MRQ 2017

School of Mathematics and Statistics

MT5836 Galois Theory

Problem Sheet I: Rings, fields, polynomials and irreducibility (Solutions)

1. **Write out the addition and multiplication tables for the field $\mathbb{F}_7$ of seven elements.**

Solution:

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

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.**

Solution:

(a) Let $L = \bigcap_{i\in I} K_i$. Since each K_i contain both 0 and 1, the same is true of the intersection L. If $a, b \in L$, then $a, b \in K_i$ for each i. Thus, as each K_i is a subfield,

$$a + b, -a, ab \in K_i \qquad \text{for all } i$$

and if $a \neq 0$ then

$$1/a \in K_i \qquad \text{for all } i.$$

Hence, upon taking the intersection, $a + b, -a, ab \in L$ and, if $a \neq 0$, $1/a \in L$. This shows that the intersection L is indeed a subfield.

(b) Let $\{ K_i \mid i \in I \}$ be the collection of all subfields of F. By part (a), $L = \bigcap_{i\in I} K_i$ is a subfield of F. However, the prime subfield P of F is the unique minimal subfield of F, contained in all other subfields, so $P \subseteq L$. On the other hand, some K_j equals P, so $L \subseteq K_j = P$ by definition. Hence $P = L$, the intersection of all the subfields of F.

3. **Show that every finite integral domain with $1 \neq 0$ is a field.**

Solution: Let R be a finite integral domain with $1 \neq 0$. We need to show every non-zero element of R has a multiplicative inverse. Let $a \in R,\ a \neq 0$. Consider the map $\phi\colon R \to R$ given by $x \mapsto ax$. If $x\phi = y\phi$, then $ax = ay$, so $a(x-y) = 0$. Since R is an integral domain and $a \neq 0$, we conclude $x - y = 0$; that is, $x = y$. Hence ϕ is injective. Now as R is finite, it follows, by the Pigeonhole Principle, that ϕ is also surjective. In particular, there exists some $x \in R$ with $x\phi = ax = 1$. This x is then a multiplicative inverse for a. Hence R is indeed 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.

Solution:

(a) Since R is a commutative ring and F is a subring, the following all hold (as they are special cases of the ring axioms):

- R is an abelian group under addition;
- multiplication determines a map $F \times R \to R$ given by $(a, x) \mapsto ax$;
- $a(x + y) = ax + ay$ for all $a \in F$ and $x, y \in R$;
- $(a + b)x = ax + bx$ for all $a, b \in F$ and $x \in R$;
- $(ab)x = a(bx)$ for all $a, b \in F$ and $x \in R$;
- $1x = x$ for all $x \in R$.

These conditions, together with the fact that F is a field (by assumption), say that R has the structure of a vector space over F.

(b) Since $F \subseteq R$, certainly R satisfies $1 \neq 0$. We must show that every non-zero element of R has a multiplicative inverse. Let $a \in R,\ a \neq 0$. Consider the map $\phi\colon R \to R$ given by $x \mapsto ax$. In our solution to Question 3 we showed that ϕ is injective. (The hypothesis of finiteness in that question is only used at a later stage of the question.) Note also that

$$(x + y)\phi = a(x + y) = ax + ay = x\phi + y\phi$$

and

$$(bx)\phi = a(bx) = b(ax) = b(x\phi)$$

for all $x, y \in R$ and $b \in F$. Thus ϕ is a linear map $R \to R$ when R is viewed as a vector space over F as in (a). Since ϕ is injective, the kernel $\ker \phi = \{0\}$. Now the Rank-Nullity Theorem states that

$$\dim \ker \phi + \dim \operatorname{im} \phi = \dim R.$$

Thus $\dim \operatorname{im} \phi = \dim R$ and, since R is finite-dimensional over F by assumption, we conclude $\operatorname{im} \phi = R$; that is, ϕ is surjective. Now (as in Question 3) we conclude there exists $x \in R$ with $x\phi = ax = 1$ and this x is a multiplicative inverse for a, as required.

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 $\mathbb{F}_p[X]$,

$$X^p - X = X(X - 1)(X - 2)\dots(X - (p - 1)).$$

Solution:

(a) The set of non-zero elements of $\mathbb{F}_p$ comprise the multiplicative group $\mathbb{F}_p^*$. This is a finite group of order $p-1$ and, by Lagrange's Theorem, the order of every element a in $\mathbb{F}_p^*$ divides $p-1$. Hence

$$a^{p-1} = 1 \qquad \text{for all } a \in \mathbb{F}_p,\ a \neq 0.$$

(b) Using part (a), $a^p = a^{p-1} \cdot a = a$ for all $a \in \mathbb{F}_p,\ a \neq 0$, while $0^p = 0$ is true by definition. Hence all of the elements $0, 1, \ldots, p-1$ of $\mathbb{F}_p$ are roots of the polynomial $X^p - X$. Thus $X - a$ is a divisor of $X^p - X$ for all $a \in \mathbb{F}_p$. Note

$$X(X-1)(X-2)\ldots(X-(p-1))$$

is a polynomial of degree p that is a product of distinct irreducible polynomials (the linear factors) each of which divides $X^p - X$. The uniqueness of factorization in $\mathbb{F}_p[X]$ then tells us

$$X^p - X = X(X-1)(X-2)\ldots(X-(p-1))$$

as both sides have degree p.

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.

Solution:

(a) By definition, every element of $R = \mathbb{F}_2[X]/I$ is a coset $I + g(X)$ for some $g(X) \in \mathbb{F}_2[X]$. Divide such a polynomial $g(X)$ by X^4+1 in the Euclidean domain $\mathbb{F}_2[X]$ to obtain an expression

$$g(X) = q(X) \cdot (X^4+1) + r(X)$$

where $r(X) = 0$ or $\deg r(X) < 4$. Note $q(X) \cdot (X^4+1) \in I$, by definition of $I = (X^4+1)$, so

$$I + g(X) = I + r(X).$$

Thus every element of R can be written as $I + r(X)$ where $r(X) \in \mathbb{F}_2[X]$ has degree at most three.

If $r(X), s(X)$ are polynomials of degree at most three and $I + r(X) = I + s(X)$, then

$$r(X) - s(X) \in I = (X^4+1);$$

that is,

$$r(X) - s(X) = q(X) \cdot (X^4+1)$$

for some polynomial $q(X) \in \mathbb{F}_2[X]$. If $q(X) \neq 0$, then the right-hand side has degree $4 + \deg q(X) \geqslant 4$, contrary to our assumption that $\deg r(X), \deg s(X) \leqslant 3$. Hence $q(X) = 0$ and we conclude $r(X) = s(X)$.

Thus, every element of $R = \mathbb{F}_2[X]/I$ is *uniquely* expressible in the form $I + r(X)$ where $r(X) = 0$ or $\deg r(X) \leqslant 3$, that is, uniquely expressible in the form

$$I + (aX^3 + bX^2 + cX + d)$$

with $a, b, c, d \in \mathbb{F}_2$.

(b) This follows from part (a). As there are two possible choices for each of a, b, c, d and each different set of choices determine distinct elements of R, we conclude

$$|R| = 2^4 = 16.$$

(c) Define $\iota\colon \mathbb{F}_2 \to R$ by

$$d \mapsto I + d.$$

If $d, e \in \mathbb{F}_2$,

$$(d+e)\iota = I + (d+e) = (I+d) + (I+e) = d\iota + e\iota$$

and

$$(de)\iota = I + de = (I+d)(I+e) = (d\iota)(e\iota).$$

Hence ι is a ring homomorphism. Note

$$0\iota = I + 0 \qquad \text{and} \qquad 1\iota = I + 1 \neq I + 0,$$

so $\ker \iota = \{0\}$ and ι is injective. Hence

$$\mathbb{F}_2 \cong \operatorname{im} \iota,$$

which is a subring of R.

(d) Identify $\mathbb{F}_2$ with the subring $\operatorname{im} \iota$ using the map ι. Thus R is a ring containing $\mathbb{F}_2$ as a subring. It therefore has the structure of a vector space over $\mathbb{F}_2$ by the same argument as used in Question 4(a). If $\{v_1, v_2, \ldots, v_n\}$ were a basis for R over $\mathbb{F}_2$, then every element of R would be uniquely expressible as

$$a_1 v_1 + a_2 v_2 + \cdots + a_n v_n,$$

where $a_1, a_2, \ldots, a_n \in \mathbb{F}_2$, and we would conclude $|R| = 2^n$. In view of our answer to part (b) we deduce

$$\dim_{\mathbb{F}_2} R = 4.$$

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) $X^3 + 2X^2 - 3X + 5$.

Solution: There are multiple alternative solutions to some of the following. For example, we covered different solutions to (c) in the tutorials. The following are some examples of valid solutions.

(a) $X^n - p$ (p prime) satisfies the conditions of Eisenstein's Criterion (with respect to the given prime p) and so is irreducible over $\mathbb{Q}$.

(b) $X^6 + 168X^2 - 147X + 63$ satisfies the conditions of Eisenstein's Criterion with $p = 7$ (as 7 divides 63, 147 and 168 but 7^2 does not divide 63). Hence this polynomial is irreducible over $\mathbb{Q}$.

(c) Substitute $X = Y + 1$. The polynomial becomes

$$(Y+1)^3 - 3(Y+1) - 1 = Y^3 + 3Y^2 - 3.$$

This latter polynomial in the indeterminate Y is irreducible as it satisfies Eisenstein's Criterion with $p = 3$. It follows that the original polynomial is irreducible since if it were a product of two polynomials in X of smaller degree then, upon substituting $X = Y + 1$, we would obtain a factorization of $Y^3 + 3Y^2 - 3$.

(d) Suppose $f(X) = X^3 + 2X^2 - 3X + 5$ is reducible over $\mathbb{Q}$, then, by Gauss's Lemma, it would be factorizable as a product of two polynomials of smaller degree with integer coefficients. The ring homomorphism $\phi\colon \mathbb{Z} \to \mathbb{F}_2$ determined by reducing an integer modulo 2 induces a ring homomorphism $\bar{\phi}\colon \mathbb{Z}[X] \to \mathbb{F}_2[X]$ by reducing the coefficients of each polynomial modulo 2. Applying $\bar{\phi}$ to the factorization of $f(X)$, we conclude that

$$\bar{f}(X) = (X^3 + 2X^2 - 3X + 5)\bar{\phi} = X^3 + X + 1$$

is reducible over $\mathbb{F}_2$. However, $\bar{f}(X)$ would necessarily have a linear factor, but

$$\bar{f}(0) = \bar{f}(1) = 1,$$

so this is not the case. Hence $X^3 + 2X^2 - 3X + 5$ is irreducible over $\mathbb{Q}$.

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

(a) $\boldsymbol{X^4 + 7}$ **over** $\boldsymbol{\mathbb{F}_{17}}$**;**
(b) $\boldsymbol{X^3 - 5}$ **over** $\boldsymbol{\mathbb{F}_{11}}$**.**

Solution:

(a) Let $f(X) = X^4 + 7 \in \mathbb{F}_{17}[X]$. Since $\alpha^4 = (-\alpha)^4$ for all $\alpha \in \mathbb{F}_{17}$, we first calculate:

$$\begin{aligned} f(0) &= 7, \\ f(1) = f(16) &= 1^4 + 7 = 8, & f(2) = f(15) &= 2^4 + 7 = 6, \\ f(3) = f(14) &= 3^4 + 7 = 3, & f(4) = f(13) &= 4^4 + 7 = 8, \\ f(5) = f(12) &= 5^4 + 7 = 3, & f(6) = f(11) &= 6^4 + 7 = 11, \\ f(7) = f(1) &= 7^4 + 7 = 11, & f(8) = f(9) &= 8^4 + 7 = 6. \end{aligned}$$

Thus $f(\alpha) \neq 0$ for all $\alpha \in \mathbb{F}_{17}$ and hence $f(X)$ has no linear factors in $\mathbb{F}_{17}[X]$.
Suppose that $f(X)$ is reducible over $\mathbb{F}_{17}$. Then it would necessarily factorize as a product of two quadratic factors. Since $f(X)$ is monic, we reduce to a factorization of the form

$$X^4 + 7 = (X^2 + \alpha X + \beta)(X^2 + \gamma X + \delta)$$

for some $\alpha, \beta, \gamma, \delta \in \mathbb{F}_{17}$. Equating coefficients yields the following four equations:

$$\begin{aligned} \alpha + \gamma &= 0 & \alpha\gamma + \beta + \delta &= 0 \\ \alpha\delta + \beta\gamma &= 0 & \beta\delta &= 7 \end{aligned}$$

This first equation (X^3 coefficient) yields $\gamma = -\alpha$ which, when subtituted into the third equation (X coefficient), gives

$$\alpha(\delta - \beta) = 0.$$

Hence either $\alpha = \gamma = 0$ or $\beta = \delta$. We split into these cases.

Case 1: $\alpha = \gamma = 0$.
The second equation (X^2 coefficient) then tells us $\delta = -\beta$ and the fourth equation (constant term) gives $-\beta^2 = 7$; that is, $\beta^2 = 10$. To show this is impossible we calculate all squares in $\mathbb{F}_{17}$:

$$\begin{aligned} 0^2 &= 0, \\ 1^2 = 16^2 &= 1, & 2^2 = 15^2 &= 4, \\ 3^2 = 14^2 &= 9, & 4^2 = 13^2 &= 16, \\ 5^2 = 12^2 &= 8, & 6^2 = 11^2 &= 2, \\ 7^2 = 10^2 &= 15, & 8^2 = 9^2 &= 13. \end{aligned}$$

Hence there is no β in $\mathbb{F}_{17}$ satisfying $\beta^2 = 10$, giving our required contradiction.

Case 2: $\beta = \delta$.
The fourth equation (constant term) then becomes $\beta^2 = 7$, which is impossible by our calculation of squares in Case 1.

In conclusion, $f(X)$ is not factorizable as a product of quadratic polynomials, so is irreducible over $\mathbb{F}_{17}$.

(b) Observe $3^3 = 5$ in $\mathbb{F}_{11}$, so $X^3 - 5$ has a root in $\mathbb{F}_{11}$ and hence factorizes as a product of a linear factor and a quadratic polynomial over $\mathbb{F}_{11}$. Hence $X^3 - 5$ is reducible over $\mathbb{F}_{11}$.

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

Solution: If $f(X)$ is a polynomial over $\mathbb{F}_2$, then $f(0)$ equals the constant term and $f(1)$ is congruent to the number of terms in the polynomial modulo 2. Hence if $f(X)$ is irreducible over $\mathbb{F}_2$ and $\deg f(X) \geqslant 2$ then $f(X)$ must have constant term 1 and an odd number of terms (so as to avoid having any linear factors).

First note that the two linear polynomials over $\mathbb{F}_2$ are necessarily irreducible:

$$X \qquad \text{and} \qquad X + 1.$$

By the first paragraph of the solution, the only irreducible polynomial of degree 2 (that is, with no linear factors) is

$$X^2 + X + 1.$$

Similarly any reducible cubic has a linear factor, so the irreducible polynomials over $\mathbb{F}_2$ are those produced by the method of the first paragraph:

$$X^3 + X + 1 \qquad \text{and} \qquad X^3 + X^2 + 1.$$

A reducible quartic polynomial over $\mathbb{F}_2$ either has a linear factor (and is as described in the first paragraph of the solution) or is a product of two irreducible quadratic polynomials. By above, the latter is necessarily

$$(X^2 + X + 1)^2 = X^4 + X^2 + 1.$$

Excluding all such polynomials, we conclude that the irreducible polynomials of degree 4 over $\mathbb{F}_2$ are

$$X^4 + X + 1, \qquad X^4 + X^3 + 1 \qquad \text{and} \qquad X^4 + X^3 + X^2 + X + 1.$$

10. **Find a reducible polynomial of degree 4 over the field $\mathbb{F}_2$ of two elements that has no roots in $\mathbb{F}_2$.**

Solution: We observed in Question 9 that

$$X^4 + X^2 + 1 = (X^2 + X + 1)^2$$

is reducible, but is a product of two irreducible quadratic polynomials, so has no linear factors and hence no root in $\mathbb{F}_2$.