38 Irreducibility criteria in rings of polynomials

38.1 Theorem. Let \( p(x), q(x) \in R[x] \) be polynomials such that
\[
p(x) = a_0 + a_1 x + \ldots + a_n x^n, \quad q(x) = b_0 + b_1 x + \ldots + b_m x^m
\]
and \( a_n, b_m \neq 0 \). If \( b_m \) is a unit in \( R \) then there exist unique polynomials \( r(x), s(x) \in R[x] \) such that
\[
p(x) = s(x)q(x) + r(x)
\]
and either \( \deg r(x) < \deg q(x) \) or \( r(x) = 0 \).

Proof. Exercise (or see Hungerford p.158).

38.2 Definition. If \( R \) is a ring and \( p(x) \in R[x] \) then \( p(x) \) defines a function
\[
p: R \rightarrow R, \quad a \mapsto p(a)
\]
A function of this form is called a polynomial function.

38.3 Note. Different polynomials may define the same polynomial function.

E.g. if \( p(x) = x + 1 \), \( q(x) = x^2 + 1 \) are polynomials in \( \mathbb{Z}/2\mathbb{Z}[x] \) then \( p(x), q(x) \) define the same function \( \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \):
\[
p(0) = q(0) = 1, \quad p(1) = q(1) = 0
\]

38.4 Definition. Let \( p(x) \in R[x] \). An element \( a \in R \) is a root of \( p(x) \) if \( f(a) = 0 \).
38.5 Proposition. An element \( a \in R \) is a root of \( p(x) \in R[x] \) iff \( (x - a) \mid p(x) \).

Proof.

(\(\Leftarrow\)) If \( (x - a) \mid p(x) \) then \( p(x) = q(x)(x - a) \) for some \( q(x) \in R[x] \) so \( p(a) = q(a)(a - a) = 0 \).

(\(\Rightarrow\)) Assume that \( p(a) = 0 \). By Theorem 38.1 we have

\[
p(x) = s(x)(x - a) + r(x)
\]

where \( \deg r(x) = 0 \), so \( r(x) = b \) for some \( b \in R \). This gives

\[
0 = p(a) = s(a)(a - a) + b
\]

Thus \( b = 0 \), and so \( p(x) = s(x)(x - a) \).

\[\square\]

38.6 Corollary. If \( R \) is an integral domain and \( 0 \neq p(x) \in R[x] \) is a polynomial of degree \( n \) then \( R[x] \) has at most \( n \) distinct roots in \( R \).

Proof. Let \( a_1, \ldots, a_k \in R \) be all distinct roots of \( p(x) \). By (38.5) we have

\[
p(x) = (x - a_1)q_1(x)
\]

for some \( q_1(x) \in R[x] \). Also we have

\[
0 = p(a_2) = (a_2 - a_1)q_1(a_2)
\]

Since \( R \) is an integral domain and \( a_2 - a_1 \neq 0 \) we obtain \( q_1(a_2) \), and so

\[
q_2(x) = (x - a_2)q_3(x)
\]

for some \( q_3(x) \in R[x] \). This gives

\[
p(x) = (x - a_1)(x - a_2)q_3(x)
\]

151
By induction we obtain
\[ p(x) = (x - a_1) \cdot \ldots \cdot (x - a_k) q_k(x) \]
for some \( 0 \neq q_k(x) \in R[x] \). This gives
\[ \deg p(x) = \deg((x - a_1) \cdot \ldots \cdot (x - a_k) q_k(x)) \geq k \]

38.7 Note.

1) Corollary 38.6 in not true if \( R \) is not an integral domain. E.g. if \( R = \mathbb{Z}/6\mathbb{Z} \) and \( p(x) = x^2 + x \) then \( 0, 2, 3 \in \mathbb{Z}/6\mathbb{Z} \) are roots of \( p(x) \).

2) Corollary 38.6 is not true is \( R \) is a non-commutative ring (even if \( R \) is an integral domain). For example, if \( R = \mathbb{H} \) and \( p(x) = x^2 + 1 \) then \( \pm i, \pm j, \pm k \in \mathbb{H} \) are roots of \( p(x) \).

Recall:

33.7 Proposition. If \( p \in \mathbb{Z} \) is a prime number then the groups of units \((\mathbb{Z}/p\mathbb{Z})^*\) of the ring \( \mathbb{Z}/p\mathbb{Z} \) is a cyclic group of order \((p - 1)\).

Proof. For a prime \( q \) let \( P_q \) be the Sylow \( q \)-subgroup of \((\mathbb{Z}/p\mathbb{Z})^*\). We have
\[ (\mathbb{Z}/p\mathbb{Z})^* = \bigoplus_{q | (p-1)} P_q \]
It suffices to show that \( P_q \) is cyclic for ever \( q \mid (p - 1) \).

Let \( a \) be an element of the largest order in \( P_q \). We will show that \( P_q = \langle a \rangle \). Let \( |a| = q^m \). If \( b \in P_q \) then \( |b| = q^k \) for some \( k \leq m \). As a consequence all elements of \( P_q \) are roots of the polynomial
\[ r(x) = x^{q^m} - 1 \]
On the other hand by (38.6) \( r(x) \) has at most \( q^m \) distinct roots in \( \mathbb{Z}/p\mathbb{Z} \). It follows that

\[
|P_q| \leq q^m = |\langle a \rangle|
\]

Since \( \langle a \rangle \subseteq P_q \) this shows that \( \langle a \rangle = P_q \).

38.8 Note. Proposition 33.7 can be generalized as follows: if \( \mathbb{F} \) is a finite field and \( \mathbb{F}^* = \mathbb{F} - \{0\} \) is the multiplicative group of units of \( \mathbb{F} \) then \( \mathbb{F}^* \) is a cyclic group. The proof is the same as for \( \mathbb{F} = \mathbb{Z}/p\mathbb{Z} \).

38.9 Proposition. If \( \mathbb{F} \) is a field and \( p(x) \in \mathbb{F}[x] \) is a polynomial such that \( \deg p(x) > 1 \) and \( p(x) \) has a root in \( \mathbb{F} \) then \( p(x) \) is not irreducible in \( \mathbb{F}[x] \).

Proof. By (38.6) we have \( p(x) = q(x)(x-a) \) for some \( q(x) \in \mathbb{F}[x] \). Since \( \deg p(x) > 1 \) we have \( \deg q(x) > 0 \), so \( q(x) \) and \( (x-a) \) are not units in \( \mathbb{R}[x] \).

38.10 Corollary. Let \( R \) be a UFD and let \( K \) be the field of fractions of \( R \). If \( p(x) \in R[x] \) is a polynomial such that \( \deg p(x) > 1 \) and \( p(x) \) has a root in \( K \) then \( p(x) \) is not irreducible in \( R[x] \).

Proof. By (38.6) \( p(x) \) is not irreducible in \( K[x] \), so by (37.10) it is also not irreducible in \( R[x] \).

38.11 Proposition (Integral root test). Let \( R \) be a UFD, let \( K \) be the field of fractions of \( R \) and let \( p(x) \in R[x] \) be a polynomial

\[
p(x) = a_0 + a_1 x + \ldots + a_n x^n
\]

153
where $a_n \neq 0$. If $a \in K$ is a root of $p(x)$ then $a$ is of the form $a = b/s$ where $b, s \in R$, $\gcd(b, s) \sim 1$, $b \mid a_0$ and $s \mid a_n$.

In particular, in $a_n = 1$ then $a \in R$ and $a \mid a_0$.

**Proof.** Exercise. \qed

**38.12 Theorem** (Eisenstein Irreducibility Criterion). *Let $R$ be a UFD. If

$$p(x) = a_0 + a_1 x + \ldots + a_n x^n$$

is a primitive polynomial in $R[x]$ such that $\deg p(x) > 0$, and $b \in R$ is an irreducible element $b \in R$ such that

1) $b \nmid a_n$
2) $b \mid a_i$ for all $i < n$
3) $b^2 \nmid a_0$

then $p(x)$ is irreducible in $R[x]$.\]

**Proof.** Assume that $p(x)$ is not irreducible in $R[x]$. Then we have

$$p(x) = q(x)r(x)$$

for some non-units $q(x), r(x) \in R[x]$. Since $p(x)$ is primitive we must have $\deg q(x), \deg r(x) > 0$. Let

$$q(x) = c_0 + c_1 x + \ldots + c_k x^k, \quad r(x) = d_0 + d_1 x + \ldots + d_l x^l$$

Notice that since $b$ is irreducible it is a prime element of $R$ and so by (32.4) the ideal $\langle b \rangle$ is a prime ideal of $R$. As a consequence $R/\langle b \rangle$ is an integral domain. Consider the canonical epimorphism $\pi: R \to R/\langle b \rangle$ and the induced homomorphism of rings of polynomials

$$\bar{\pi}: R[x] \longrightarrow R/\langle b \rangle[x]$$

154
By assumption on $p(x)$ we have
\[ \tilde{\pi}(p(x)) = \pi(a_n)x^n \]

On the other hand we have
\[ \tilde{\pi}(p(x)) = \tilde{\pi}(q(x))\tilde{\pi}(r(x)) \]

Check: since $R/\langle b \rangle$ is an integral domain we must have
\[ \tilde{\pi}(q(x)) = \pi(c_k)x^k, \quad \tilde{\pi}(r(x)) = \pi(d_l)x^l \]

In particular $\pi(c_0) = \pi(d_0) = 0$, so $b \mid c_0$ and $b \mid d_0$. On the other hand $a_0 = c_0d_0$, so $b^2 \mid a_0$ which contradicts the assumption on $a_0$. \qed

\textbf{38.13 Example.} If $p \in \mathbb{Z}$ is a prime number then $q(x) = x^n - p$ is an irreducible polynomial in $\mathbb{Z}[x]$.

Note: by (37.10) $q(x)$ is also irreducible in $\mathbb{Q}[x]$. This shows in particular that $q(x)$ has no roots in $\mathbb{Q}$, and so that $n\sqrt{p}$ is an irrational number for all primes $p$ and all $n > 1$.

\textbf{38.14 Proposition.} Let $R$ be an integral domain and let $c \in R$. A polynomial $p(x) = \sum_{i=0}^{n} a_i x^i$ is irreducible iff the polynomial $p(x - c) = \sum_{i=0}^{n} (x - c)^i$ is irreducible.

\textbf{Proof.} It is enough to notice that the map
\[ f: R[x] \to R[x], \quad f(p(x)) = p(x - c) \]

is an isomorphism of rings. \qed
38.15 Example. Let $p \in \mathbb{Z}$ be a prime number, and let

$$q(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$$

We will show that $q(x)$ is irreducible in $\mathbb{Z}[x]$. We have

$$q(x) = \frac{x^p - 1}{x - 1}$$

This gives

$$q(x + 1) = \frac{(x + 1)^p - 1}{(x + 1) - 1} = \frac{(x + 1)^p - 1}{x} = x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \ldots + \binom{p}{p-1}$$

Since $p \mid \binom{p}{k}$ for $k = 1, \ldots, p - 1$ and $p^2 \nmid \binom{p}{p-1}$ the polynomial $q(x + 1)$ is irreducible in $\mathbb{Z}[x]$, and so $q(x)$ is also irreducible.
39 Modules

39.1 Definition. Let $R$ be a (possibly non-commutative) ring. A **left $R$-module** is an abelian group $M$ together with a map
\[ R \times M \rightarrow M, \quad (r, m) \mapsto rm \]
satisfying the following conditions:

1) $r(m + n) = rm + rn$
2) $(r + s)m = rm + sm$
3) $(rs)m = r(sm)$
4) If $R$ is a ring with identity $1 \in R$ then $1m = m$ for all $m \in M$.

A **right $R$-module** is defined analogously.

39.2 Definition. If $M, N$ are left $R$-modules then a map
\[ f : M \rightarrow N \]
is a **left $R$-modules homomorphism** if $f$ is a homomorphism of abelian groups and $f(rm) = rf(m)$ for all $r \in R$, $m \in M$.

39.3 Note. Left $R$-modules and their homomorphisms form a category $R$-$\text{Mod}$. Analogously, right $R$-modules form a category $\text{Mod}$-$R$.

39.4 Examples.

1) If $I$ is a left ideal of $R$ then $I$ is a left module of $R$. In particular $R$ is a left $R$-module.

2) If $\mathbb{F}$ is a field then (or right ) $\mathbb{F}$-modules are vector spaces over $\mathbb{F}$, and homomorphisms of $\mathbb{F}$-modules are $\mathbb{F}$-linear maps.
3) The category of left (or right) $\mathbb{Z}$-modules is isomorphic to the category of abelian groups: if $G$ is an abelian group then $G$ has a natural $\mathbb{Z}$-module structure such that for $n \in \mathbb{Z}$ and $g \in G$ we have

\[ ng = \begin{cases} 
\underbrace{g + \cdots + g}_{\text{n times}} & \text{for } n > 0 \\
0 & \text{for } n = 0 \\
\underbrace{(-g) + \cdots + (-g)}_{|n| \text{ times}} & \text{for } n < 0
\end{cases} \]

4) Let $G$ be an abelian group, and let $R = \text{Hom}(G, G)$ be the ring of homomorphisms of $G$ (with the usual addition of homomorphisms and multiplication given by composition of homomorphisms). We have a map

\[ R \times G \to G, \quad \varphi \cdot g = \varphi(g) \]

Check: this defines a left $R$-module structure on $G$.

Note: the multiplication

\[ G \times R \to G, \quad g \cdot \varphi = \varphi(g) \]

does not define a right module structure on $G$. Indeed, for $\varphi, \psi \in R$ we have:

\[(g \cdot \psi) \cdot \varphi = (\psi(g)) \cdot \varphi = \varphi(\psi(g)) \]

One the other hand $g \cdot (\psi \cdot \varphi) = \psi(\varphi(g))$. Since in general $\psi(\varphi(g)) \neq \varphi(\psi(g))$ we get that

\[(g \cdot \psi) \cdot \varphi \neq g \cdot (\psi \cdot \varphi) \]

39.5 Note. For a ring $R$ define a ring $R^{\text{op}}$ as follows:

- $R^{\text{op}} = R$ as abelian group
- $r \cdot_{\text{new}} s := sr$
We have:

\[(\text{left } R\text{-modules}) = (\text{right } R^{\text{op}}\text{-modules})\]

(check!). In particular, if \(R\) is a commutative ring then \(R = R^{\text{op}}\), and so

\[(\text{left } R\text{-modules}) = (\text{right } R\text{-modules})\]

**Note.** From now on by an \(R\)-module we will understand a *left* \(R\)-module.
40 Basic operations on modules

40.1 Definition. If $M$ in an $R$-module then a submodule of $M$ is an additive subgroup $N \subseteq M$ such that if $r \in R$ and $n \in N$ then $rn \in N$.

40.2 Note. If $f: M \to N$ is a homomorphism of $R$-modules then $\ker(f) := f^{-1}(0)$ is a submodule of $M$ and $\operatorname{Im}(f) := f(M)$ is a submodule of $N$.

40.3 Definition. If $M$ is an $R$-module and $S$ is a subset of $M$ then the module generated by $S$ is the submodule $\langle S \rangle \subseteq M$ that is the smallest submodule of $M$ containing $S$.

If $\langle S \rangle = M$ then we say that the set $S$ generates $M$. A module $M$ is finitely generated if $M = \langle S \rangle$ for some finite set $S$.

40.4 Note. If $M$ is an $R$-module and $S \subseteq M$ then

$$\langle S \rangle = \{ r_1m_1 + \ldots + r_km_k \mid r_i \in R, m_i \in M \}$$

40.5 Definition. If $M$ is an $R$-module and $N \subseteq M$ is a submodule then the quotient module $M/N$ is the quotient abelian group with multiplication defined by

$$r(m + N) := rm + N$$

for $r \in R, m + N \in M/N$.

40.6 First Isomorphism Theorem. If $f: M \to N$ is a homomorphism of $R$-modules that is onto then

$$M/\ker(f) \cong N$$
Proof. Similar to the proof of Theorem 6.1 for groups.

40.7 Definition. If \( \{ M_i \}_{i \in I} \) is a family of \( R \)-modules then the direct product of \( \{ M_i \}_{i \in I} \) is the module

\[
\prod_{i \in I} M_i = \{ (m_i)_{i \in I} \mid m_i \in M_i \}
\]

with addition and multiplication by \( R \) defined coordinatewise.

The direct sum of \( \{ M_i \}_{i \in I} \) is the submodule \( \bigoplus_{i \in I} M_i \) of \( \prod_{i \in I} M_i \) given by

\[
\bigoplus_{i \in I} M_i := \{ (m_i)_{i \in I} \mid m_i \neq 0 \text{ for finitely many } i \text{ only } \}
\]

40.8 Note. Recall the notions of categorical products and coproducts (Section 12). Check:

\( \prod_{i \in I} M_i \) is the categorical product of the family \( \{ M_i \}_{i \in I} \) in the category \( R\text{-Mod} \).

\( \bigoplus_{i \in I} M_i \) is the categorical coproduct of \( \{ M_i \}_{i \in I} \) in the category \( R\text{-Mod} \).
41 Free modules and vector spaces

41.1 Definition. Let $M$ be an $R$-module. A set $S \subseteq M$ is linearly independent if for any distinct $m_1, \ldots, m_k \in S$ we have

$$r_1 m_1 + \ldots + r_k m_k = 0$$

only if $r_1 = \ldots = r_k = 0$.

41.2 Definition. Let $M$ be an $R$-module. A set $B \subseteq M$ is a basis of $M$ if $B$ is linearly independent and $B$ generates $M$.

41.3 Definition. An $R$-module $M$ is a free module if $M$ has a basis.

41.4 Theorem. Let $R$ be a ring with identity $1 \neq 0$ and let $F$ be an $R$-module. The following conditions are equivalent.

1) $F$ is a free module.

2) $F \cong \bigoplus_{i \in I} R$ for some set $I$.

3) There is a non-empty subset $B \subseteq F$ satisfying the following universal property. For any $R$-module $M$ and any map of sets $f: B \to M$ there is a unique $R$-module homomorphism $\bar{f}: F \to N$ such that the following diagram commutes:

$$\begin{array}{ccc}
B & \xrightarrow{f} & M \\
\downarrow i & & \downarrow \bar{f} \\
F & \xleftarrow{f} & \\
\end{array}$$

Here $i: B \hookrightarrow F$ is the inclusion map.

Proof. Exercise. \qed

162
41.5 Note. Let $U: R\text{-Mod} \to \text{Set}$ be the forgetful functor. Check: $U$ has a left adjoint functor

$$F_{R\text{Mod}}: \text{Set} \to R\text{-Mod}$$

One can show that an $R$-module $M$ is free iff $M \cong F_{R\text{Mod}}(S)$ for some set $S$ (exercise).

41.6 Note. We have:

$$(\text{free } \mathbb{Z}\text{-modules}) = (\text{free abelian groups})$$

41.7 Theorem. If $R$ is a division ring then every $R$-module is free.

Proof. Let $M$ be an $R$-module. It is enough to show that $M$ has a basis.

Let $S$ be the set of all linearly independent subsets of $M$ ordered with respect to inclusion of subsets.

Claim 1. $S$ has a maximal element.

Indeed, by Zorn’s Lemma (29.10) it is enough to show that every chain in $S$ has an upper bound. Let then $T = \{B_i\}_{i \in I}$ be a chain in $S$. Take $B := \bigcup_{i \in I} B_i$. We have $B_i \subseteq B$ for all $i \in I$, so it suffices check that $B$ is a linearly independent. Let then $b_1, \ldots, b_k \in B$, and assume that

$$r_1b_1 + \ldots + r_kb_k = 0$$

We need to show that $r_1 = \ldots = r_k = 0$.

We have $b_1 \in B_{i_1}, \ldots, b_k \in B_{i_k}$ for some $i_1, \ldots, i_k \in I$. Since $\{B_i\}_{i \in I}$ is a chain we can assume that

$$B_{i_1} \subseteq B_{i_2} \subseteq \ldots \subseteq B_{i_k}$$

As a consequence $b_1, \ldots, b_k \in B_{i_k}$, and since $B_{i_k}$ is a linearly independent set we get that $r_1 = \ldots = r_k = 0$. 163
Claim 2. If \( B \) is a maximal element in \( S \) then \( B \) is a basis of \( M \).

Indeed, by the definition of \( S \) the set \( B \) is linearly independent so it is enough to show that \( \langle B \rangle = M \). Assume that this is not true, and let \( m \in M - \langle B \rangle \). Take the set

\[
B' = B \cup \{ m \}
\]

Notice that the set \( B' \) is linearly independent. To see this, assume that for some \( b_1, \ldots, b_k \in B \) and \( r_1, \ldots, r_k, s \in R \) we have

\[
r_1 b_1 + \ldots + r_k b_k + sm = 0
\]

If \( s \neq 0 \) then \( s \) is a unit (since \( R \) is a division ring) and so

\[
m = (-s^{-1}r_1)b_1 + \ldots + (-s^{-1}r_k)b_k
\]

This is however impossible since \( m \not\in \langle B \rangle \). Therefore \( s = 0 \), and so

\[
r_1 b_1 + \ldots + r_k b_k = 0
\]

Linear independence of \( B \) gives then \( s = r_1 = \ldots = r_k = 0 \)

As a consequence we get that \( B' \in S \) and \( B \subsetneq B' \). This is however a contradiction since \( B \) is a maximal element of \( S \).

\[\square\]

41.8 Note. Let \( R \) be a division algebra and let \( M \) be an \( R \)-module. By a similar argument as in the proof of Theorem 41.7 we can show that:

1) if \( V \subseteq M \) is a linearly independent set then there is a basis \( B \) of \( M \) such that \( V \subseteq B \);

2) if \( V \subseteq M \) is a set generating \( M \) then there is a basis \( B \) of \( M \) such that \( B \subseteq V \).
41.9 Note.

1) For a general ring $R$ it is not true that a linearly independent subset $V$ of a free $R$-module $F$ can be always extended to a basis. Take e.g.

$$R = \mathbb{Z}, \quad F = \mathbb{Z}, \quad V = \{2\}$$

2) It is also not true in general that if $V$ is a set generating a free $R$-module then $V$ contains a basis of $F$. Take e.g.

$$R = \mathbb{Z}, \quad F = \mathbb{Z}, \quad V = \{2, 3\}$$