Fields and Galois Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

Euclidean Domains

Euclidean Domains

- An integral domain D is called a **Euclidean domain** if there is a mapping δ from D into the set $\mathbb{N}^0$ of non-negative integers with the properties:
  - $\delta(0)=0$;
  - For all a in D and all b in $D\backslash\{0\}$, there exist q,r in D, such that
$$a=qb+r, \qquad \delta(r)<\delta(b).$$
- It follows that $\delta^{-1}\{0\}=\{0\}$.

  Suppose for some $b\neq 0$, $\delta(b)=0$.

  Then it would not be possible to find r, such that $\delta(r)<\delta(b)$.

Example: The Integers

- The most important example of a Euclidean domain is the ring $\mathbb{Z}$.
- $\delta(a)$ is defined as $|a|$.
- The process, known as the **division algorithm**, is the familiar one of dividing a by b and obtaining a **quotient** q and a **remainder** r.
  - If b is positive, then there exists q, such that
$$qb \leq a < (q+1)b.$$
Thus $0 \leq a - qb < b$. Taking $r = a - qb$, we see that $a = qb + r$ and $|r| < |b|$.
  - If b is negative, then there exists q, such that
$$(q+1)b < a \leq qb.$$
Thus, $b < r = a - qb \leq 0$. It follows again that $a = qb + r$ and $|r| < |b|$.

Principal Ideal Domains

- An integral domain D is called a **principal ideal domain** if all of its ideals are principal.

Theorem

Every Euclidean domain is a principal ideal domain.

- Let D be a Euclidean domain. The ideal $\{0\}$ is certainly principal. Let I be a non-zero ideal. Let b be a non-zero element of I, such that

$$\delta(b) = \min\{\delta(x) : x \in I \backslash \{0\}\}.$$

Let $a \in I$. There exist q, r, such that $a = qb + r$ and $\delta(r) < \delta(b)$. But $r = a - qb \in I$. By the minimality of $\delta(b)$, $r = 0$. Thus, $a = qb$.

So $I = Db = \langle b \rangle$ is a principal ideal.

Greatest Common Divisors

- Let a, b be non-zero members of a principal ideal domain D.
- Let $\langle a, b\rangle = \{sa + tb : s, t \in D\}$ be the ideal generated by a and b.
- Since D is a principal ideal domain, there exists d in D, such that $\langle a, b\rangle = \langle d\rangle$.
  - Since $\langle a\rangle \subseteq \langle d\rangle$ and $\langle b\rangle \subseteq \langle d\rangle$, we have $d \mid a$ and $d \mid b$.
  - Since $d \in \langle a, b\rangle$, there exist s, t in D, such that $d = sa + tb$.
    If $d' \mid a$ and $d' \mid b$, then $d' \mid sa + tb$, i.e., $d' \mid d$.
- We say that d is a **greatest common divisor**, or a **highest common factor**, of a and b.
- If $\langle a, b\rangle = \langle d\rangle = \langle d^*\rangle$, then that $d^* \sim d$.

Greatest Common Divisors (Cont'd)

- Let a, b be non-zero members of a principal ideal domain D.
- Summarizing, d is the greatest common divisor of a and b, written

$$d = \gcd(a, b),$$

if it has the following properties:

(GCD1) $d \mid a$ and $d \mid b$;
(GCD2) if $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

- If $\gcd(a, b) \sim 1$, we call a and b **coprime**, or **relatively prime**.

Examples of Greatest Common Divisor

- In the case of the domain $\mathbb{Z}$, where the group of units is $\{1, -1\}$, we have, e.g., that
$$\langle 12, 18 \rangle = \langle 6 \rangle = \langle -6 \rangle.$$
- A simple modification of the argument enables us to conclude that, in a principal ideal domain D, every finite set $\{a_1, a_2, \ldots, a_n\}$ has a greatest common divisor.

The Euclidean Algorithm (Dividing)

- Let a and b be non-zero elements of a Euclidean domain D.
- Suppose, without loss of generality, that $\delta(b) \leq \delta(a)$.
- Then there exist $q_1, q_2, \ldots$ and $r_1, r_2, \ldots$, such that:

$$\begin{aligned} a &= q_1 b + r_1, & \delta(r_1) &< \delta(b), \\ b &= q_2 r_1 + r_2, & \delta(r_2) &< \delta(r_1), \\ r_1 &= q_3 r_2 + r_3, & \delta(r_3) &< \delta(r_2), \\ r_2 &= q_4 r_3 + r_4, & \delta(r_4) &< \delta(r_3), \\ &\vdots \end{aligned}$$

- The process must end with some $r_k = 0$.
  The final equations are:

$$\begin{aligned} r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1}, \quad \delta(r_{k-1}) < \delta(r_{k-2}), \\ r_{k-2} &= q_k r_{k-1}. \end{aligned}$$

The Euclidean Algorithm (Finding the GCD)

- From $a = q_1 b + r_1$, we deduce that $\langle a, b\rangle = \langle b, r_1\rangle$.
  - Every element $sa + tb$ in $\langle a, b\rangle$ can be rewritten as

    $$sa + tb = s(q_1 b + r_1) + tb = (t + sq_1)b + sr_1 \in \langle b, r_1\rangle.$$

    Every element $xb + yr_1$ in $\langle b, r_1\rangle$ can be rewritten as

    $$xb + yr_1 = xb + y(a - q_1 b) = ya + (x - yq_1)b \in \langle a, b\rangle.$$

- Similarly, the subsequent equations give

$$\langle b, r_1\rangle = \langle r_1, r_2\rangle, \langle r_1, r_2\rangle = \langle r_2, r_3\rangle, \ldots,$$
$$\langle r_{k-3}, r_{k-2}\rangle = \langle r_{k-2}, r_{k-1}\rangle, \langle r_{k-2}, r_{k-1}\rangle = \langle r_{k-1}\rangle.$$

- We conclude that $\langle a, b\rangle = \langle r_{k-1}\rangle$.
- So r_{k-1} is the (essentially unique) greatest common divisor of a and b.

Example

- We determine the greatest common divisor of 615 and 345, and express it in the form $615x + 345y$.

$$\begin{aligned} 615 &= 1 \times 345 + 270 \\ 345 &= 1 \times 270 + 75 \\ 270 &= 3 \times 75 + 45 \\ 75 &= 1 \times 45 + 30 \\ 45 &= 1 \times 30 + 15 \\ 30 &= 2 \times 15 + 0. \end{aligned}$$

The greatest common divisor is 15, the last non-zero remainder. Moreover,

$$\begin{aligned} 15 &= 45 - 30 = 45 - (75 - 45) = 2 \times 45 - 75 \\ &= 2 \times (270 - 3 \times 75) - 75 = 2 \times 270 - 7 \times 75 \\ &= 2 \times 270 - 7 \times (345 - 270) = 9 \times 270 - 7 \times 345 \\ &= 9 \times (615 - 345) - 7 \times 345 = 9 \times 615 - 16 \times 345. \end{aligned}$$

Example of Coprime Elements

- Two elements a and b of a principal ideal domain D are coprime if their greatest common divisor is 1.
- This happens if and only if there exist s and t in D, such that $sa+tb=1$.
- For example, 75 and 64 are coprime:

$$\begin{array}{rcl} 75 & = & 1\times 64+11 \\ 64 & = & 5\times 11+9 \\ 11 & = & 1\times 9+2 \\ 9 & = & 4\times 2+1 \\ 2 & = & 2\times 1+0. \end{array}$$

Therefore,

$$\begin{array}{rcl} 1 & = & 9-4\times 2=9-4(11-9)=5\times 9-4\times 11 \\ & = & 5(64-5\times 11)-4\times 11=5\times 64-29\times 11 \\ & = & 5\times 64-29(75-64)=34\times 64-29\times 75. \end{array}$$

Subsection 2

Unique Factorization

Irreducibles in Principal Ideal Domains

- Let D be an integral domain with group U of units, and let $p \in D$ be such that $p \neq 0, p \notin U$.

  Then p is said to be **irreducible** if it has no proper factors.

Theorem

Let p be an element of a principal ideal domain D. Then the following statements are equivalent:

(i) p is irreducible;

(ii) $\langle p \rangle$ is a maximal proper ideal of D;

(iii) $D/\langle p \rangle$ is a field.

(i)⇒(ii): Suppose that p is irreducible. Then p is not a unit, and so $\langle p \rangle$ is a proper ideal of D. Suppose, for a contradiction, that there is a (principal) ideal $\langle q \rangle$, such that $\langle p \rangle \subset \langle q \rangle \subset D$. Then $p \in \langle q \rangle$. So $p = aq$, for some non-unit a. This contradicts the irreducibility of p.

Irreducibles in Principal Ideal Domains (Cont'd)

(ii)⇒(iii): Let $a+\langle p\rangle$ be a non-zero element of $D/\langle p\rangle$. Then $a\notin\langle p\rangle$. So the ideal $\langle a\rangle+\langle p\rangle$ properly contains $\langle p\rangle$. Since $\langle p\rangle$ is maximal, $\langle a\rangle+\langle p\rangle=\{sa+tp:s,t\in D\}=D$. Hence, there exist s,t in D such that $sa+tp=1$. Therefore, $sa-1=tp\in\langle p\rangle$. That is,

$$(s+\langle p\rangle)(a+\langle p\rangle)=1+\langle p\rangle.$$

Thus, $D/\langle p\rangle$ is a field.

(iii)⇒(i): If p is not irreducible, then there exist non-units q and r, such that $p=qr$. Then $q+\langle p\rangle$ and $r+\langle p\rangle$ are both non-zero elements of $D/\langle p\rangle$. On the other hand,

$$(q+\langle p\rangle)(r+\langle p\rangle)=p+\langle p\rangle=0+\langle p\rangle.$$

Thus, $D/\langle p\rangle$ has divisors of zero. So it is not a field.

Unique Factorization Domains

- An element d of an integral domain D has a **factorization into irreducible elements** if there exist irreducible elements $p_1, p_2, \ldots, p_k$, such that
$$d = p_1 p_2 \cdots p_k.$$
- The factorization is **essentially unique** if, for irreducible elements $p_1, p_2, \ldots, p_k$ and $q_1, q_2, \ldots, q_\ell$,
$$d = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$$
implies that $k = \ell$ and, for some permutation $\sigma : \{1, 2, \ldots, k\} \to \{1, 2, \ldots, k\}$,
$$p_i \sim q_{\sigma(i)}, \qquad i = 1, 2, \ldots, k.$$
- An integral domain D is said to be a **factorial domain**, or a **unique factorization domain**, if every non-unit $a \neq 0$ of D has an essentially unique factorization into irreducible elements.

Example of a Unique Factorization Domain

- $\mathbb{Z}$, in which the (positive and negative) prime numbers are the irreducible elements, provides a familiar example of a unique factorization domain.
- For example
$$60 = 2 \cdot 2 \cdot 3 \cdot 5.$$
The factorization is essentially unique, for nothing more different than (say) $(-2) \cdot (-5) \cdot 3 \cdot 2$ is possible.

Chains of Ideals in Principal Ideal Domains

Lemma

In a principal ideal domain there are no infinite ascending chains of ideals.

- In any integral domain D, an ascending chain $I_1 \subseteq I_2 \subseteq_3 \subseteq \cdots$ of ideals has the property that $I = \bigcup_{j \geq 1} I_j$ is an ideal.
  - Let $a, b \in I$. There exist k, ℓ, such that $a \in I_k, b \in I_\ell$. So $a - b \in I_{\max\{k,\ell\}} \subseteq I$.
  - Let $a \in I$ and $s \in D$. Then $a \in I_k$, for some k. So $sa \in I_k \subseteq I$.

Let D be a principal ideal domain, and $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \cdots$ be an ascending chain of (principal) ideals. We know that the union of all the ideals in this chain must be an ideal. By our assumption, this must be a principal ideal $\langle a \rangle$. Since $a \in \bigcup_{j \geq 1} \langle a_j \rangle$, $a \in \langle a_k \rangle$, for some k. Thus, $\langle a \rangle \subseteq \langle a_k \rangle$. But we also have $\langle a_k \rangle \subseteq \langle a \rangle$. Hence, $\langle a \rangle = \langle a_k \rangle$. So $\langle a_k \rangle = \langle a_{k+1} \rangle = \langle a_{k+2} \rangle = \cdots = \langle a \rangle$. Thus, the infinite chain of inclusions terminates at $\langle a_k \rangle$.

Irreducible Elements and Divisilbility

Lemma

Let D be a principal ideal domain, let p be an irreducible element in D, and let $a, b \in D$. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

- Suppose that $p \mid ab$ and $p \nmid a$. Then the greatest common divisor of a and p must be 1. So there exist s, t in D, such that $sa + tp = 1$. Hence, $sab + tpb = b$. But p clearly divides $sab + tpb$. Therefore, $p \mid b$.
- It is a routine matter to extend this result to products of more than two elements.

Corollary

Let D be a principal ideal domain, let p be an irreducible element in D, and let $a_1, a_2, \ldots, a_m \in D$. If $p \mid a_1 a_2 \cdots a_m$, then $p \mid a_1$ or $p \mid a_2$ or $\cdots$ or $p \mid a_m$.

Factoriality of Principal Ideal Domains

Theorem

Every principal ideal domain is factorial.

- We show, first, that any $a \neq 0$ in D can be expressed as a product of irreducible elements. Let a be a non-unit in D. Then either a is irreducible, or it has a proper divisor a_1. Similarly, either a_1 is irreducible, or a_1 has a proper divisor a_2. Continuing, we obtain a sequence $a = a_0, a_1, a_2, \ldots$ in which, for $i = 1, 2, \ldots$, a_i is a proper divisor of a_{i-1}. The sequence must terminate at some a_k; Otherwise the infinite ascending sequence $\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots$ would contradict the lemma.

  Hence a has a proper irreducible divisor $a_k = z_1$, and $a = z_1 b_1$.

Factoriality of Principal Ideal Domains (Cont'd)

- We found a proper irreducible divisor $a_k = z_1$ of a, yielding the expression $a = z_1 b_1$.

  If b_1 is irreducible, then the proof is complete.

  Otherwise we can repeat the argument we used for a to find a proper irreducible divisor z_2 of b_1, and $a = z_1 z_2 b_2$.

  We continue this process.

  It too must terminate; Otherwise the infinite ascending sequence $\langle a \rangle \subset \langle b_1 \rangle \subset \langle b_2 \rangle \subset \cdots$ would again contradict the lemma.

  Hence, some b_ℓ must be irreducible.

  So $a = z_1 z_2 \cdots z_{\ell-1} b_\ell$ is a product of irreducible elements.

Uniqueness of the Factorization

- Suppose that $p_1p_2\cdots p_k \sim q_1q_2\cdots q_\ell$, where $p_1,p_2,\ldots,p_k$ and $q_1,q_2,\ldots,q_\ell$ are irreducible.
  - Suppose first that $k=1$. Since $q_1q_2\cdots q_\ell$ is irreducible, $\ell=1$. So $p_1 \sim q_1$.
  - Suppose inductively that, for all $n \geq 2$ and all $k<n$, any statement of the form $p_1p_2\cdots p_k \sim q_1q_2\cdots q_\ell$ implies that $k=\ell$ and that, for some permutation σ of $\{1,2,\ldots,k\}$, $q_i \sim p_{\sigma(i)}$, $i=1,2,\ldots,k$.
  - Let $k=n$. Since $p_1 \mid q_1q_2\cdots q_\ell$, by the corollary $p_1 \mid q_j$, for some j in $\{1,2,\ldots,\ell\}$. Since q_j is irreducible and p_1 is not a unit, $p_1 \sim q_j$. By cancelation, $p_2p_3\cdots p_n \sim q_1\cdots q_{j-1}q_{j+1}\cdots q_\ell$. By the induction hypothesis, $n-1=\ell-1$ and, for $i \in \{1,2,\ldots,n\}\backslash\{j\}$, $q_i \sim p_{\sigma(i)}$, for some permutation σ of $\{2,3,\ldots,n\}$. Hence, extending σ to a permutation σ of $\{1,2,\ldots,n\}$ by defining $\sigma(1)=j$, we obtain the desired result.

Corollary

Every Euclidean domain is factorial.

Subsection 3

Polynomials

Polynomials

- In the following, R is an integral domain and K is a field.
- A **polynomial f with coefficients in R** is a sequence $(a_0, a_1, \ldots)$, where $a_i \in R$, for all $i \geq 0$, and where only finitely many of $\{a_0, a_1, \ldots\}$ are non-zero.
- If the last non-zero element in the sequence is a_n, we say that f has **degree** n, and write $\partial f = n$.
- The entry a_n is called the **leading coefficient** of f.
- If $a_n = 1$ we say that the polynomial is **monic**.

More on Polynomials

- In the case where all of the coefficients are 0, it is convenient to ascribe the formal degree of $-\infty$ to the polynomial $(0,0,0,\ldots)$.
- We also make the conventions, for every n in $\mathbb{Z}$,

$$-\infty < n, \quad -\infty + (-\infty) = -\infty, \quad -\infty + n = -\infty.$$

- Polynomials $(a,0,0,\ldots)$ of degree 0 or $-\infty$ are called **constant**.
- For other polynomials of small degree we have names as follows:

∂f	1	2	3	4	5	6
name	**linear**	**quadratic**	**cubic**	**quartic**	**quintic**	**sextic**

Addition and Multiplication of Polynomials

- **Addition** of polynomials is defined as follows:

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots).$$

- **Multiplication** is defined by

$$(a_0, a_1, \ldots)(b_0, b_1, \ldots) = (c_0, c_1, \ldots),$$

where, for $k = 0, 1, 2, \ldots$,

$$c_k = \sum_{\{(i,j): i+j=k\}} a_i b_j.$$

Thus,

$$c_0 = a_0 b_0, \ c_1 = a_0 b_1 + a_1 b_0, \ c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0, \ \ldots.$$

Structure of the Set P of Polynomials

- With respect to these two operations, the set P of all polynomials with coefficients in R becomes a commutative ring with unity.
- Most of the ring axioms are easily verified.
  - The zero element is $(0,0,0,\ldots)$;
  - The unity element is $(1,0,0,\ldots)$;
  - The negative of $(a_0,a_1,\ldots)$ is $(-a_0,-a_1,\ldots)$.
- For associativity of multiplication: Let $p=(a_0,a_1,\ldots)$, $q=(b_0,b_1,\ldots)$, $r=(c_0,c_1,\ldots)$ be polynomials. Then $(pq)r=(d_0,d_1,\ldots)$, where, for $m=0,1,2,\ldots$,

$$\begin{aligned} d_m &= \sum_{\{(k,\ell):k+\ell=m\}} \left(\sum_{\{(i,j):i+j=k\}} a_i b_j \right) c_\ell = \sum_{\{(i,j,\ell):i+j+\ell=m\}} a_i b_j c_\ell \\ &= \sum_{\{(i,n):i+n=m\}} a_i \left(\sum_{\{(j,\ell):j+\ell=n\}} b_j c_\ell \right). \end{aligned}$$

  The latter is the m-th entry of $p(qr)$. So multiplication is associative.

Identifying R in P

- There is a monomorphism $\theta : R \to P$ given by

$$\theta(a) = (a, 0, 0, \ldots), \quad \text{for all } a \in R.$$

- Thus, we may identify

$$\theta(a) = (a, 0, 0, \ldots)$$

  with the element a of R.
- In this way we view R as a subring of P.

The Indeterminate Form

- Let X be the polynomial $(0,1,0,0,\ldots)$.
- Then the multiplication rule gives:
  - $X^2=(0,0,1,0,\ldots)$;
  - $X^3=(0,0,0,1,0,\ldots)$;
  - In general,

$$X^n=(x_0,x_1,\ldots),\ \text{where } x_m=\begin{cases} 1, & \text{if } m=n \\ 0, & \text{otherwise} \end{cases}$$

- Now we get

$$\begin{aligned}
&(a_0,a_1,\ldots,a_n,0,\ldots)\\
&=(a_0,0,\ldots,0,0,\ldots)+(0,a_1,0,\ldots,0,0,\ldots)+\cdots+(0,0,0,\ldots,a_n,0,\ldots)\\
&=(a_0,0,\ldots,0,0,0,\ldots)+(a_1,0,0,\ldots,0,0,0,\ldots)(0,1,0,\ldots,0,0,0,\ldots)+\cdots\\
&\quad+(a_n,0,0,\ldots,0,0,0,\ldots)(0,0,0,\ldots,1,0,0,\ldots)\\
&=\theta(a_0)+\theta(a_1)X+\cdots+\theta(a_n)X^n.
\end{aligned}$$

- Identifying $\theta(a_i)$ with a_i, we get $a_0+a_1X+a_2X^2+\cdots+a_nX^n$.

Polynomial Ring of R

- Despite the expression of a polynomial in terms of $X := (0,1,0,0,\ldots)$ (regarded as an "indeterminate") it is important to note that:
  - We are talking of *polynomial forms*, wholly determined by the coefficients a_i in R;
  - X is not a member of R but only a notation for the tuple $(0,1,0,\ldots)$ of the ring P of polynomials with coefficients in R.
- We sometimes write $f = f(X)$ and say that it is a **polynomial over** R **in the indeterminate** X.
- The ring P of all such polynomials is written $R[X]$.
- We refer to $R[X]$ simply as the **polynomial ring** of R.

Properties of Polynomials

Theorem

Let D be an integral domain, and let $D[X]$ be the polynomial ring of D. Then:

(i) $D[X]$ is an integral domain.

(ii) If $p, q \in D[X]$, then $\partial(p+q) \le \max\{\partial p, \partial q\}$.

(iii) For all p, q in $D[X]$, $\partial(pq) = \partial p + \partial q$.

(iv) The group of units of $D[X]$ coincides with the group of units of D.

(i) We have already noted that $D[X]$ is a commutative ring with unity.

We show that $D[X]$ has no divisors of 0.

Suppose that p and q are non-zero polynomials with leading terms a_m, b_n, respectively. The product of p and q has leading term $a_m b_n$. By hypothesis, D has no zero divisors. So the coefficient $a_m b_n$ is non-zero. This ensures that $pq \neq 0$.

Properties of Polynomials

(ii) Let p and q be non-zero. Let $\partial p = m$, $\partial q = n$, and suppose, without loss of generality, that $m \geq n$.

- If $m > n$, then it is clear that the leading term of $p + q$ is a_m. So $\partial(p+q) = \max\{\partial p, \partial q\}$.
- If $m = n$, then we may have $a_m + b_m = 0$. So all we can say is that $\partial(p+q) \leq \max\{\partial p, \partial q\}$.

The conventions regarding $-\infty$ ensure that this result holds also if one or both of p, q are equal to 0.

(iii) By the argument in Part (i), if p and q are non-zero, then $\partial(pq) = m + n = \partial p + \partial q$. If one or both of p and q are zero, then the result holds by the conventions on $-\infty$.

(iv) Let $p, q \in D[X]$, and suppose that $pq = 1$. From Part (iii), $\partial p = \partial q = 0$. Thus $p, q \in D$, and $pq = 1$ if and only if p and q are in the group of units of D.

Polynomial in Several Variables

- Since the ring of polynomials over the integral domain D is itself an integral domain, we can repeat the preceding process.
- So we may form the ring of polynomials with coefficients in $D[X]$.
- We need to use a different letter for a new indeterminate, and the new integral domain is $(D[X])[Y]$, denoted by $D[X, Y]$.
- It consists of polynomials in X and Y with coefficients in D.
- By repeating, we obtain the integral domain $D[X_1, X_2, \ldots, X_n]$.

Rational Forms

- The field of fractions of $D[X]$ consists of **rational forms**

$$\frac{a_0 + a_1 X + \cdots + a_m X^m}{b_0 + b_1 X + \cdots + b_n X^n},$$

  where the denominator is not the zero polynomial.
- The field is denoted by $D(X)$ (with parenthesis instead of brackets).
- In a similar way one arrives at the field $D(X_1, X_2, \ldots, X_n)$ of rational forms in the n indeterminates $X_1, X_2, \ldots, X_n$, with coefficients in D.

Extension of an Isomorphism $\varphi : D \to D'$

Theorem

Let D, D' be integral domains, and let $\varphi : D \to D'$ be an isomorphism. Then the mapping $\widehat{\varphi} : D[X] \to D'[X]$ defined by

$$\widehat{\varphi}(a_0 + a_1X + \cdots + a_nX^n) = \varphi(a_0) + \varphi(a_1)X + \cdots + \varphi(a_n)X^n$$

is an isomorphism.

- The isomorphism $\widehat{\varphi}$ is called the **canonical extension** of φ.
- A further extension $\varphi^* : D(X) \to D'(X)$ is defined by

$$\varphi^*\left(\frac{f}{g}\right) = \frac{\widehat{\varphi}(f)}{\widehat{\varphi}(g)}, \quad \frac{f}{g} \in D(X).$$

On the Case of Coefficients in a Field

- Suppose that the ring R of coefficients is actually a field K.
- The group of units of $K[X]$ is the group of units of K.

  That is, it the group K^* of non-zero elements of the field K.
- As usual, we write

$$f \sim g \quad \text{iff} \quad f = ag, \text{ for some } a \text{ in } K^*.$$

The Euclidean Process in $K[X]$

Theorem (Euclidean Algorithm in $K[X]$)

Let K be a field, and let f,g be elements of the polynomial ring $K[X]$, with $g \neq 0$. Then there exist unique elements q,r in $K[X]$, such that $f = qg + r$ and $\partial r < \partial g$.

- If $f = 0$ the result is trivial, since $f = 0g + 0$.
  So suppose that $f \neq 0$. The proof is by induction on ∂f.
  - First, suppose that $\partial f = 0$, so that $f \in K^*$. If $\partial g = 0$ also, let $q = \frac{f}{g}$ and $r = 0$; otherwise, let $q = 0$ and $r = f$.
  - Suppose now that $\partial f = n$, and suppose also that the theorem holds for all polynomials f of all degrees up to $n-1$.
    - If $\partial g > \partial f$, let $q = 0$ and $r = f$.
    - Assume $\partial g \leq \partial f$. Let $a_n X^n, b_m X^m$, be the leading terms of f,g, where $m \leq n$. Then the polynomial $h = f - \left(\frac{a_n}{b_m} X^{n-m}\right) g$ has degree $\leq n-1$. So there exist q_1, r, such that $h = q_1 g + r$, with $\partial r < \partial g$. It follows that $f = h + \left(\frac{a_n}{b_m} X^{n-m}\right) g = (q_1 g + r) + \left(\frac{a_n}{b_m} X^{n-m}\right) g = \left(q_1 + \frac{a_n}{b_m} X^{n-m}\right) g + r.$

The Euclidean Process in $K[X]$ (Uniqueness)

- To prove uniqueness, suppose that

$$f = qg + r = q'g + r', \text{ with } \partial r, \partial r' < \partial g.$$

Then

$$r - r' = (q' - q)g.$$

So

$$\partial((q' - q)g) = \partial(r - r') < \partial g.$$

By a previous theorem, this cannot happen unless $q' - q = 0$. Hence $q = q'$. Consequently, $r = r'$ also.

Example of Polynomial Division

- Let $f = X^4 - X$ and $g = X^2 + 3X + 2$.

  We have

$$
\begin{array}{rrrrrr}
 & & & X^2 & -3X & +7 \\
 \cline{3-6}
X^2+3X+2 \mid & \overline{X^4} & & & \overline{-X} & \\
 & X^4 & +3X^3 & +2x^2 & & \\
 & & -3X^3 & -2X^2 & -X & \\
 & & -3X^3 & -9x^2 & -6X & \\
 & & & 7X^2 & +5X & \\
 & & & 7X^2 & +21X & +14 \\
 & & & & -16X & -14
\end{array}
$$

Thus, $X^4 - X = \underbrace{(X^2 - 3X + 7)}_{q}\underbrace{(X^2 + 3X + 2)}_{g}\underbrace{-(16X + 14)}_{r}$.

Properties of $K[X]$ for a Field K

Theorem

If K is a field, then $K[X]$ is a Euclidean domain.

- If, for all f in $K[X]$, we define $\delta(f)$ as $2^{\partial f}$, with the convention that $2^{-\infty} = 0$, we have the right properties.
- We summarize the important properties of $K[X]$.

Theorem

Let K be a field. Then:

(i) Every pair (f, g) of polynomials in $K[X]$ has a greatest common divisor d, which can be expressed as $af + bg$, with a, b in $K[X]$;

(ii) $K[X]$ is a principal ideal domain;

(iii) $K[X]$ is a factorial domain;

(iv) If $f \in K[X]$, then $K[X]/\langle f \rangle$ is a field if and only if f is irreducible.

Example

- Consider the polynomials X^2+X+1 and X^3+2X-4 in $\mathbb{Q}[X]$.
- Then one may calculate that

$$\begin{array}{rcl} X^3+2X-4 & = & (X-1)(X^2+X+1)+2X-3 \\ X^2+X+1 & = & (\frac{1}{2}X+\frac{5}{4})(2X-3)+\frac{19}{4}. \end{array}$$

- So the greatest common divisor is $\frac{19}{4}$.
- But the group of units of $\mathbb{Q}[X]$ is $Q^*=\mathbb{Q}\setminus\{0\}$. So $\frac{19}{4}\sim 1$.
- The two given polynomials are coprime.

$$\begin{array}{rcl} \frac{19}{4} & = & (X^2+X+1)-(\frac{1}{2}X+\frac{5}{4})(2X-3) \\ & = & (X^2+X+1)-(\frac{1}{2}X+\frac{5}{4})[(X^3+2X-4)-(X-1)(X^2+X+1)] \\ & = & [1+(\frac{1}{2}X+\frac{5}{4})(X-1)](X^2+X+1)-(\frac{1}{2}X+\frac{5}{4})(X^3+2X-4) \\ & = & (\frac{1}{2}X^2+\frac{3}{4}X-\frac{1}{4})(X^2+X+1)-(\frac{1}{2}X+\frac{5}{4})(X^3+2X-4). \end{array}$$

Isomorphism $\mathbb{R}[X]/\langle X^2+1\rangle \cong \mathbb{C}$

- Since X^2+1 is irreducible in $\mathbb{R}[X]$, $K=\mathbb{R}[X]/\langle X^2+1\rangle$ is a field.
- The elements of K are the residue classes $a+bX+\langle X^2+1\rangle$, $a,b\in\mathbb{R}$.
- Addition is defined by the rule

$$(a+bX+\langle X^2+1\rangle)+(c+dX+\langle X^2+1\rangle)=(a+c)+(b+d)X+\langle X^2+1\rangle.$$

- Multiplication is given by

$$\begin{aligned}&(a+bX+\langle X^2+1\rangle)(c+dX+\langle X^2+1\rangle)\\ &=ac+(ad+bc)X+bdX^2+\langle X^2+1\rangle\\ &=(ac-bd)+(ad+bc)X+bd(X^2+1)+\langle X^2+1\rangle\\ &=(ac-bd)+(ad+bc)X+\langle X^2+1\rangle.\end{aligned}$$

- These mimic the rules for adding and multiplying complex numbers.
- The map $\varphi:\mathbb{R}[X]/\langle X^2+1\rangle\to\mathbb{C}$, given by

$$\varphi(a+bX+\langle X^2+1\rangle)=a+bi,\quad a,b\in\mathbb{R},$$

is in fact an isomorphism.

Evaluation Homomorphisms

- Let D be an integral domain and let $\alpha \in D$.
- The **homomorphism** σ_α from $D[X]$ into D is defined by

$$\sigma_\alpha(a_0 + a_1 X + \cdots + a_n X^n) = a_0 + a_1\alpha + \cdots + a_n\alpha^n.$$

- This is indeed a homomorphism. Let $f(X) = a_0 + a_1 X + \cdots + a_n X^n$, $g(X) = b_0 + b_1 X + \cdots + b_m X^m$. We have, e.g.,

$$\begin{array}{rcl}\sigma_\alpha(f \cdot g) & = & \sigma_\alpha\left(\sum_{k=0}^{n+m}(\sum_{i+j=k} a_i b_j) X^k\right) \\ & = & \sum_{k=0}^{n+m}(\sum_{i+j=k} a_i b_j)\alpha^k \\ & = & (a_0 + a_1\alpha + \cdots + a_n\alpha^n)(b_0 + b_1\alpha + \cdots + b_m\alpha^m) \\ & = & \sigma_\alpha(f)\sigma_\alpha(g).\end{array}$$

- We usually write $f(\alpha)$ instead of $\sigma_\alpha(f)$.
- If $f(\alpha) = 0$, we say that α is a **root**, or a **zero**, of the polynomial f.

The Remainder Theorem

Theorem (The Remainder Theorem)

Let K be a field, let $\beta \in K$ and let f be a non-zero polynomial in $K[X]$. Then the remainder upon dividing f by $X - \beta$ is $f(\beta)$. In particular, β is a root of f if and only if $(X - \beta) \mid f$.

- By the division algorithm, there exist q, r in $K[X]$, such that

$$f = (X - \beta)q + r, \quad \partial r < \partial(X - \beta) = 1.$$

Thus r is a constant.

Substituting β for X, we see that $f(\beta) = r$.

In particular, $f(\beta) = 0$ if and only if $r = 0$ if and only if $(X - \beta) \mid f$.

Subsection 4

Irreducible Polynomials

Embedding of K Into $K[X]/\langle g(X)\rangle$

Theorem

Let K be a field, and let $g(X)$ be an irreducible polynomial in $K[X]$. Then $K[X]/\langle g(X)\rangle$ is a field containing K up to isomorphism.

- We know that $K[X]/\langle g(X)\rangle$ is a field. The map $\varphi : K \to K[X]/\langle g(X)\rangle$, given by

$$\varphi(a) = a + \langle g(X)\rangle, \quad a \in K,$$

is easily seen to be a homomorphism. It is even a monomorphism, since

$$\begin{aligned} a + \langle g(X)\rangle = b + \langle g(X)\rangle \quad & \text{iff} \quad a - b \in \langle g(X)\rangle \\ & \text{iff} \quad a = b. \end{aligned}$$

Irreducible Polynomials and Field Extensions

- This shows we have a highly effective method of constructing new fields provided we have a way of identifying irreducible polynomials.
- Certainly every linear polynomial is irreducible.
- If the field of coefficients is the complex field $\mathbb{C}$, by the Fundamental Theorem of Algebra, every polynomial in $\mathbb{C}[X]$ factorizes, essentially uniquely, into linear factors.
- Linear polynomials are of little interest as related to the preceding theorem, for $K[X]/\langle g(X)\rangle$ coincides with $\varphi(K)$ in this case, and so is isomorphic to K.

  Suppose $g(X) = X - a$. Let $f(X)$ in $K[X]$ be arbitrary. By the Euclidean Property of $K[X]$, we have that $f(X) = q(X-a) + f(a)$.

  So $f(X) + \langle g\rangle = f(a) + \langle g\rangle \in \varphi(K)$.

Irreducible Elements in $\mathbb{R}[X]$

Theorem

The irreducible elements of the polynomial ring $\mathbb{R}[X]$ are either linear or quadratic. Every polynomial $g(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ in $\mathbb{R}[X]$ has a unique factorization

$$a_n (X - \beta_1) \cdots (X - \beta_r)(X^2 + \lambda_1 X + \mu_1) \cdots (X^2 + \lambda_s X + \mu_s),$$

in $\mathbb{R}[X]$, where $a_n \in \mathbb{R}$, $r, s \geq 0$ and $r + 2s = n$.

- If $\gamma \in \mathbb{C} \backslash \mathbb{R}$ is a root, then $a_n \gamma^n + a_{n-1} \gamma^{n-1} + \cdots + a_1 \gamma + a_0 = 0$. Hence, the complex conjugate of the left-hand side is zero also. Since the coefficients $a_0, a_1, \ldots, a_n$ are real,

$$a_n \overline{\gamma}^n + a_{n-1} \overline{\gamma}^{n-1} + \cdots + a_1 \overline{\gamma} + a_0 = 0.$$

Thus, the non-real roots of the polynomial occur in conjugate pairs.

Irreducible Elements in $\mathbb{R}[X]$ (Cont'd)

- Thus, we obtain a factorization

$$g(X) = a_n(X-\beta_1)\cdots(X-\beta_r)(X-\gamma_1)(X-\overline{\gamma}_1)\cdots(X-\gamma_s)(X-\overline{\gamma}_s),$$

  in $\mathbb{C}[X]$, where $\beta_1,\ldots,\beta_r \in \mathbb{R}$, $\gamma_1,\ldots,\gamma_s \in \mathbb{C}\backslash\mathbb{R}$, $r,s \geq 0$ and $r+2s=n$.
  This gives rise to a factorization

$$a_n(X-\beta_1)\cdots(X-\beta_r)(X^2-(\gamma_+\overline{\gamma}_1)X+\gamma_1\overline{\gamma}_1)\cdots(X^2-(\gamma_s+\overline{\gamma}_s)X+\gamma_s\overline{\gamma}_s)$$

  in $\mathbb{R}[X]$. In this factorization the quadratic factors must be irreducible in $\mathbb{R}[X]$. If they had real linear factors, they would have two distinct factorizations in $\mathbb{C}[X]$, which cannot happen.
- We know that a quadratic polynomial aX^2+bX+c in $\mathbb{R}[X]$ is irreducible if and only if the discriminant $b^2-4ac<0$.

Quadratic Polynomials in $\mathbb{Q}[X]$

- In $\mathbb{Q}[X]$, the situation is not so easy, because there are irreducible polynomials of arbitrarily large degree.

Theorem

Let $g(X) = X^2 + a_1 X + a_0$ be a polynomial with coefficients in $\mathbb{Q}$. Then:

(i) If $g(X)$ is irreducible over $\mathbb{R}$, then it is irreducible over $\mathbb{Q}$;

(ii) If $g(X) = (X - \beta_1)(X - \beta_2)$, with $\beta_1, \beta_2 \in \mathbb{R}$, then $g(X)$ is irreducible in $\mathbb{Q}[X]$ if and only if β_1 and β_2 are irrational.

(i) Let $g(X)$ be irreducible over $\mathbb{R}$. Suppose $g(X) = (X - q_1)(X - q_2)$ were a factorization in $\mathbb{Q}[X]$. This would also be a factorization in $\mathbb{R}[X]$, a contradiction.

(ii) If β_1, β_2 were rational we would have a factorization in $\mathbb{Q}[X]$, and $g(X)$ would not be irreducible. Suppose β_1, β_2 are irrational. Then $(X - \beta_1)(X - \beta_2)$ is the only factorization in $\mathbb{R}[X]$. So a factorization in $\mathbb{Q}[X]$ into linear factors is not possible.

Example

- We examine the following polynomials for irreducibility in $\mathbb{R}[X]$ and $\mathbb{Q}[X]$:
$$X^2+X+1, \quad X^2+X-1, \quad X^2+X-2.$$
The first polynomial is irreducible over $\mathbb{R}$, since the discriminant is -3. It follows that it is irreducible over $\mathbb{Q}$.
The second polynomial factorizes over $\mathbb{R}$ as $(X-\beta_1)(X-\beta_2)$, where
$$\beta_1 = \frac{-1+\sqrt{5}}{2}, \quad \beta_2 = \frac{-1-\sqrt{5}}{2}.$$
It is irreducible over $\mathbb{Q}$.
The third polynomial factorizes over $\mathbb{Q}$ as $(X-1)(X+2)$.
So it is not irreducible.

The Prime Factor Divisibility Lemma

Lemma

Suppose that $n \in \mathbb{Z}$ is positive and $f, g', h' \in \mathbb{Z}[X]$, such that $nf = g'h'$. If p is a prime factor of n, then either p divides all the coefficients of g', or p divides all the coefficients of h'.

- Suppose, for a contradiction, that p does not divide all the coefficients of $g' = a_0 + a_1 X + \cdots + a_k X^k$, and that p does not divide all the coefficients of $h' = b_0 + b_1 X + \cdots + b_\ell X^\ell$. Suppose that p divides $a_0, \ldots, a_{i-1}$, but $p \nmid a_i$, and that p divides $b_0, \ldots, b_{j-1}$, but $p \nmid b_j$. The coefficient of X^{i+j} in nf is $a_0 b_{i+j} + \cdots + a_i b_j + \cdots + a_{i+j} b_0$. In this sum, all the terms preceding $a_i b_j$ are divisible by p, since p divides $a_0, \ldots, a_{j-1}$; and all the terms following $a_i b_j$ are divisible by p, since p divides $b_0, \ldots, b_{j-1}$. Hence, only the term $a_i b_j$ is not divisible by p, and it follows that the coefficient of X^{i+j} in nf is not divisible by p. This gives a contradiction, since the coefficient of f are integers, and so certainly all the coefficients of nf are divisible by p.

Gauss's Lemma

Theorem (Gauss's Lemma)

Let f be a polynomial in $\mathbb{Z}[X]$, irreducible over $\mathbb{Z}$. Then f, considered as a polynomial in $\mathbb{Q}[X]$, is irreducible over $\mathbb{Q}$.

- Suppose, for a contradiction, that $f = gh$, with $g, h \in \mathbb{Q}[X]$ and $\partial g, \partial h < \partial f$. Then there exists a positive integer n, such that $nf = g'h'$, where $g', h' \in \mathbb{Z}[X]$. Suppose that n is the smallest positive integer with this property. Let $g' = a_0 + a_1 X + \cdots + a_k X^k$ and $h' = b_0 + b_1 X + \cdots + b_\ell X^\ell$.
  - If $n = 1$, then $g' = g, h' = h$. This contradicts irreducibility of f over $\mathbb{Z}$.
  - Otherwise, let p be a prime factor of n. By the lemma, we may suppose, without loss of generality, that $g' = pg''$, where $g'' \in \mathbb{Z}[X]$. It follows that $\frac{n}{p} f = g'' h'$. This contradicts the choice of n as the least positive integer with the property $nf = g'h'$, for $g', h' \in \mathbb{Z}[X]$.

Example

- We show that $g = X^3 + 2X^2 + 4X - 6$ is irreducible over $\mathbb{Q}$.

  If the polynomial g factorizes over $\mathbb{Q}$, then it factorizes over $\mathbb{Z}$, and at least one of the factors must be linear:

  $$g = X^3 + 2X^2 + 4X - 6 = (X - a)(X^2 + bX + c).$$

  Then $ac = 6$ So $a \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$. If we substitute a for X in g, we must have $g(a) = 0$. However, the values of $g(a)$ are as follows:

a	1	−1	2	−2	3	−3	6	−6
$g(a)$	1	−9	14	−10	51	−27	306	−174

  Hence, the assumed factorization is impossible.

  So g is irreducible over $\mathbb{Q}$.

Eisenstein's Criterion

Theorem (Eisenstein's Criterion)

Let $f(X) = a_0 + a_1X + \cdots + a_nX^n$ be a polynomial in $\mathbb{Z}[X]$. Suppose that there exists a prime number p, such that:

(i) $p \nmid a_n$;

(ii) $p \mid a_i$, $i = 0, \ldots, n-1$;

(iii) $p^2 \nmid a_0$.

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

- By Gauss's Lemma, it suffices to show that f is irreducible over $\mathbb{Z}$. Suppose that $f = gh$, where

$$\begin{array}{rcl} g & = & b_0 + b_1X + \cdots + b_rX^r, \\ h & = & c_0 + c_1X + \cdots + c_sX^s, \end{array}$$

with $r, s < n$ and $r + s = n$.

Eisenstein's Criterion (Cont'd)

- Since $a_0 = b_0 c_0$, it follows from (ii) that $p \mid b_0$ or $p \mid c_0$.

  Since $p^2 \nmid a_0$, the coefficients b_0 and c_0 cannot both be divisible by p.

  We assume, without loss of generality, that $p \mid b_0$, $p \nmid c_0$.

  Suppose inductively that p divides $b_0, b_1, \ldots, b_{k-1}$, where $1 \leq k \leq r$.

  Then $a_k = b_0 c_k + b_1 c_{k-1} + \cdots + b_{k-1} c_1 + b_k c_0$.
  Since p divides each of $a_k, b_0 c_k, b_1 c_{k-1}, \ldots, b_{k-1} c_1$, $p \mid b_k c_0$.
  Hence, $p \mid b_k$.

  We conclude that $p \mid b_r$.

  So, since $a_n = b_r c_s$, we have that $p \mid a_n$.

  This contradicts (i).

  Hence f is irreducible.

Examples

- The polynomial $X^5+2X^3+\frac{8}{7}X^2-\frac{4}{7}X+\frac{2}{7}$ is irreducible over $\mathbb{Q}$:
  $7X^5+14X^3+8X^2-4X+2$ satisfies Eisenstein's criterion, with $p=2$.
- We show that $f(X)=2X^5-4X^4+8X^3+14X^2+7$ is irreducible over $\mathbb{Q}$.
  The polynomial f does not satisfy the required conditions.
  Suppose we have a factorization $f=gh$, with (say) $\partial g=3$ and $\partial h=2$.
  Then

$$\begin{array}{rcl} 7X^5+14X^3+8X^2-4X+2 & = & X^5\left(2\frac{1}{X^5}-4\frac{1}{X^4}+8\frac{1}{X^3}+14\frac{1}{X^2}+7\right) \\ & = & X^5 f\left(\frac{1}{X}\right) \\ & = & \left(X^3 g\left(\frac{1}{X}\right)\right)\left(X^2 h\left(\frac{1}{X}\right)\right). \end{array}$$

  This is a factorization of $7X^5+14X^3+8X^2-4X+2$.
  By the preceding example, we know that this cannot happen.

The Polynomial $f(X) = 1 + X + X^2 + \cdots + X^{p-1}$

- We show that, if $p > 2$ is prime, then

$$f(X) = 1 + X + X^2 + \cdots + X^{p-1}$$

is irreducible over $\mathbb{Q}$.
Observe that $f(X) = \frac{X^p - 1}{X - 1}$. Define $g(X) = f(X+1)$. Then

$$g(X) = \frac{1}{X}((X+1)^p - 1) = \sum_{r=0}^{p-1} \binom{p}{r} X^{p-r-1}.$$

The coefficients $\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}$ are all divisible by p.
Hence g is irreducible, by Eisenstein's Criterion.
Suppose $f = uv$, with $\partial u, \partial v < \partial f$ and $\partial u + \partial v = \partial f$.
Then $g(X) = u(X+1)v(X+1)$. The factors $u(X+1)$ and $v(X+1)$ are polynomials in X, of the same degrees (respectively) as u and v.
This contradicts the irreducibility of g.

Reduction Modulo a Prime

- A method for determining irreducibility over $\mathbb{Z}$ (and so over $\mathbb{Q}$) is to map the polynomial onto $\mathbb{Z}_p[X]$, for some suitably chosen prime p.
- Let $g = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$, and let p be a prime, $p \nmid a_n$.
- Let $\overline{a}_i$ be the residue class $a_i + \langle p \rangle$ in the field $\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle$, $i = 0, \ldots, n$.
- Write the polynomial $\overline{a}_0 + \overline{a}_1X + \cdots + \overline{a}_nX^n$ as $\overline{g}$.
- Our choice of p ensures that $\partial\overline{g} = n$.
- Suppose that $g = uv$, with $\partial u, \partial v < \partial g$ and $\partial u + \partial v = \partial g$.
- Then $\overline{g} = \overline{uv}$.
- So, if g is irreducible in $\mathbb{Z}_p[X]$, then g is irreducible.
- The advantage of transferring the problem from $\mathbb{Z}[X]$ to $\mathbb{Z}_p[X]$ is that $\mathbb{Z}_p$ is finite, and the verification of irreducibility is a matter of checking a finite number of cases.

Illustration of the Reduction Technique

- We show that $g = 7X^4 + 10X^3 - 2X^2 + 4X - 5$ is irreducible over $\mathbb{Q}$.

  If we choose $p = 3$, then $\overline{g} = X^4 + X^3 + X^2 + X + 1$.

  The elements of $\mathbb{Z}_3$ may be taken as $0, 1, -1$, with $1 + 1 = -1$.

  - $\overline{g}$ has no linear factor: We have $\overline{g}(0) = 1$, $\overline{g}(1) = -1$ and $\overline{g}(-1) = 1$.
  - There remains the possibility that (in $\mathbb{Z}_3[X]$)
    $X^4 + X^3 + X^2 + X + 1 = (X^2 + aX + b)(X^2 + cX + d)$.
    Equating coefficients gives $a + c = 1$, $b + ac + d = 1$, $bd = 1$, $ad + bc = 1$.
    (i) If $b = d = 1$, then $ac = -1$. So $(a, c) = (1, -1)$ or $(a, c) = (-1, 1)$. In either case $a + c = 0$, a contradiction.
    (ii) If $b = d = -1$, then $ac = 0$.
    If $a = 0$ then $c = 1$. So $1 = ad + bc = b$, a contradiction.
    If $c = 0$, then $a = 1$. Then $1 = ad + bc = d$, again a contradiction.

  We have shown that $\overline{g}$ is irreducible over $\mathbb{Z}_3$.

  It follows that g is irreducible over $\mathbb{Q}$.