Generalization of Unique Factorization and Its Application

Dr. Kundan Kumar
N.N.S.+2 School, Mansurchak, Begusarai.

ABSTRACT

In this paper our main focus is on a different property of unique factorization domain (UFD) which does not require the domain to be atomic. We define an integral domain R to be a generalized unique factorization domain (GUFD) if every nonzero nonunit of R is expressable as a finite product of mutually coprime prime quanta. The purpose of this paper is to study the generalization of unique factorization domain and its application to solve Diophantine equations.

Keywords: - generalization, diophantine, irreducible, domain Gaussian, Associate

Introduction

Let R be an integral domain. Now R is usually defined to be a unique factorization domain (UFD) if every nonzero, nonunit element of R has a factorization into irreducible elements (we often call an irreducible element an atom) and any two such factorizations are unique up to associates and order of the factors. There are many characterizations of UFD's. For example it is well known that the following conditions are all equivalent to R being a UFD.

1. Every nonzero nonunit of R is a product of primes.
2. Every nonzero prime ideal of R contains a nonzero prime element, and
3. R is Krull domain with divisor class group Cl (R) = 0.
Some properties of prime quanta:

**Propostion. 1.** Let R be an integral domain.

(1) Any nonunit factor of a prime quantum q is a prime quantum (Similar to q).

(2) Any power of a prime quantum q is a prime quantum (similar to q).

(3) If q₁ and q₂ are similar prime quanta, then q₁ q₂ is a prime quantum (similar to q₁ and q₂). Consequently, q₁|q₂ or q₂| q₁.

(4) Similarity of prime quanta is an equivalence relation.

**PROOF.** – (1) Let q be a prime quantum. Suppose that q' | q, and r/q' where r is a nonunit, then r/q, so there is an n ≥ 1 with q|rⁿ, and hence q'| rⁿ since q'|q. So Q₁ holds. Suppose that r|q'n and s|qⁿ. Then r|qⁿ and s|qⁿ, So r|s or s|r. So Q₂ Holds. Since any factor of a completely primal element is completely primal, Q₃ holds for q'.

(2) Let qⁿ be a power of the prime quantum q. Certainly qⁿ satisfies Q₂ and Q₃. Suppose that r|qⁿ. Now r|qⁿ and q|qⁿ, so by Q₂ applied to q, either r|q or q|r. In the first case, Q₁ applied to q gives that q|rᵐ for some m ≥ 1, and hence qⁿ|rᵐn, while in the second case qⁿ|rⁿ. Thus Q₁ holds.

(3) Since q₁ and q₂ are similar prime quanta, they have a nonunit common factor d. By (1), d is a prime quantum. Now d|q₁ and d|q₂ gives q₁|q₁n₁ and q₂|dⁿ₂ for some n₁, n₂ ≥ 1. Hence q₁q₂|dn³+nm. By (2), dn³+nm is a prime quantum and hence by (1) so is q₁q₂. The last statement is immediate since q₁|q₂ and q₂|q₁q₂.

(4) We only verify the transitive property. If q₁ and q₂ are similar prime quanta and q₂ and q₃ are similar prime quanta, then q₁q₂
and $q_2q_3$ are prime quanta which are similar. Hence $q_1q_2|q_2q_3$ or $q_2q_3|q_1q_2$: so $q_1|q_3$ or $q_3|q_1$. Thus $q_1$ and $q_3$ are similar.

**PROPOSITION 2.-** Let $R$ be an integral domain and $p,q,r,a,b \in R$.

1. If $q$ is a prime quantum, $q|ab$, and $(q,a)=1$, then $q|b$.
2. If $q$ is a prime quantum, $q|ab$, and $(a,b)=1$, then $q|a$ or $q|b$.
3. If $p,q,r$ are prime quanta with $(q,p)=1$ and $(r,p)=1$, then $(qr,p)=1$.

**PROOF.-**  
1. Since $q|ab$ and $q$ is completely primal, $q=q_1q_2$, where $q_1|a$ and $q_2|b$. Since $(q,a)=1$, $q_1$ is a unit, So $q|b$.

2. Since $q|ab$ and $q$ is completely primal, $q=q_2$, where $q_1|a$ and $q_2|b$. If $q_1$ or $q_2$ is a unit, then $q|b$ or $q|a$, respectively. So suppose that $q_1$ and $q_2$ are both nonunits. Then by Proposition 1 (1), (3) we can assume that $q_1|q_2$. Thus $q_1|a$ and $q_1|b$, so $(a,b) \neq 1$, a contradiction.

3. Let $d$ be a common factor or $qr$ and $p$. So $d$ is completely primal. Thus $d|qr$ gives $d=d_1d_2$, where $d_1|q$ and $d_2|r$. Then $d_1|q$ and $d_1|p$, so $(q,p)=1$ forces $d_1$ to be a unit. Likewise, $d_2$ is a unit Hence $d=d_1a_2$ is a unit.

**PROPOSITION 3.-** Let $R$ be an integral domain.

1. Let $q$ be a prime quantum. Then $P(q)=\{r \in R|(r,q) \neq 1\}$ is a prime ideal or $R$ and $(q)$ is $P$-primary.

2. Two prime quanta $q_1$ and $q_2$ are similar if and only if $P(q_1)=P(q_2)$.

3. Let $q$ be a prime quantum. Then $q'$ is a prime quantum similar to $q$ if and only if $(q')$ is $P(q)$- primary.

**PROOF.-** (1) We first show that $P(q)$ is an ideal. Let $x, y \in P (q)$. We show that $x+y \in P(q)$. We can assume that $x,y \neq 0$. Let $x_1$ (resp., $y_1$) be a nonunit common factor of $x$ (resp., $y$) and $q$. By Proposition 1 (1), (4), $x_1$ and $y_1$ are
similar prime quanta and thus by proposition 1 (3), \(x_1|y_1\) or \(y_1|x_1\), say \(x_1|y_1\). So \(x_1|(x+y)\) and \(x_1|q\), and hence \((x+y,q) \neq 1\), so \(x+y \in P(q)\). If \((r,q) \neq 1\), then \((rs,q) \neq 1\); so \(P(q)\) is an ideal. We next show that \(P(q)\) is prime. Suppose that \(xy \in P(q)\), so \((xy,q) \neq 1\). Let \(d\) be a nonunit common factor of \(xy\) and \(q\). By Q3, \(d=d_1d_2\), where \(d_1|x\) and \(d_2|y\). Since \(d\) is a nonunit, at least one of \(d_1\) or \(d_2\) must be a nonunit, say \(d_1\). But then \(d_1\) is a nonunit common divisor of \(x\) and \(q\), so \((x,q) \neq 1\), and hence \(x \in p(q)\). So \(P(q)\) is a prime ideal. Let \(0 \neq r \in P(q)\). Then there is a monunit \(d\) with \(d|r\) and \(d|q\). By Q1, there is a natural number \(n\) with \(q|d^n\), and hence \(q|r^n\). So \(r^n \in (q)\), and hence \(\sqrt(q) = P(q)\). and suppose that \(a \in P\). Then

\[(a,q) = 1\], so by Proposition 2 (1), \(q|ab\) gives \(q|b\). Thus \((q)\) is \(P(q)\)-primary.

(2) Suppose that \(q_1\) and \(q_2\) are prime quanta with \(P(q_1) = P(q_2)\). Now \(q_1 \in P(q_2)\neq 1\), that is, \(q_1\) and \(q_2\) are similar. Conversely, suppose that \(q_1\) and \(q_2\) are similar prime quanta. Then \((q_1,q_2) \neq 1\), so \(q_1 \in P(q_2)\) and hence \(P(q_2) = \sqrt(q_1) \subseteq P(q_2)\). Reversing the roles of \(q_1\) and \(q_2\) gives \(P(q_2) \subseteq P(q_1)\); so \(P(q_1) = P(q_2)\).

(3) If \(q\) is a prime quantum similar to \(q_1\) then by (1), \((q')\) is \(P(q')\)-Primary and by (2), \(P(q') = P(q)\), so \((q')\) is \(P(q)\)-primary. Conversely, suppose that \((q')\) is \(P(q)\)-primary. Then \(q' \in \sqrt(q') = P(q) = \sqrt(q)\), so \(q'|qm\) for some natural number \(n\). By Proposition 1 (2) and (1), \(q'\) is a prime quantum. Since \(P(q') \sqrt(q') = P(q)\), \(qn\) is similar to \(q\).

If \(p\) is a nonzero prime element of an integral domain, then \(p^n\) is a prime quantum, and if a \(q\) is a prime quantum then \(q\) is primary. However, if \(V\) is a rank-one nondiscrete valuation domain, then each nonzero nonunit of \(V\) is a prime quantum which is not a prime poer. Hence a rank-
one nondiscrete valuation domain is a GUFD which is not a UFD. A valuation domain is a GUFD if any only if it has Krull dimension one. Also, a primary element need not be a prime quantum. For let (R,M) be a one-dimensional quasilocal domain that is not a valuation domain. Then each 0 ≠ q ∈ M is M-primary, but q is not a prime quantum (if 0 ≠ r, s ∈ R, then r|q^n and s|q^n for sufficiently large n, and hence if q were a prime quantum we would have r|s or s|r, and thus R would be a valuation domain). In fact, a one-dimensional quasilocal domain is a GUFD if and only if it is a valuation domain.

Some consequence of unique factorization

Unique factorization helps to solve many Diophantine equations. Some examples are –

(1) The Gaussian field K(√-1)
(2) The field K(√-2)
(3) The field K(√-11)

The Gaussian fields K(√-i)

The equation \( y^2 = x^3 - 1 \) has only the solution \( y=0, x=1 \)

Proof: if the given equation has a solution then \( x^3 - 1 = 0 \) or 1 or 4 (mod 8). If \( x \) were even, then \( x^3 - 1 = 0 \) or 1 or 4 (mod 8) which is impossible. So, \( x \) must \( K(\sqrt{-1}) \) is Euclidean and so has unique factorization. Write (1.1) as

\[ y^2 + 1 = x^3 \]

or \((y+i)(y-i) = x^3\)

The factors on the left side are relatively prime; for any common divisor would divide their difference \( 2i \) (\( i \) being a unit), 2 is not a divisor of \( x^3 \) as \( x \) is odd. Then on recalling that the units in \( K(\sqrt{-1}) \) are \( \pm 1, \pm i \).

We have
\[ y+i = \pm \sigma^3 \text{ or } i \sigma^3 \text{ and } x = N(\sigma) \] for some algebraic integers \( \sigma \) in the field. Since the field is Gaussian, we have \( \sigma = a + ib \) where \( a, b \) are rational integers.

We can omit the minus sign, since \(-1\) can be incorporated in the cube. Then

\[
\begin{align*}
y+i &= (a+ib)^3 \text{ or } i(a+ib)^3 \\
&= a^3 + 3a^2bi - 3ab^2i + b^3i \\
&= a^3i - 3a^2b - 3ab^2i + b^3
\end{align*}
\]

Equating the coefficient of \( i \), we get

\[ 1 = 3a^2b - b^3 = b(3a^2 - b^2) \]

or \[ a^3 - 3a^2b = a(a^2 - 3b^2) \]

Whence \( b = -1, a = 0, a = 1, b = 0 \)

and so \( x = N(a+ib) = (a^2 + b^2) = 1 \)

the result follows.

The same method can be applied for any powers of \( x \) in (1.1).

**Conclusions:**

Each of the characterizations of UFD's or properties of UFD's (Such as every pair of elements having a GCD) is subject to various generalization. The property of unique factorization into irreducibles can be generalized in a number of ways: for a survey of factorization properties weaker than unique factorization. Instead of factoring elements into prime elements, we can consider factorizations studying Krull domain \( R \) with \( \text{Cl} (R) = 0 \) can study Krull domain \( R \) with \( \text{Cl} (R) \) torsion. Unique factorization is applicable in almost every field of mathematics and to solve Diophantine equations.

**References:**


