School of Mathematics and Statistics

MT5836 Galois Theory

Handout I: Rings, Fields and Polynomials

1 Rings, Fields and Polynomials

The first section of the module contains a review of the background material on rings, fields, polynomials, polynomial rings and the irreducibility of polynomials. The majority comes from the module *MT3505 Rings and Fields*.

Rings

Definition 1.1 A *commutative ring with a* 1 is a set R endowed with two binary operations denoted as addition and multiplication such that the following conditions hold:

(i) R forms an abelian group with respect to addition (with additive identity 0, called *zero*);

(ii) multiplication is *associative*: $a(bc) = (ab)c$ for all $a, b, c \in R$;

(iii) multiplication is *commutative*: $ab = ba$ for all $a, b \in R$;

(iv) the *distributive laws* hold:

$$\begin{aligned} a(b + c) &= ab + ac \\ (a + b)c &= ac + bc \end{aligned}$$

for all $a, b, c \in R$;

(v) there is a *multiplicative identity* 1 in R satisfying $a1 = 1a = a$ for all $a \in R$.

Definition 1.2 Let R be a commutative ring with a 1. An *ideal* I in R is a non-empty subset of R that is both an additive subgroup of R and satisfies the property that if $a \in I$ and $r \in R$, then $ar \in I$.

Thus a subset I of R is an ideal if it satisfies the following four conditions:

(i) I is non-empty (or $0 \in I$);

(ii) $a + b \in I$ for all $a, b \in I$;

(iii) $-a \in I$ for all $a \in I$;

(iv) $ar \in I$ for all $a \in I$ and $r \in R$.

Let R be a commutative ring and let I be an ideal of R. Then I is, in particular, a subgroup of the additive group of R and the latter is an abelian group. We can therefore form the additive cosets of I; that is, define

$$I + r = \{ a + r \mid a \in I \}$$

for each $r \in R$. We know from group theory when two such cosets are equal,

$$I + r = I + s \qquad \text{if and only if} \qquad r - s \in I,$$

and that the set of all cosets forms a group via addition of the representatives:

$$(I + r) + (I + s) = I + (r + s) \qquad \text{for } r, s \in R.$$

The assumption that I is an ideal then ensures that there is a well-defined multiplication on the set of cosets, given by

$$(I + r)(I + s) = I + rs \qquad \text{for } r, s \in R,$$

with respect to which the set of cosets $I + r$ forms a ring, called the *quotient ring* and denoted by R/I.

Theorem 1.3 *Let R be a commutative ring with a 1 and I be an ideal of R. Then the quotient ring R/I is a commutative ring with a 1.*

Definition 1.4 Let R and S be commutative rings with 1. A *homomorphism* $\phi\colon R \to S$ is a map such that

(i) $(a + b)\phi = a\phi + b\phi$

(ii) $(ab)\phi = (a\phi)(b\phi)$

for all $a, b \in R$.

Definition 1.5 Let R and S be commutative rings with 1 and $\phi\colon R \to S$ be a homomorphism.

(i) The *kernel* of ϕ is
$$\ker\phi = \{ a \in R \mid a\phi = 0 \}.$$

(ii) The *image* of ϕ is
$$\operatorname{im}\phi = R\phi = \{ a\phi \mid a \in R \}.$$

Theorem 1.6 (First Isomorphism Theorem) *Let R and S be commutative rings with 1 and $\phi\colon R \to S$ be a homomorphism. Then the kernel of ϕ is an ideal of R, the image of ϕ is a subring of S and*

$$R/\ker\phi \cong \operatorname{im}\phi.$$

Definition 1.7 Let R be a commutative ring with a 1.

(i) A *zero divisor* in R is a non-zero element a such that $ab = 0$ for some non-zero $b \in R$.

(ii) An *integral domain* is a commutative ring with a 1 containing no zero divisors.

Fields

Definition 1.8 A *field* F is a commutative ring with a 1 such that $0 \neq 1$ and every non-zero element is a *unit*, that is, has a multiplicative inverse.

Proposition 1.10 (i) *Every field is an integral domain.*

(ii) *The set of non-zero elements in a field forms an abelian group under multiplication.*

We write F^* for the multiplicative group of non-zero elements in a field.

If F is any field, with multiplicative identity denoted by 1, and n is a positive integer, let us define

$$\overline{n} = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}.$$

By the distributive law,

$$\overline{mn} = \overline{m}\,\overline{n}$$

for all positive integers m and n. Since F is, in particular, an integral domain, it follows that if there exists a positive integer n such that $\overline{n} = 0$ then necessarily the smallest such positive integer n is a prime number.

Definition 1.11 Let F be a field with multiplicative identity 1.

(i) If it exists, the smallest positive integer p such that $\overline{p} = 0$ is called the *characteristic* of F.

(ii) If no such positive integer exists, we say that F has *characteristic zero*.

Our observation is therefore that every field F either has characteristic zero or has characteristic p for some prime number p.

We shall say that K is a *subfield* of F when $K \subseteq F$ and that K forms a field itself under the addition and multiplication induced from F; that is, when the following conditions hold:

(i) K is non-empty and contains non-zero elements (or, equivalently when taken with the other two conditions, $0, 1 \in K$);

(ii) $a + b, -a, ab \in K$ for all $a, b \in K$;

(iii) $1/a \in K$ for all non-zero $a \in K$.

Theorem 1.12 *Let F be a field.*

(i) *If F has characteristic zero, then F has a unique subfield isomorphic to the rationals $\mathbb{Q}$ and this is contained in every subfield of F.*

(ii) *If F has characteristic p (prime), then F has a unique subfield isomorphic to the field $\mathbb{F}_p$ of integers modulo p and this is contained in every subfield of F.*

Definition 1.13 This unique minimal subfield in F is called the *prime subfield* of F.

Polynomials

Definition 1.14 Let F be a field. A *polynomial* over F in the indeterminate X is an expression of the form

$$f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

where n is a non-negative integer and the coefficients a_0, a_1, …, a_n are elements of F.

We shall write $F[X]$ for the set of all polynomials in the indeterminate X with coefficients taken from the field F.

Proposition 1.15 *If F is a field, the polynomial ring $F[X]$ is a* Euclidean domain.

The Euclidean function associated to $F[X]$ is the degree of a polynomial. If $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ is a *non-zero* polynomial with leading term having non-zero coefficient, that is, $a_n \neq 0$, the *degree* of $f(X)$ is

$$\deg f(X) = n.$$

The properties of the degree are:

(i) if $f(X)$ and $g(X)$ are non-zero, then $\deg f(X)g(X) = \deg f(X) + \deg g(X)$;

(ii) if $f(X)$ and $g(X)$ are polynomials with $f(X) \neq 0$, then there exist unique polynomials $q(X)$ and $r(X)$ satisfying

$$g(X) = q(X)\, f(X) + r(X) \qquad \text{with either } r(X) = 0 \text{ or } \deg r(X) < \deg f(X).$$

Proposition 1.16 *If F is a field, the polynomial ring $F[X]$ is a principal ideal domain; that is, every ideal I in $F[X]$ has the form $I = (f(X)) = \{\, f(X)g(X) \mid g(X) \in F[X] \,\}$ for some polynomial $f(X)$.*

Definition 1.17 Suppose $f(X)$ and $g(X)$ are polynomials over the field F. A *greatest common divisor* of $f(X)$ and $g(X)$ is a polynomial $h(X)$ of greatest degree such that $h(X)$ divides both $f(X)$ and $g(X)$.

To say that $h(X)$ *divides* $f(X)$ means that $f(X)$ is a multiple of $h(X)$; that is, $f(X) = h(X)\, q(X)$ for some $q(X) \in F[X]$. In a general Euclidean domain, the greatest common divisor is defined uniquely up to multiplication by a unit. In the polynomial ring $F[X]$, the units are constant polynomials (that is, elements of the base field F viewed as elements of $F[X]$). As a consequence, the greatest common divisor of a pair of polynomials is defined uniquely up to multiplication by a scalar from the field F.

Theorem 1.18 *Let F be a field and $f(X)$ and $g(X)$ be two non-zero polynomials over F. Then there exist $u(X), v(X) \in F[X]$ such that the greatest common divisor of $f(X)$ and $g(X)$ is given by*

$$h(X) = u(X)\, f(X) + v(x)\, g(X).$$

Definition 1.19 Let $f(X)$ be a polynomial over a field F of degree at least 1. We say that $f(X)$ is *irreducible* over F if it cannot be factorized as $f(X) = g_1(X)\,g_2(X)$ where $g_1(X)$ and $g_2(X)$ are polynomials in $F[X]$ of degree smaller than $f(X)$.

The term *reducible* is used for a polynomial that is not irreducible; that is, that can be factorized as a product of two polynomials of smaller degree.

Theorem 1.22 (Gauss's Lemma) *Let $f(X)$ be a polynomial with integer coefficients. Then $f(X)$ is irreducible over $\mathbb{Z}$ if and only if it is irreducible over $\mathbb{Q}$.*

Theorem 1.23 (Eisenstein's Irreducibility Criterion) *Let*

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n$$

be a polynomial over $\mathbb{Z}$. Suppose there exists a prime number p such that

(i) *p does not divide a_n;*

(ii) *p divides a_0, a_1, ..., a_{n-1};*

(iii) *p^2 does not divide a_0.*

Then $f(X)$ is irreducible over $\mathbb{Q}$.

Every integral domain has a field of fractions. To be precise, if R is an integral domain, the field of fractions of R is the set of all expressions of the form r/s where (i) $r, s \in R$ with $s \neq 0$, and (ii) we define $r_1/s_1 = r_2/s_2$ if and only if $r_1 s_2 = r_2 s_1$. We define

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \qquad \text{and} \qquad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$$

for such fractions r_1/s_1 and r_2/s_2. With respect to these operations, the set of all fractions r/s forms a field. Finally R embeds in the field of fractions via the map $r \mapsto r/1$; that is, the set $\{\, r/1 \mid r \in R \,\}$ is a subring isomorphic to the original integral domain R.

We apply this construction in the case when $R = F[X]$, the integral domain of polynomials with coefficients from the field F:

Definition 1.24 Let F be a field. The *field of rational functions* with coefficients in F is denoted by $F(X)$ and is the field of fractions of the polynomial ring $F[X]$.

The elements of $F(X)$ are expressions of the form

$$\frac{f(X)}{g(X)}$$

where $f(X)$ and $g(X)$ are polynomials with coefficients from F.

Proposition 1.25 *The field F occurs as a subfield of the field $F(X)$ of rational functions with coefficients in F.*