# School of Mathematics and Statistics

# MT5836 Galois Theory

# Problem Sheet IV: Separability; separable extensions; the Theorem of the Primitive Element (Solutions)

1. **Show that $X^3 + 5$ is separable over $\mathbb{F}_7$.**

**Solution:** First calculate the cubes in $\mathbb{F}_7$:

$$\begin{aligned} 0^3 &= 0, & 1^3 &= 1, \\ 2^3 &= 1, & 3^3 &= 6, \\ 4^3 &= 1, & 5^3 &= 6, \\ 6^3 &= 6. \end{aligned}$$

Since $a^3 \neq 2$ for all $a \in \mathbb{F}_7$, we conclude $f(X) = X^3 + 5$ has no roots in $\mathbb{F}_7$. Therefore it has no linear factors over $\mathbb{F}_7$ and so is irreducible.

There are now (at least) two different ways to proceed. The first is to note that if $\alpha$ is a root of $f(X)$ in some splitting field, then $\alpha^3 + 5 = 0$,

$$(2\alpha)^3 + 5 = 2^3\alpha^3 + 5 = \alpha^3 + 5 = 0$$

and

$$(4\alpha)^3 + 5 = 4^3\alpha^3 + 5 = \alpha^3 + 5 = 0.$$

Hence $f(X)$ has three distinct roots, $\alpha$, $2\alpha$ and $4\alpha$, in the splitting field.

Alternatively, the formal derivative is

$$Df(X) = 3X^2$$

and since $X$ does not divide $f(X)$ (as $f(0) \neq 0$, for example), we conclude $f(X)$ and $Df(X)$ have no common factor of degree $\geqslant 1$. Thus $f(X)$ has no repeated roots in the splitting field.

Using either of the above methods, we conclude $f(X) = X^3 + 5$ is separable over $\mathbb{F}_7$.

2. **Let $F$ be a field of positive characteristic $p$ and let $f(X)$ be an *irreducible* polynomial over $F$. Show that $f(X)$ is inseparable over $F$ if and only if it has the form**

$$f(X) = a_0 + a_1X^p + a_2X^{2p} + \cdots + a_kX^{kp}$$

**for some positive integer $k$ and some coefficients $a_0, a_1, \ldots, a_k \in F$.**

**Solution:** Suppose $f(X)$ has the form

$$f(X) = a_0 + a_1 X^p + a_2 X^{2p} + \cdots + a_k X^{kp}.$$

Then $Df(X) = 0$, since $F$ has characteristic $p$. Thus $f(X)$ is a common factor of both $f(X)$ and $Df(X)$, of degree $kp > 1$. Hence $f(X)$ has a repeated root in a splitting field.

Conversely, if $f(X)$ does not have the above form then $f(X)$ has some term $b_i X^i$ where $b_i \neq 0$ and $i$ is not a multiple of $p$. Then $b_i i X^{i-1}$ occurs as a non-zero term in the formal derivative $Df(X)$, so $Df(X) \neq 0$. Now the greatest common divisor $h(X)$ divides $f(X)$, which is irreducible, so $h(X) = 1$ or $f(X)$. However, the formal derivative is a non-zero polynomial of degree $\deg Df(X) \leqslant \deg f(X) - 1$, so $h(X)$ has degree less than that of $f(X)$. This forces $h(X) = 1$ and we conclude $f(X)$ and $Df(X)$ have no common factor of degree $\geqslant 1$. This shows $f(X)$ has no common factor in a splitting field.

In conclusion, $f(X)$ is inseparable over $F$ if and only if it has the form

$$f(X) = a_0 + a_1 X^p + a_2 X^{2p} + \cdots + a_k X^{kp}$$

for some positive integer $k$ and some $a_i \in F$.

3. **Let $F \subseteq K \subseteq L$ be field extensions such that $L$ is a separable extension of $F$.**

   **(a) Show that $K$ is a separable extension of $F$.**

   **(b) Show that $L$ is a separable extension of $K$.**

**Solution:** (a) Let $\alpha \in K$. Then as $K \subseteq L$, we use the fact that $L$ is a separable extension of $F$ to conclude that the minimum polynomial of $\alpha$ over $F$ is separable. We therefore conclude $K$ is a separable extension of $F$.

(b) Let $\alpha \in L$. Let $f(X)$ be the minimum polynomial of $\alpha$ over $K$ and $g(X)$ be the minimum polynomial of $\alpha$ over $F$. Since $F \subseteq K$, $g(X)$ is also a polynomial in $K[X]$ that has $\alpha$ as a root, so it is divisible by $f(X)$ (as the latter is the minimum polynomial of $\alpha$ over $K$). Now by hypothesis, $g(X)$ has distinct roots in a field in which it splits. The same therefore applies to the polynomial $f(X)$ as it divides $g(X)$. We conclude that $f(X)$ has distinct roots in its splitting field. This establishes that $L$ is a separable extension of $K$.

4. **Find $\alpha$ such that $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\alpha)$.**

**Solution:** One method is to follow the proof of Lemma 4.10. The minimum polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $f(X) = X^2 - 2$ with roots

$$\beta_1 = \sqrt{2} \qquad \text{and} \qquad \beta_2 = -\sqrt{2}$$

in $\mathbb{Q}(\sqrt{2}, i)$. The minimum polynomial of $i$ over $\mathbb{Q}$ is $g(X) = X^2 + 1$ with roots

$$\gamma_1 = i \qquad \text{and} \qquad \gamma_2 = -i$$

in $\mathbb{Q}(\sqrt{2}, i)$. We now take $c \in \mathbb{Q}$ with $c \neq 0$ and

$$c \neq \frac{\beta_1 - \beta_2}{\gamma_1 - \gamma_2} = \frac{2\sqrt{2}}{2i} = -i\sqrt{2}.$$

The proof of the lemma shows that

$$\mathbb{Q}(\beta_1 - c\gamma_1) = \mathbb{Q}(\beta_1, \gamma_1) = \mathbb{Q}(\sqrt{2}, i).$$

For example, taking $c = 1$, we conclude

$$\mathbb{Q}(\sqrt{2} - i) = \mathbb{Q}(\sqrt{2}, i).$$

So $\alpha = \sqrt{2} - i$ is a valid solution.

An alternative method to establish the same thing (at least once we have guessed a suitable $\alpha$) is to proceed more directly and exploit the Tower Law. Observe

$$|\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}| = |\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})| \cdot |\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 4$$

since the minimum polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $X^2 - 2$, so $|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$, and the minimum polynomial of $i$ over $\mathbb{Q}(\sqrt{2})$ is $X^2 + 1$ (as the latter has non-real complex roots so is not factorizable into linear factors over $\mathbb{Q}(\sqrt{2})$), so $|\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})| = 2$.

Now $\mathbb{Q}(\sqrt{2} - i)$ is a subfield of $\mathbb{Q}(\sqrt{2}, i)$, so $|\mathbb{Q}(\sqrt{2} - i) : \mathbb{Q}|$ divides $|\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}| = 4$. Thus the minimum polynomial of $\alpha = \sqrt{2} - i$ over $\mathbb{Q}$ has degree 1, 2 or 4. Now $\sqrt{2} - i \notin \mathbb{Q}$ (as it is not real), so the minimum polynomial cannot have degree 1. If it were to have degree 2, there exists $p, q \in \mathbb{Q}$ such that

$$\alpha^2 + p\alpha + q = 0;$$

that is,

$$(\sqrt{2} - i)^2 + p(\sqrt{2} - i) + q = 0,$$

or

$$-\sqrt{2}\, i + p\sqrt{2} - pi + (q + 1) = 0.$$

This equation asserts that $\{\sqrt{2}\, i, \sqrt{2}, i, 1\}$ are linearly dependent over $\mathbb{Q}$, which is a contradiction to our above application of the Tower Law as $|\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}| = 4$ corresponding to $\{\sqrt{2}\, i, \sqrt{2}, i, 1\}$ being a basis for $\mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$.

We conclude that the minimum polynomial of $\alpha = \sqrt{2} - i$ over $\mathbb{Q}$ has degree 4, so we determine that $|\mathbb{Q}(\sqrt{2} - i) : \mathbb{Q}| = 4$. As this is the same degree over $\mathbb{Q}$ as $\mathbb{Q}(\sqrt{2}, i)$, we therefore conclude

$$\mathbb{Q}(\sqrt{2} - i) = \mathbb{Q}(\sqrt{2}, i),$$

as required.

5. **Let $p$ be a prime, $F = \mathbb{F}_p(t)$ be the field of rational functions over the finite field $\mathbb{F}_p$, and $f(X)$ be the following polynomial from the polynomial ring $F[X]$:**

$$f(X) = X^p - t.$$

   (a) **Show that $f(X)$ has no roots in $F$.**

   (b) **Let $\alpha$ be a root of an irreducible factor of $f(X)$ in some extension field. Show that $K = F(\alpha)$ is a splitting field for $f(X)$ and that**

$$f(X) = (X - \alpha)^p$$

   **over the field $K$.**

   (c) **By considering the factorization of $g(X)$ over $K$, or otherwise, show that it is impossible to factorize $f(X)$ as $f(X) = g(X)\, h(X)$ where $g(X), h(X) \in F[X]$ are polynomials over $F$ of smaller degree than $f(X)$.**

   (d) **Conclude that $f(X)$ is a inseparable polynomial over $F$.**

**Solution:** (a) Suppose $\alpha \in F$ is a root of $f(X)$. Then $\alpha = q(t)/r(t)$ for some polynomials $q(t), r(t) \in \mathbb{F}_p[t]$. Then

$$\left(\frac{q(t)}{r(t)}\right)^p - t = 0;$$

that is,

$$q(t)^p = r(t)^p\, t.$$

Since $r(t)$ is necessarily non-zero, the same is then true for $q(t)$. Let $m$ and $n$ be the degrees of $q(t)$ and $r(t)$, respectively. Then

$$pm = pn + 1,$$

which is impossible as $p \nmid 1$. Hence $f(X)$ has no roots in $F$.

(b) Let $\alpha$ be a root of $f(X)$ in some extension. Then $\alpha^p = t$, so

$$f(X) = X^p - t = X^p - \alpha^p = (X - \alpha)^p$$

in $F(\alpha)$, using the fact that $F$ has characteristic $p$. We conclude that $f(X)$ factorizes as a product of linear factors in $F(\alpha)$. As $\alpha$ is the only root of $f(X)$, we conclude $K = F(\alpha)$ is indeed a splitting field for $f(X)$ over $F$.

(c) Suppose $f(X)$ factorizes as $f(X) = g(X)\, h(X)$ over $F$ with $g(X), h(X) \in F[X]$ of smaller degree than $f(X)$. Passing to the splitting field $K = F(\alpha)$, we obtain

$$g(X)\, h(X) = (X - \alpha)^p.$$

The right-hand side is a factorization into irreducible factors (as each $X - \alpha$ has degree 1), so by uniqueness of factorization in $K[X]$,

$$g(X) = (X - \alpha)^k$$

where $1 \leqslant k \leqslant p - 1$. Thus

$$g(X) = X^k + k\alpha X^{k-1} + \sum_{i=2}^{k} \binom{k}{i} \alpha^i X^{k-i}.$$

In particular, $k\alpha \in F$ and as $k < p$ we can divide by $k$ (it is non-zero in $F$) to conclude $\alpha \in F$. This contradicts the conclusion of part (a). Hence $f(X)$ is not factorizable as a product of polynomials in $F[X]$ of smaller degree; that is, $f(X)$ is irreducible over $F$.

(d) We observed in (c) that $f(X)$ is irreducible over $F$ and in (b) that $f(X)$ has repeated roots in the splitting field $K = F(\alpha)$. Hence $f(X)$ is an inseparable polynomial over $F$.