Introduction to Factorization Theory

Vadim Ponomarenko

Department of Mathematics and Statistics
San Diego State University

REUT Orientation June 23, 2008

http://www-rohan.sdsu.edu/~vadim/factorization.pdf

Semigroups

- A semigroup is a set S together with a binary operation that is closed and associative.
- Other things you might like:
  neutral element, inverses, commutativity, a second operation, candy...
- Familiar examples: $(\mathbb{N}_0, +), (\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{N}, \times), (\mathbb{Z}, \times)$

Semigroups

- A semigroup is a set S together with a binary operation that is closed and associative.
- Other things you might like:
  neutral element, inverses, commutativity, a second operation, candy...
- Familiar examples: $(\mathbb{N}_0, +), (\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{N}, \times), (\mathbb{Z}, \times)$

Semigroups

- A semigroup is a set S together with a binary operation that is closed and associative.
- Other things you might like:
  neutral element, inverses, commutativity, a second operation, candy...
- Familiar examples: $(\mathbb{N}_0, +), (\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{N}, \times), (\mathbb{Z}, \times)$

Semigroups

- A semigroup is a set S together with a binary operation that is closed and associative.
- Other things you might like:
  neutral element, inverses, commutativity, a second operation, candy...
- Familiar examples: $(\mathbb{N}_0, +), (\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{N}, \times), (\mathbb{Z}, \times)$

Semigroups

- A semigroup is a set S together with a binary operation that is closed and associative.
- Other things you might like:

  neutral element, inverses, commutativity, a second operation, candy...
- Familiar examples: $(\mathbb{N}_0, +), (\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{N}, \times), (\mathbb{Z}, \times)$

Semigroups

- A semigroup is a set S together with a binary operation that is closed and associative.
- Other things you might like:

  neutral element, inverses, commutativity, a second operation, candy...
- Familiar examples: $(\mathbb{N}_0, +), (\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{N}, \times), (\mathbb{Z}, \times)$

Semigroups

- A semigroup is a set S together with a binary operation that is closed and associative.
- Other things you might like:

  neutral element, inverses, commutativity, a second operation, candy. . .
- Familiar examples: $(\mathbb{N}_0, +), (\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{N}, \times), (\mathbb{Z}, \times)$

Units

- A unit is a semigroup element that has an inverse.
- Note 1: If no neutral element, then no units.
- Note 2: If every element is a unit, then it's a group.
- Familiar examples: $(\mathbb{N}_0, +), (\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{N}, \times), (\mathbb{Z}, \times)$

Units

- A unit is a semigroup element that has an inverse.

- Note 1: If no neutral element, then no units.
- Note 2: If every element is a unit, then it's a group.

- Familiar examples: $(\mathbb{N}_0, +), (\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{N}, \times), (\mathbb{Z}, \times)$

Units

- A unit is a semigroup element that has an inverse.
- Note 1: If no neutral element, then no units.
- Note 2: If every element is a unit, then it's a group.
- Familiar examples: $(\mathbb{N}_0, +), (\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{N}, \times), (\mathbb{Z}, \times)$

Atoms

- An atom is a semigroup element that cannot be factored in a nontrivial way.

  Note: We can always factor x by tossing units around: $x = u(u^{-1}x)$.

- More precisely, a is an atom if $a = bc$ implies that either b or c is a unit, but not both (units can't be atoms).

- Familiar examples: $(\mathbb{N}_0, +), (\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{N}, \times), (\mathbb{Z}, \times)$

Atoms

- An atom is a semigroup element that cannot be factored in a nontrivial way.

  Note: We can always factor x by tossing units around: $x = u(u^{-1}x)$.

- More precisely, a is an atom if $a = bc$ implies that either b or c is a unit, but not both (units can't be atoms).

- Familiar examples: $(\mathbb{N}_0, +), (\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{N}, \times), (\mathbb{Z}, \times)$

Atoms

- An atom is a semigroup element that cannot be factored in a nontrivial way.

  Note: We can always factor x by tossing units around: $x = u(u^{-1}x)$.

- More precisely, a is an atom if $a = bc$ implies that either b or c is a unit, but not both (units can't be atoms).

- Familiar examples: $(\mathbb{N}_0, +), (\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{N}, \times), (\mathbb{Z}, \times)$

Primes

- a is a prime if $a|bc$ implies that either $a|b$ or $a|c$.
- All primes are atoms. In a UFD, all atoms are prime. Not in general! (examples to come)
- Factorization into primes is unique, up to order and units.
- Factorization into atoms is what we're interested in.

Primes

- a is a prime if $a|bc$ implies that either $a|b$ or $a|c$.
- All primes are atoms. In a UFD, all atoms are prime.
  Not in general! (examples to come)
- Factorization into primes is unique, up to order and units.
- Factorization into atoms is what we're interested in.

Primes

- a is a prime if $a|bc$ implies that either $a|b$ or $a|c$.
- All primes are atoms. In a UFD, all atoms are prime. Not in general! (examples to come)
- Factorization into primes is unique, up to order and units.
- Factorization into atoms is what we're interested in.

Example 1

- Let S denote the set of words built out of lower-case letters. The operation $\cdot$ is concatenation, e.g. $ab \cdot xyz = abxyz$
- Not very interesting structure. . .

Example 1

- Let S denote the set of words built out of lower-case letters. The operation $\cdot$ is concatenation, e.g. $ab \cdot xyz = abxyz$
- Not very interesting structure...

Example 2

- Let S denote the set of nonnegative rational numbers, under addition.
- Surprising structure, dead end.

Example 2

- Let S denote the set of nonnegative rational numbers, under addition.
- Surprising structure, dead end.

Example 3

- Let $S = < {}^1/_p \mid p \text{ prime} >$, under addition.
- S contains ${}^5/_6$ but not ${}^1/_6$ (consider primes in denom.)
- $1 = {}^1/_2 + {}^1/_2 = {}^1/_3 + {}^1/_3 + {}^1/_3$

Example 3

- Let $S = < 1/p \mid p \text{ prime} >$, under addition.
- S contains $5/6$ but not $1/6$ (consider primes in denom.)
- $1 = 1/2 + 1/2 = 1/3 + 1/3 + 1/3$

Example 3

- Let $S = < 1/p \mid p$ prime $>$, under addition.
- S contains $5/6$ but not $1/6$ (consider primes in denom.)
- $1 = 1/2 + 1/2 = 1/3 + 1/3 + 1/3$

Example 4

- Let S be the set of positive even integers, under $\times$.
- If $x|y$ in S, then $x|y$ in $\mathbb{Z}$, but not in reverse
  For example, 2 does not divide 6.
- $36 = 6 \times 6 = 2 \times 18$
  "half-factorial"

Example 4

- Let S be the set of positive even integers, under $\times$.
- If $x|y$ in S, then $x|y$ in $\mathbb{Z}$, but not in reverse
  For example, 2 does not divide 6.
- $36 = 6 \times 6 = 2 \times 18$
  "half-factorial"

Example 4

- Let S be the set of positive even integers, under $\times$.
- If $x|y$ in S, then $x|y$ in $\mathbb{Z}$, but not in reverse
  For example, 2 does not divide 6.
- $36 = 6 \times 6 = 2 \times 18$
  "half-factorial"

Example 5

- Let S be the set of positive composite integers, under $\times$.
  Note: 4 does not divide 8.
- $64 = 4 \times 4 \times 4 = 8 \times 8$

Example 5

- Let S be the set of positive composite integers, under $\times$.
  Note: 4 does not divide 8.
- $64 = 4 \times 4 \times 4 = 8 \times 8$

Example 6

- Let S be the set of positive integers congruent to 1 modulo 4, under $\times$.

  i.e. $\{1, 5, 9, 13, 17, 21, 25, 29, 33, \ldots\}$ "Hilbert semigroup"

- Two kinds of atoms: p and qr

  $(3 \times 7) \times (3 \times 11) = (3 \times 3) \times (7 \times 11)$

San Diego State University

Example 6

- Let S be the set of positive integers congruent to 1 modulo 4, under $\times$.

  i.e. $\{1, 5, 9, 13, 17, 21, 25, 29, 33, \ldots\}$ "Hilbert semigroup"

- Two kinds of atoms: p and qr

  $(3 \times 7) \times (3 \times 11) = (3 \times 3) \times (7 \times 11)$

Example 7

- Let $S = \mathbb{N} \setminus \{1, 2, 4\} = \{3, 5, 6, 7, 8, 9, 10, 11, \ldots\}$, under $+$. "Numerical semigroup"
- Three atoms.
- $15 = 5 + 5 + 5 = 3 + 3 + 3 + 3 + 3$

Example 7

- Let $S = \mathbb{N} \setminus \{1, 2, 4\} = \{3, 5, 6, 7, 8, 9, 10, 11, \ldots\}$, under $+$. "Numerical semigroup"
- Three atoms.
- $15 = 5 + 5 + 5 = 3 + 3 + 3 + 3 + 3$

Example 7

- Let $S = \mathbb{N} \setminus \{1, 2, 4\} = \{3, 5, 6, 7, 8, 9, 10, 11, \ldots\}$, under $+$.
  "Numerical semigroup"
- Three atoms.
- $15 = 5 + 5 + 5 = 3 + 3 + 3 + 3 + 3$

Example 8

- Let $S = \mathbb{Z}[\sqrt{-7}]$, under $\times$.
  "Quadratic Number Field"
- $N(a + b\sqrt{-7}) = a^2 + 7b^2$, multiplicative
- ± 2 $[N = 4]$, $\pm 1 \pm \sqrt{-7}$ $[N = 8]$, $\pm 3 \pm \sqrt{-7}$ $[N = 16]$

  $2 \times 2 \times 2 = (1 + \sqrt{-7}) \times (1 - \sqrt{-7})$ $[64 = 4^3 = 8^2]$
  $2 \times (-3 + \sqrt{-7}) = (1 + \sqrt{-7}) \times (1 + \sqrt{-7})$
  $[64 = 4 \times 16 = 8^2]$

Example 8

- Let $S = \mathbb{Z}[\sqrt{-7}]$, under $\times$.
  "Quadratic Number Field"

- $N(a + b\sqrt{-7}) = a^2 + 7b^2$, multiplicative

- ± 2 $[N = 4]$, $\pm 1 \pm \sqrt{-7}$ $[N = 8]$, $\pm 3 \pm \sqrt{-7}$ $[N = 16]$

  $2 \times 2 \times 2 = (1 + \sqrt{-7}) \times (1 - \sqrt{-7})$ $[64 = 4^3 = 8^2]$
  $2 \times (-3 + \sqrt{-7}) = (1 + \sqrt{-7}) \times (1 + \sqrt{-7})$
  $[64 = 4 \times 16 = 8^2]$

Example 8

- Let $S = \mathbb{Z}[\sqrt{-7}]$, under $\times$.
  "Quadratic Number Field"
- $N(a + b\sqrt{-7}) = a^2 + 7b^2$, multiplicative
- ± 2 $[N = 4]$, $\pm 1 \pm \sqrt{-7}$ $[N = 8]$, $\pm 3 \pm \sqrt{-7}$ $[N = 16]$

  $2 \times 2 \times 2 = (1 + \sqrt{-7}) \times (1 - \sqrt{-7})$ $[64 = 4^3 = 8^2]$
  $2 \times (-3 + \sqrt{-7}) = (1 + \sqrt{-7}) \times (1 + \sqrt{-7})$
  $[64 = 4 \times 16 = 8^2]$

Example 8

- Let $S = \mathbb{Z}[\sqrt{-7}]$, under $\times$.
  "Quadratic Number Field"

- $N(a + b\sqrt{-7}) = a^2 + 7b^2$, multiplicative

- $\pm 2\ [N = 4],\quad \pm 1 \pm \sqrt{-7}\ [N = 8],\quad \pm 3 \pm \sqrt{-7}\ [N = 16]$

  $2 \times 2 \times 2 = (1 + \sqrt{-7}) \times (1 - \sqrt{-7})\ \ [64 = 4^3 = 8^2]$
  $2 \times (-3 + \sqrt{-7}) = (1 + \sqrt{-7}) \times (1 + \sqrt{-7})$
  $[64 = 4 \times 16 = 8^2]$

What does factorization theory study?

- What is the structure of factorization into atoms?
- unique? “factorial”
- always the same length? “half-factorial”
- what possible lengths can we get?
- how many factorizations can we get?