if it is irreducible over $k[t, X]$. If $P(X) - tQ(X) = R(X, t)U(X, t)$ with $R(X, t), U(X, t) \in k[X, t]$, then the degree of one of the polynomials $R(X, t), U(X, t)$ as a polynomial in $t$ must be equal to 0. Say $R(X, t) = R(X)$ has degree 0. But then $R(X)$ is a common divisor of $P(X)$ and $Q(X)$ so $R(X)$ must be constant. This shows that $P(X) - tQ(X)$ is irreducible.

(b) The degree of $P(X) - tQ(X)$ as a polynomial in $X$ is clearly $\max\{\deg(P(X)), \deg(Q(X))\}$.

(c) So $[k(x) : k(t)] = [k(t)(x) : k(t)] = \deg_x(P(X) - tQ(X)) = \max\{\deg(P(X)), \deg(Q(X))\}$, because $P(X) - tQ(X)$ is, up to a scalar, the minimum polynomial of $x$. 


Solution. The map \( \varphi : K_1 \times K_2 \to K_1 K_2 \) given by \( \varphi(a, b) = ab \) is clearly bilinear (over the field \( F \)). Therefore, there is a unique linear map \( \Phi : K_1 \otimes_F K_2 \to K_1 K_2 \) such that \( \Phi(a \otimes b) = ab \) for all \( a \in K_1, b \in K_2 \). The ring homomorphism \( \Phi \) is surjective. This follows from the proof of Theorem 14: Elements of the form \( ab \) with \( a \in K_1 \) and \( b \in K_2 \) span \( K_1 K_2 \) if \( K_1, K_2 \) are finite extensions of \( F \).

Note that \( \dim_F K_1 \otimes_F K_2 = \dim_F K_1 \cdot \dim_F K_2 = [K_1 : F][K_2 : F] \).

If \( [K_1 K_2 : F] = [K_1 : F][K_2 : F] \) then \( \dim_F K_1 \otimes_F K_2 = \dim_F K_1 K_2 \) and \( \Phi \) must be bijective. It follows that \( \Phi \) is an isomorphism of rings, hence \( K_1 \otimes_F K_2 \) is a field because \( K_1 K_2 \) is a field.

If \( [K_1 K_2 : F] \neq [K_1 : F][K_2 : F] \), then \( \Phi \) is not injective. Then the kernel of \( \Phi \) is a nontrivial ideal, and \( K_1 \otimes_F K_2 \) cannot be a field.

Harm Derksen, 3067EH, 763 2309
Office hours: **MWF 3-4pm**.

http://www.math.lsa.umich.edu/~hderksen/math594.w06/index.html