MRQ 2019

School of Mathematics and Statistics

MT5836 Galois Theory

Problem Sheet I: Rings, fields, polynomials and irreducibility

1. Write out the addition and multiplication tables for the field $\mathbb{F}_7$ of seven elements.
2. Let F be a field.
   (a) If $\{ K_i \mid i \in I \}$ is a collection of subfields of F, show that $\bigcap_{i \in I} K_i$ is a subfield of F.
   (b) Show that the prime subfield of F is the intersection of all the subfields of F.
3. Show that every finite integral domain with $1 \neq 0$ is a field.
4. Let R be an integral domain containing a subring F that happens to be a field.
   (a) Show that R has the structure of a vector space over F.
   (b) Show that if R has finite dimension over F, then R is a field.
   (c) Is the result of (b) still valid if we permit R to have infinite dimension over the field F?
5. Let p be a prime number and consider the finite field $\mathbb{F}_p$ of p elements.
   (a) Show that $a^{p-1} = 1$ for all non-zero elements a in $\mathbb{F}_p$.
   (b) Show that in the polynomial ring $\mathbb{F}_p[X]$,
   $$X^p - X = X(X-1)(X-2)\dots(X-(p-1)).$$
6. Let $I = (X^4 + 1)$ be the ideal of the polynomial ring $\mathbb{F}_2[X]$ generated by the polynomial $X^4 + 1$. Let $R = \mathbb{F}_2[X]/I$ be the quotient ring.
   (a) Show that every element of R can be expressed uniquely in the form
   $$I + (aX^3 + bX^2 + cX + d)$$
   where $a, b, c, d \in \mathbb{F}_2$.
   (b) Show that $|R| = 16$.
   (c) Show that $d \mapsto I + d$ determines an isomorphism between $\mathbb{F}_2$ and a subring of R.
   (d) Show that R can be endowed with the structure of a vector space over the field $\mathbb{F}_2$ and determine the dimension of this vector space.
7. Show that the following polynomials are irreducible over $\mathbb{Q}$:
   (a) $X^n - p$, where n is a positive integer and p is a prime;
   (b) $X^6 + 168X^2 - 147X + 63$;
   (c) $X^3 - 3X - 1$;
   (d) $X^3 + 2X^2 - 3X + 5$.

8. Determine whether or not the following polynomials are irreducible over the given field:

   (a) $X^4 + 7$ over $\mathbb{F}_{17}$;

   (b) $X^3 - 5$ over $\mathbb{F}_{11}$.

9. Determine all the irreducible polynomials of degree at most four over the field $\mathbb{F}_2$ of two elements.

MRQ 2019

School of Mathematics and Statistics

MT5836 Galois Theory

Problem Sheet II: Field extensionions: Algebraic elements, minimum polynomials, simple extensions

1. Let K be an extension of the field F such that the degree $|K : F|$ is a prime number. Show that there are no *intermediate* fields between F and K; that is, no fields L satisfying $F \subset L \subset K$.

2. For each choice of values of $a, b \in \mathbb{Q}$, determine the minimum polynomial of $a + b\sqrt{2}$ over $\mathbb{Q}$.

3. (a) Show that $\mathbb{C}$ is a simple extension of $\mathbb{R}$.
   (b) What are the irreducible polynomials over $\mathbb{C}$?
   (c) Show that if α is algebraic over $\mathbb{C}$, then $\mathbb{C}(\alpha) = \mathbb{C}$.

4. Let α be algebraic over the base field F. Show that every element of the simple extension $F(\alpha)$ is algebraic over F.

5. Show that the polynomial $f(X) = X^4 - 16X^2 + 4$ is irreducible over $\mathbb{Q}$.

   Let α be a root of $f(X)$ in some field extension of $\mathbb{Q}$. Determine the minimum polynomials of α^2 and of $\alpha^3 - 14\alpha$ over $\mathbb{Q}$.

6. Determine the following degrees of field extensions:

   (a) $|\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}|$
   (b) $|\mathbb{Q}(\mathrm{e}^{2\pi i/5}) : \mathbb{Q}|$
   (c) $|\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}|$
   (d) $|\mathbb{Q}(\sqrt{2}i) : \mathbb{Q}|$
   (e) $|\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}|$
   (f) $|\mathbb{Q}(\sqrt{6}, i) : \mathbb{Q}(i)|$

7. Let $\alpha \in \mathbb{C}$ be a root of the polynomial $X^2 + 2X + 5$. Express the element

$$\frac{\alpha^3 + \alpha - 2}{\alpha^2 - 3}$$

   of $\mathbb{Q}(\alpha)$ as a linear combination of the basis $\{1, \alpha\}$.

8. Show that $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\sqrt{2} + \sqrt{5})$.

   Determine the minimum polynomial of $\sqrt{2} + \sqrt{5}$ over the following subfields:

   (i) $\mathbb{Q}$; (ii) $\mathbb{Q}(\sqrt{2})$; (iii) $\mathbb{Q}(\sqrt{5})$.

9. Let α and β be algebraic elements over the base field F. Suppose that the minimum polynomial of α over F has degree m, the minimum polynomial of β over F has degree n, and that m and n are coprime. Show that $|F(\alpha, \beta) : F| = mn$.

10. Let α be transcendental over the field F. Show that there is an isomorphism ψ from the field $F(X)$ of rational functions in the indeterminate X over F to the simple extension $F(\alpha)$ satisfying $X\psi = \alpha$ and $b\psi = b$ for all $b \in F$.

11. (a) Show that the field $\mathbb{A}$ of algebraic numbers over $\mathbb{Q}$ is countable.
    (b) Show that $\mathbb{C}$ is an infinite degree extension of $\mathbb{A}$.
    (c) Show that $\mathbb{C}$ contains elements that are transcendental over $\mathbb{Q}$.

MRQ 2019

School of Mathematics and Statistics

MT5836 Galois Theory

Problem Sheet III: Splitting Fields and Normal Extensions

1. For each of the following polynomials $f(X)$ and given base field F, determine the splitting field K of $f(X)$ over F and calculate the degree $|K : F|$ of the extension:

   (a) $X^2 + 1$ over $\mathbb{Q}$;
   (b) $X^2 + 1$ over $\mathbb{R}$;
   (c) $X^2 - 4$ over $\mathbb{Q}$;
   (d) $X^4 + 4$ over $\mathbb{Q}$;
   (e) $X^4 - 1$ over $\mathbb{Q}$;
   (f) $X^4 + 1$ over $\mathbb{Q}$;
   (g) $X^6 - 1$ over $\mathbb{Q}$;
   (h) $X^6 + 1$ over $\mathbb{Q}$;
   (i) $X^6 - 27$ over $\mathbb{Q}$.

2. For each of the following polynomials $f(X)$ and given base field F, determine the degree of the splitting field of $f(X)$ over F:

   (a) $X^3 - 2$ over $\mathbb{F}_5$;
   (b) $X^3 - 3$ over $\mathbb{F}_{13}$.

   [Hint: If $f(X)$ is irreducible over the base field F, consider adjoining some root α to F and examine the behaviour of $f(X)$ over the resulting field $F(\alpha)$.]

3. Let p be a prime and $f(X) = X^p - 2$. Find the splitting field of $f(X)$ over $\mathbb{Q}$ and show that the degree of this extension is $p(p-1)$.

4. Let $f(X)$ be a polynomial over a field F and let K be the splitting field of $f(X)$ over F. If L is an intermediate field (that is, $F \subseteq L \subseteq K$), show that K is the splitting field of $f(X)$ over L.

5. Let ϕ be an automorphism of a field F. Show that the set of fixed-points of ϕ,

   $$\mathrm{Fix}_F(\phi) = \{\, a \in F \mid a\phi = a \,\},$$

   is a subfield of F. Hence deduce that ϕ is a P-isomorphism where P is the prime subfield of F.

6. (a) Determine all automorphisms of $\mathbb{Q}$.
   (b) Determine all automorphisms of $\mathbb{Q}(\sqrt{2})$.
   (c) Determine all $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.
   (d) Show that the only automorphism of $\mathbb{R}$ is the identity.

7. Suppose that $f(X)$ is an arbitrary polynomial over a field F, K is the splitting field for $f(X)$ over F, and α and β are roots of $f(X)$ in K. Does there necessarily exist an automorphism of K that maps α to β?

8. Which of the following fields are normal extensions of $\mathbb{Q}$? [As always, justify your answers.]

   (a) $\mathbb{Q}(\sqrt{2})$;
   (b) $\mathbb{Q}(\sqrt[4]{2})$;
   (c) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$;
   (d) $\mathbb{Q}(\theta)$, where $\theta^4 - 10\theta^2 + 1 = 0$.

9. Let $F \subseteq K \subseteq L$ be field extensions where L is a finite extension of F. Prove, or give a counterexample, to each of the following assertions:

   (a) If L is a normal extension of K, then L is a normal extension of F.
   (b) If L is a normal extension of F, then L is a normal extension of K.
   (c) If L is a normal extension of F, then K is a normal extension of F.

MRQ 2019

School of Mathematics and Statistics

MT5836 Galois Theory

Problem Sheet IV: Separability; separable extensions; the Theorem of the Primitive Element

1. Show that $X^3 + 5$ 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

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

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

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.

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

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 α 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.

MRQ 2019

School of Mathematics and Statistics

MT5836 Galois Theory

Problem Sheet V: Finite Fields

1. (a) Find an irreducible polynomial of degree 3 over $\mathbb{F}_2$ and hence construct the addition and multiplication tables of the field $\mathbb{F}_8$ of order 8.

   (b) Find an irreducible polynomial of degree 2 over $\mathbb{F}_3$ and hence construct the addition and multiplication tables of the field $\mathbb{F}_9$ of order 9.

2. Let $F \subseteq K$ be an extension of finite fields.

   (a) Show that K is a normal extension of F.

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

3. Consider the Galois field $\mathbb{F}_{p^n}$ for order p^n where p is a prime number and n is a positive integer.

   (a) If F is a subfield of $\mathbb{F}_{p^n}$, show that $F \cong \mathbb{F}_{p^d}$ for some divisor d of n. [Hint: Recall $|\mathbb{F}_{p^n} : \mathbb{F}_p| = n$.]

   (b) Suppose that d is a divisor of n.

   (i) Set $k = n/d$, $r = \sum_{i=0}^{k-1} p^{id} = (p^n - 1)/(p^d - 1)$ and

   $$g(X) = \sum_{i=1}^{r} X^{p^n - i(p^d-1)-1}.$$

   Show that

   $$g(X)\,(X^{p^d} - X) = X^{p^n} - X.$$

   (ii) Show that $\mathbb{F}_{p^n}$ contains precisely p^d roots of $X^{p^d} - X$.

   (iii) Show that $L = \{\, a \in \mathbb{F}_{p^n} \mid a^{p^d} = a \,\}$ is a subfield of $\mathbb{F}_{p^n}$ of order p^d.

   (c) Conclude that $\mathbb{F}_{p^n}$ has a unique subfield of order p^d for each divisor d of n.

4. (a) Using information about the Galois field $\mathbb{F}_{16}$ of order 16, or otherwise, factorize $X^{15} - 1$ into a product of polynomials irreducible over $\mathbb{F}_2$.
   [Hint: What are the subfields of $\mathbb{F}_{16}$? If an element lies in a particular subfield, what is the degree of its minimum polynomial?]

   (b) Using information about the Galois field $\mathbb{F}_{27}$ of order 27, or otherwise, find the degrees of the irreducible factors of $X^{26} - 1$ over $\mathbb{F}_3$. Find the number of irreducible factors of each degree.

5. The following question provides an alternative solution to Question 8(a) on Problem Sheet I.

   (a) Show that 10 is a generator for the multiplicative group of the field $\mathbb{F}_{17}$ of order 17.

   (b) Let F be a finite field with prime subfield $\mathbb{F}_{17}$. If $x \in F$ is such that $x^4 = 10$, what is the order of x in the multiplicative group F^* of F?

   (c) Hence (and *not otherwise*!) show that $X^4 + 7$ is irreducible over $\mathbb{F}_{17}$.

6. A *primitive nth root of unity* in a finite field F is an element x of order n in the multiplicative group F^*. [The terminology indicates that x satisfies $x^n = 1$ and that its powers $1, x, x^2, \ldots, x^{n-1}$ are the n distinct roots of $X^n - 1$ in F.]

   Let q be a power of a prime.

   (a) Show that the Galois field $\mathbb{F}_q$ of order q contains a primitive nth root of unity if and only if $q \equiv 1 \pmod{n}$.

   (b) Suppose that n and q are coprime. Show that the splitting field of $X^n - 1$ over $\mathbb{F}_q$ is $\mathbb{F}_{q^m}$ where m is minimal subject to $q^m \equiv 1 \pmod{n}$.

   (c) For each value of n in the range $1 \leqslant n \leqslant 12$, determine the degree of the splitting field of $X^n - 1$ over $\mathbb{F}_5$.

   (d) Determine for which n in the range $1 \leqslant n \leqslant 12$ does the Galois field $\mathbb{F}_{5^{36}}$ of order 5^{36} contain a primitive nth root of unity?

7. Let F be a finite field with q elements where q is odd. Prove that the splitting field of $X^4 + 1$ over F has degree one or two and that $X^4 + 1$ factorizes in $F[X]$ either as a product of four distinct linear polynomials when 8 divides $q - 1$ or as a product of two distinct quadratic irreducible polynomials when 8 does not divide $q - 1$.

   [Hint: Consider the elements $-\alpha$, $1/\alpha$ and $-1/\alpha$ where α is a root of $X^4 + 1$ in some extension of F.]

8. Let G be a finite abelian group.

   (a) If x_1 and x_2 are elements of G with coprime orders, show that $x_1 x_2$ has order given by $o(x_1 x_2) = o(x_1)\, o(x_2)$.

   (b) Suppose $p_1, p_2, \ldots, p_k$ are distinct prime numbers and that $x_1, x_2, \ldots, x_k \in G$ with $o(x_i) = p_i^{\alpha_i}$. Show that

   $$o(x_1 x_2 \ldots x_k) = o(x_1)\, o(x_2) \ldots o(x_k) = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}.$$

9. Give an example of a finite group (necessarily non-abelian) which has no element of order equal to its exponent.

MRQ 2019

School of Mathematics and Statistics

MT5836 Galois Theory

Problem Sheet VI: Galois groups, the Galois correspondence and the Fundamental Theorem of Galois Theory

1. Let F be a field *not* of characteristic 2 and let K be an extension of F of degree 2. Show that K is a Galois extension of F.

2. Find an example of field extensions $F \subseteq K \subseteq L$ such that K is a Galois extension of F, L is a Galois extension of K, but L is not a Galois extension of F.

   [Hint: Consider $\sqrt[4]{2}$.]

3. Let n be a natural number and $F = \mathbb{Q}(\sqrt[n]{2})$. Show that $|F : \mathbb{Q}| = n$. Show that $\mathrm{Gal}(F/\mathbb{Q})$ is trivial or cyclic of order 2 according to whether n is odd or even.

4. Let $f(X) = X^4 + 5X^2 + 5$ over $\mathbb{Q}$.

   (a) Show that $f(X)$ is irreducible over $\mathbb{Q}$.
   (b) Find a splitting field K for $f(X)$ over $\mathbb{Q}$.
   (c) Find an element of order 4 in $\mathrm{Gal}(K/\mathbb{Q})$.
   (d) Describe the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ up to isomorphism.

5. Let $f(X) = X^8 - 1$ over $\mathbb{Q}$.

   (a) Factorize $f(X)$ into irreducible polynomials over $\mathbb{Q}$.
   (b) Find a splitting field K for $f(X)$ over $\mathbb{Q}$.
   (c) Determine the elements of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.
   (d) Describe the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ up to isomorphism.

6. Describe the Galois group $\mathrm{Gal}(\mathbb{Q}(i + \sqrt{3})/\mathbb{Q})$.

7. For each of the following field extensions, find the Galois group, find all of its subgroups, and find the subfield corresponding to each subgroup under the Galois correspondence. Determine which of the subfields are normal extensions of the base field.

   (a) The splitting field of $X^3 - 1$ over $\mathbb{Q}$.
   (b) The splitting field of $X^3 - 2$ over $\mathbb{Q}$.
   (c) The splitting field of $X^4 - 1$ over $\mathbb{Q}$.
   (d) The splitting field of $X^5 - 1$ over $\mathbb{Q}$.
   (e) The splitting field of $X^6 - 1$ over $\mathbb{Q}$.
   (f) The splitting field of $X^6 + X^3 + 1$ over $\mathbb{Q}$.
   (g) $\mathbb{Q}(\sqrt[3]{5}, i\sqrt{3})$ over $\mathbb{Q}$.
   (h) The splitting field of $X^4 - 2$ over $\mathbb{Q}(i)$.

8. Let $f(X) = X^5 - 5X^4 + 5$ over some finite field F. For each of the following groups G either find a finite field F such that the Galois group of $f(X)$ over F is isomorphic to G, or prove that no such field F exists.

   (a) The trivial group $\mathbf{1}$.

   (b) The Klein 4-group $V_4 \cong C_2 \times C_2$.

   (c) The cyclic group C_5 of order 5.

   (d) The cyclic group C_6 of order 6.

   (e) The cyclic group C_{10} of order 10.

   (f) The symmetric group S_5 of degree 5.

9. Let $f(X)$ be an irreducible polynomial over the finite field $\mathbb{F}_p$ (where p is a prime number). Show that if α is a root of $f(X)$ in some extension field, then $\mathbb{F}_p(\alpha)$ is a splitting field for $f(X)$ over $\mathbb{F}_p$.

   In each of the following cases, let α be a root of $f(X)$. Show that $f(X)$ is irreducible over $\mathbb{F}_p$ and express the roots of $f(X)$ as polynomials in α of degree less than the degree of $f(X)$ [that is, express the roots in terms of our standard basis for the usual extension $\mathbb{F}_p(\alpha)$ over $\mathbb{F}_p$]:

   (a) $f(X) = X^2 + 1, \ \ p = 7$;

   (b) $f(X) = X^3 + 2X^2 + X + 1, \ \ p = 3$.

MRQ 2019

School of Mathematics and Statistics

MT5836 Galois Theory

Problem Sheet VII: Radical extensions; solution of equations by radicals; soluble groups

1. Find a normal radical extension of $\mathbb{Q}$ that contains $\mathbb{Q}(\sqrt[3]{2})$.
2. Find three radical extensions of $\mathbb{Q}$ all containing $\mathbb{Q}(\sqrt{2})$ such that the Galois groups are distinct.
3. Let $f(X) = X^3 - 3X + 1$ and let K be the splitting field of $f(X)$ over $\mathbb{Q}$. Show that $|K : \mathbb{Q}| = 3$ and find a radical extension of $\mathbb{Q}$ containing K.

   Show that K is not itself a radical extension of $\mathbb{Q}$.
4. Show that $X^5 - 6X + 3$ is not soluble by radicals over $\mathbb{Q}$.
5. Let F be a field of characteristic zero. Show that a polynomial of the form $X^4 + bX^2 + c$ is soluble by radicals over F.
6. Let G be a soluble group with a chain of subgroups

   $$G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \ldots \geqslant G_d = \mathbf{1}$$

   where, for $i = 1, 2, \ldots, d$, G_i is a normal subgroup of G_{i-1} and G_{i-1}/G_i is abelian.

   (a) If H is a subgroup of G, show that $H \cap G_i$ is a normal subgroup of $H \cap G_{i-1}$ and that $(H \cap G_{i-1})/(H \cap G_i)$ is isomorphic to a subgroup of G_{i-1}/G_i for each i. [Hint: Second Isomorphism Theorem.]

   Deduce that subgroups of soluble groups are soluble.

   (b) If A, B and C are subgroups of G with $A \leqslant B$, show that $A(B \cap C) = AC \cap B$. [This result is known as the *Modular Law*.]

   (c) If N is a normal subgroup of G, show that G_iN/N is a normal subgroup of $G_{i-1}N/N$ and that $(G_{i-1}N/N)/(G_iN/N)$ is isomorphic to a quotient of G_{i-1}/G_i for each i. [Hint: Use the Second and Third Isomorphism Theorems and the Modular Law.]

   Deduce that quotients of soluble groups are soluble.
7. Let G be a group and N be a normal subgroup of G.

   (a) If G/N is soluble, show that there is a chain of subgroups

   $$G = G_0 \geqslant G_1 \geqslant \ldots \geqslant G_k = N$$

   such that G_i is a normal subgroup of G_{i-1} and G_{i-1}/G_i is abelian for $i = 1, 2, \ldots, k$. [Hint: Correspondence Theorem.]

   (b) Deduce that if G/N and N are soluble, then G is soluble.