31 Prime elements

31.1 Definition. Let $R$ be an integral domain, and let $a, b \in R$. We say that $a$ divides $b$ if $b = ac$ for some $c \in R$. We then write: $a \mid b$.

31.2 Proposition. If $R$ is an integral domain and $a, b \in R$ then $a \sim b$ iff $a \mid b$ and $b \mid a$.

Proof. Exercise. \qed

31.3 Definition. Let $R$ be an integral domain. An element $a \in R$ is a prime element if $p \neq 0$, $p$ is a non-unit and if $a \mid bc$ then either $a \mid b$ or $a \mid c$.

31.4 Example.

1) In $\mathbb{Z}$ we have

$$\{\text{prime elements}\} = \{\pm \text{prime numbers}\} = \{\text{irreducible elements}\}$$

2) By the proof of Proposition 30.9 in $\mathbb{Z}[\sqrt{-5}]$ the element $\alpha = 2 + \sqrt{5}i$ is irreducible. On the other hand $\alpha$ is not a prime element:

$$\alpha \mid (3 \cdot 3) \quad \text{but} \quad \alpha \nmid 3$$

31.5 Proposition. If $R$ is an integral domain and $a \in R$ is a prime element then $a$ is irreducible.

Proof. Let $a \in R$ be a prime element and let $a = bc$. We want to show that either $b$ or $c$ must be a unit in $R$. 

124
We have $a \mid (bc)$, and since $a$ is a prime element it implies that $a \mid b$ or $a \mid c$.

We can assume that $a \mid b$. Since also $b \mid a$, thus by (31.2) we obtain that $a \sim b$, i.e. $a = bu$ for some unit $u \in R$. Therefore we have

$$bc = a = bu$$

By (25.6) this gives $u = c$, and so $c$ is a unit.

31.6 Proposition. If $R$ is a UFD and $a \in R$ then $a$ is an irreducible element iff $a$ is a prime element.

Proof.

$(\Leftarrow)$ Follows from Proposition 31.5.

$(\Rightarrow)$ Assume that $a \in R$ is irreducible and that $a \mid (bc)$. We want to show that either $a \mid b$ or $a \mid c$.

If $b = 0$ then $b = a \cdot 0$ so $a \mid 0$. If $b$ is a unit then $c = b^{-1}bc$ so $a \mid c$.

As a consequence we can assume that $b, c$ are non-zero, non-units.

Since $a \mid (bc)$ there is $d \in R$ such that $bc = ad$. Assume that $d$ is not a unit.

Since $R$ is a UFD we have decompositions:

$$b = b_1 \cdots b_m, \quad c = c_1 \cdots c_n, \quad d = d_1 \cdots d_p$$

where $b_i, c_j, d_k$ are irreducible. This gives

$$b_1 \cdots b_m \cdot c_1 \cdots c_n = a \cdot d_1 \cdots d_p$$

By the uniqueness of decomposition in UFDs this implies that either $a \sim b_i$ for some $i$ or $a \sim c_j$ for some $j$. In the first case we get $a \mid b$, and in the second case $a \mid c$.

If $d$ is a unit the argument is similar. \qed
31.7 Theorem. An integral domain \( R \) is a UFD iff

1) every non-zero, non-unit element of \( R \) is a product of irreducible elements
2) every irreducible element in \( R \) is a prime element.

Proof.

(\( \Rightarrow \)) Follows from the definition of UFD (30.7) and Proposition 31.6.

(\( \Leftarrow \)) Assume that \( R \) satisfies conditions 1)-2) of the theorem. We only need to show that if \( b_1, \ldots, b_k, c_1, \ldots, c_l \) are irreducible elements in \( R \) such that
\[
b_1 \cdot \ldots \cdot b_k = c_1 \cdot \ldots \cdot c_l
\]
then \( k = l \), and after reordering factors we have \( b_1 \sim c_1, \ldots, b_k \sim c_k \).

We argue by induction with respect to \( k \).

If \( k = 1 \) then we have \( b_1 = c_1 \cdot \ldots \cdot c_l \). Since \( b_1 \) is irreducible this implies that \( l = 1 \), and so \( b_1 = c_1 \).

Next, assume that the uniqueness property holds for some \( k \) and that we have
\[
b_1 \cdot \ldots \cdot b_k \cdot b_{k+1} = c_1 \cdot \ldots \cdot c_l
\]
where \( b_i, c_j \) are irreducible elements. This implies that \( b_{k+1} \mid (c_1 \cdot \ldots \cdot c_l) \). By condition 2) of the theorem \( b_{k+1} \) is a prime element. It follows that \( b_k \mid c_j \) for some \( 1 \leq j \leq l \). We can assume that \( b_{k+1} \mid c_l \). Then \( c_l = ab_{k+1} \) for some \( a \in R \). Also, since \( c_l, b_{k+1} \) are irreducible \( a \) must be a unit. This shows that \( b_{k+1} \sim c_l \). Furthermore, we obtain from here that
\[
b_1 \cdot \ldots \cdot b_k \cdot b_{k+1} = c_1 \cdot \ldots \cdot c_{l-1} \cdot ab_{k+1}
\]
Since \( R \) is an integral domain we get
\[
b_1 \cdot \ldots \cdot b_k = c_1 \cdot \ldots \cdot c_{l-1} a
\]
Since \( b_k \) is irreducible and \( a \) is a unit the product \( c_{l-1} a \) is an irreducible element. Therefore by the inductive assumption \( k = l - 1 \), and after reordering of factors we have
\[
b_1 \sim c_1, \ldots, b_{k-1} \sim c_{k-1}, \ b_k \sim c_{l-1} a \sim c_{l-1}
\]
32 PIDs and UFDs

32.1 Theorem. If $R$ is a PID then it is a UFD.

32.2 Lemma. If $R$ is a PID and $I_1, I_2, \ldots$ are ideals of $R$ such that

$$I_1 \subseteq I_2 \subseteq \ldots$$

then there exists $n \geq 1$ such that $I_n = I_{n+1} = \ldots$.

Proof. Take $I = \bigcup_{i=1}^{\infty} I_i$. Check: $I$ is an ideal of $R$. Since $R$ is a PID we have $I = \langle a \rangle$ for some $a \in I$. Take $n \geq 1$ such that $a \in I_n$. Then we get

$$I \subseteq I_n \subseteq I_{n+1} \subseteq \ldots \subseteq I$$

It follows that $I_n = I_{n+1} = \ldots = I$. \hfill \Box

32.3 Lemma. Let $R$ be a PID. An element $a \in R$ is irreducible iff $\langle a \rangle$ is a maximal ideal of $R$.

Proof. Exercise. \hfill \Box

32.4 Lemma. If $R$ is an integral domain then $a \in R$ is a prime element iff $\langle a \rangle$ is a non-zero prime ideal of $R$.

Proof. Exercise. \hfill \Box

Proof of Theorem 32.1. Let $R$ be a PID. By Theorem 31.7 it suffices to show that
1) every non-zero, non-unit element of $R$ is a product of irreducible elements
2) every irreducible element in $R$ is a prime element.

1) We argue by contradiction. Assume that $a_0 \in R$ is a non-zero, non-unit
element that is not a product of irreducibles. This implies that

$$a_0 = a_1 b_1$$

for some non-zero, non-unit elements $a_1, b_1 \in R$.

Next, if both $a_1$ and $b_1$ were products of irreducibles, then $a_0$ would be also a
product of irreducibles, contradicting our assumption. We can then assume that
$a_1$ is not a product of irreducibles, and so in particular we have

$$a_1 = a_2 b_2$$

for some non-zero, non-unit elements $a_2, b_2 \in R$.

By induction we obtain that for $i = 1, 2, \ldots$ there exists non-zero, non-unit
elements $a_i, b_i \in R$ such that $a_i = a_{i+1} b_{i+1}$ for all $i \geq 0$.

Consider the chain of ideals

$$\langle a_0 \rangle \subseteq \langle a_1 \rangle \subseteq \ldots$$

By Lemma 32.2 we obtain that $\langle a_n \rangle = \langle a_{n+1} \rangle$ for some $n \geq 0$. This means that
$a_n = a_{n+1} u$ for some unit $u \in R$ (check!). As a consequence we obtain

$$a_{n+1} b_{n+1} = a_n = a_{n+1} u$$

and so $b_{n+1} = u$. This is a contradiction, since $b_{n+1}$ is not a unit.

2) Let $a \in R$ be an irreducible element and let $a \mid (bc)$. We need to show that
either $a \mid b$ or $a \mid c$.

Assume that $a \nmid b$. This implies that $b \not\in \langle a \rangle$ and so

$$\langle a \rangle \neq \langle a \rangle + \langle b \rangle$$
Since by Lemma 32.3 the ideal $\langle a \rangle$ is a maximal ideal we obtain then that $\langle a \rangle + \langle b \rangle = R$, and so in particular $1 \in \langle a \rangle + \langle b \rangle$. Therefore

$$1 = ar + bs$$

for some $r, s \in R$, and so

$$c = a(rc) + (bc)s$$

Since $a \mid a(rc)$ and $a \mid (bc)s$ we obtain from here that $a \mid c$. 

$\Box$
33 Application: sums of two squares

Recall. The ring of Gaussian integers:

\[ \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \]

\(\mathbb{Z}[i]\) is a Euclidean domain with the norm function \(N(a + bi) = a^2 + b^2\). In particular it follows that \(\mathbb{Z}[i]\) is a UFD.

33.1 Note. For \(\alpha, \beta \in \mathbb{Z}[i]\) we have

\[ N(\alpha \beta) = N(\alpha)N(\beta) \]

33.2 Proposition. An element \(\alpha \in \mathbb{Z}[i]\) is a unit iff \(N(\alpha) = 1\).

Proof. Exercise. \(\square\)

33.3 Corollary. The only units in \(\mathbb{Z}[i]\) are \(\pm 1\) and \(\pm i\).

33.4 Proposition. If \(p \in \mathbb{Z}\) is a prime number and for some \(\alpha \in \mathbb{Z}[i]\) we have \(N(\alpha) = p\) then \(\alpha\) is an irreducible element in \(\mathbb{Z}[i]\).

Proof. Assume that \(\alpha = \beta \gamma\). Then we have

\[ p = N(\alpha) = N(\beta)N(\gamma) \]

Since \(p\) is a prime number we get that either \(N(\beta) = 1\) or \(N(\gamma) = 1\), and so either \(\beta\) or \(\gamma\) is a unit in \(\mathbb{Z}[i]\). \(\square\)
33.5 Theorem. Let \( p \) be an odd prime. The following conditions are equivalent.

1) \( p = a^2 + b^2 \) for some \( a, b \in \mathbb{Z} \)
2) \( p \equiv 1 \pmod{4} \)

33.6 Lemma. If \( p \in \mathbb{Z} \) is a prime number and \( p \equiv 1 \pmod{4} \) then there is \( m \in \mathbb{Z} \) such that
\[
m^2 \equiv -1 \pmod{p}
\]

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 of Lemma 33.6. By Proposition 33.7 we have
\[(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p - 1)\mathbb{Z}\]
Since \( p \equiv 1 \pmod{4} \), thus \( 4 \mid (p - 1) \), and so the group \((\mathbb{Z}/p\mathbb{Z})^*\) has a cyclic subgroup of order 4. Let \( a \in \mathbb{Z}/p\mathbb{Z} \) be a generator of this subgroup. Then \( a^2 \) is an element of order 2 in \((\mathbb{Z}/p\mathbb{Z})^*\), so \( a^2 = -1 \).

Take the canonical epimorphism \( \pi: \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \) and let \( m \in \pi^{-1}(a) \). Then
\[
\pi(m^2) = a^2 = \pi(-1)
\]
which gives \( m^2 \equiv -1 \pmod{p} \) \(\square\)

Proof of Theorem 33.5.

1) \(\Rightarrow\) 2) Assume that \( p = a^2 + b^2 \). Since \( p \) is odd we can assume that \( a \) is even, \( a = 2m \), and \( b \) is odd, \( b = 2n + 1 \). Then we have
\[
p = (2m)^2 + (2n + 1)^2 = 4m^2 + 4n^2 + 4n + 1
\]
and so $p \equiv 1 \pmod{4}$.

2) $\Rightarrow$ 1) Since $p \equiv 1 \pmod{4}$ by Lemma 33.6 there exists $m \in \mathbb{Z}$ such that $p \mid (m^2 + 1)$. In $\mathbb{Z}[i]$ we have

$$m^2 + 1 = (m + i)(m - i)$$

Therefore in $\mathbb{Z}[i]$ we have $p \mid (m + i)(m - i)$. On the other hand $p \nmid (m \pm i)$ since otherwise for some $a, b \in \mathbb{Z}$ we would have

$$m \pm i = p(a + bi) = pa + pbi$$

and so $pb = \pm 1$ which is impossible.

As a consequence we obtain that $p$ is not a prime element in $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a UFD, prime elements in $\mathbb{Z}[i]$ coincide with irreducible elements and so $p$ is not irreducible. Therefore

$$p = \alpha \beta$$

for some non-units $\alpha, \beta \in \mathbb{Z}[i]$. We have

$$p^2 = N(p) = N(\alpha)N(\beta)$$

By Lemma 33.2 we have $N(\alpha) \neq 1 \neq N(\beta)$ so $N(\alpha) = N(\beta) = p$. Therefore, if $\alpha = a + bi$ then $p = a^2 + b^2$. \hfill \Box

33.8 Note.

1) One can use factorization in $\mathbb{Z}[i]$ to show that, in general, a positive integer $n$ is a sum of two squares iff $n$ is of the form

$$n = 2^k p_1^{m_1} \cdots p_r^{m_r} q_1^{2n_1} \cdots q_s^{2n_s}$$

where $k, m_i, n_j \geq 0$, and $p_i, q_j$ are prime numbers such that $p_i \equiv 1 \pmod{4}$ and $q_j \equiv 3 \pmod{4}$.

2) The ring $\mathbb{Z}[i]$ can be also used to describe all Pythagorean triples, e.i. triples of integers $(x, y, z)$ that satisfy the equation $x^2 + y^2 = z^2$. 

132
34 Application: Fermat’s Last Theorem

34.1 Fermat’s Last Theorem.

For \( n \geq 3 \) there are no integers \( x, y, z > 0 \) such that \( x^n + y^n = z^n \).

Kummer’s idea of the proof.

1) It is enough to show that \( x^n + y^n = z^n \) has no integral solutions for \( n = 4 \) and for \( n = p \) where \( p \) is an odd prime. Indeed, if \( n \geq 3 \) is any integer then \( n = mk \) where either \( k = 4 \) or \( k \) is an odd prime, and if \( x = a, y = b, z = c \) would be a solution of

\[
x^n + y^n = z^n
\]

then \( x = a^m, y = b^m, z = c^m \) would be a solution of

\[
x^k + y^k = z^k
\]

2) The case \( m = 4 \) was proved by Fermat.

3) Take an odd prime \( p \). Let \( \zeta = e^{2\pi i/p} \) be a \( p \)th primitive root of 1, and let \( \mathbb{Z}[\zeta] \) be the smallest subring of \( \mathbb{C} \) that contains \( \zeta \).

For any \( x, y \in \mathbb{Z} \) we have a factorization in \( \mathbb{Z}[\zeta] \):

\[
x^p + y^p = \prod_{i=0}^{p-1} (x + \zeta^i y)
\]

Therefore, if \( x^p + y^p = z^p \) then in \( \mathbb{Z}[\zeta] \) we have

\[
z^p = \prod_{i=0}^{p-1} (x + \zeta^i y)
\]

Assuming that \( \mathbb{Z}[\zeta] \) is a UFD we can compare these factorizations and try to get a contradiction.

Problem. For some values of \( p \) (e.g. \( p = 23 \)) the ring \( \mathbb{Z}[\zeta] \) is not a UFD.
35 Greatest common divisor

35.1 Definition. Let $R$ be a ring and let $a_1, \ldots, a_n \in R$. We say that $b \in R$ is a greatest common divisor of $a_1, \ldots, a_n$ if

1) $b | a_i$ for $i = 1, \ldots, n$
2) if $c | a_i$ for $i = 1, \ldots, n$ then $c | b.$

In such case we write $b \sim \gcd(a_1, \ldots, a_n)$.

35.2 Note.

1) If $b$ is a greatest common divisor of $a_1, \ldots, a_n$ and $b' \sim b$ then $b'$ is also a greatest common divisor of $a_1, \ldots, a_n$.

2) In general $\gcd(a_1, \ldots, a_n)$ need not exists. E.g. $\gcd(9, 3(2 + \sqrt{5}i))$ does not exist in $\mathbb{Z}[\sqrt{-5}]$.

35.3 Theorem. If $R$ is a UFD then $\gcd(a_1, \ldots, a_n)$ exists for any $a_1, \ldots, a_n$.

35.4 Lemma. If $R$ is a ring such that $\gcd(a_1, a_2)$ exists for any $a_1, a_2 \in R$ then $\gcd(a_1, \ldots, a_n)$ exists for any $a_1, \ldots, a_n \in R$.

Proof. Check:

$$\gcd(a_1, \ldots, a_n) \sim \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n)$$

Proof of Theorem 35.3. Let $a, b \in R$. By Lemma 35.4 it is enough to show that $\gcd(a, b)$ exists.
If \( a = 0 \) then \( \gcd(a, b) \sim b \) (check!).

If \( a \) is a unit then \( \gcd(a, b) \sim a \) (check!).

Therefore we can assume that \( a, b \) are non-zero, non-unit elements of \( R \). Since \( R \) is a UFD in such case we have

\[
a = u c_1^{k_1} c_2^{k_2} \cdots c_m^{k_m}, \quad b = v c_1^{l_1} c_2^{l_2} \cdots c_m^{l_m}
\]

where \( u, v \) are units, \( c_1, \ldots, c_m \) are distinct irreducible elements, and \( k_i, l_i \geq 0 \).

Check: we have

\[
\gcd(a, b) \sim c_1^{n_1} c_2^{n_2} \cdots c_m^{n_m}
\]

where \( n_i = \min\{k_i, l_i\} \) for \( i = 1, \ldots, m \). □

35.5 Definition. Let \( R \) be a ring. Elements \( a_1, \ldots, a_n \in R \) are relatively prime if \( \gcd(a_1, \ldots, a_n) \sim 1 \).

35.6 Note.

1) The elements \( a_1, \ldots, a_n \) are relatively prime iff every common divisor of \( a_1, \ldots, a_n \) is a unit (check!).

2) If \( R \) is a UFD, \( a, b, c \in R \), \( \gcd(a, b) \sim 1 \) and \( a \mid bc \) then \( a \mid c \) (check!).