Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Abstract Algebra, Lecture 1

Overview of the course

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Linköping, fall 2019

Lecture notes availabe at course homepage
`http://courses.mai.liu.se/GU/TATA55/`

Summary

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Summary

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

The integers

- Divisibility
- Primes, unique factorization
- Greatest common divisor
- Division with remainder
- Euclidean algorithm, Bezout
- Diophantine equations
- Congruences

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Binary operations

- Examples
- Associativity
- Semigroups, monoids
- Maps from a finite set to itself
- Free monoid
- Units, inverses

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Groups

- Definition
- S_X
- Inverse, units, cancellation, linear equations
- Abelian groups
- Cyclic groups
- Direct sums
- Subgroups
- Cayley (multiplication) table
- Symmetry groups, dihedral groups

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Cyclic groups

- Power laws (exponents)
- $\langle g \rangle$
- Examples: the circle, $\mathbb{Z}$, $\mathbb{Z}_n$, U_n.
- Order of an element, definition
- Subgroups of cyclic groups
- Order of power of elments, and of products of elements
- Classification of cyclic groups
- $\langle S \rangle$
- Free groups (brief overview)
- U_n, primitive roots

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Permutation groups

- S_X
- S_n
- Representations of permutations: graphs, matrices, one or two row tables
- Permutation statistics
- The sign of a permutation, the alternating group
- Disjoint cycle factorization
- Products of transpositions
- Cycle type
- Permutation representation of a finite group
- Matrix representation

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Cosets

- Left and right cosets
- Examples, S_3, symmetry group of cube
- Lagrange's theorem
- Fermat's and Euler's theorems
- The size of HK
- Normal subgroups

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Direct products

- Exterior direct product
- Inner direct product
- Abelian groups: torsion subgroups, p-groups
- Structure theorem for finite abelian groups
- Exampels

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Homomorphisms

- Definitions, kernel
- Examples
- Congruence
- Quotient groups
- Isomorphism theorems
- Correspondence theorem
- Simple groups

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Group actions

- Definition
- Examples
- Orbits, stabilizers, fixed points
- Orbit-Stabilizer relation
- Burnside's lemma
- Class equation, center, centralizer, normalizer, conjugacy classes
- Sylow's theorems

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Ring theory

- Definition, simple properties
- Ideals, homomorphisms, quotients
- Ideal operations

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Polynomial rings

- Degree, division with reminder, gcd
- Ideal theory for polynomial rings, they are PIDs
- Unique factorization
- Quotients of polynomial rings

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Unique factorization domains

- Polynomial rings in several variables
- Gaussian integers

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Field extensions

- Simple extensions, algebraic extensions
- Degree of extension
- Splitting fields

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Finite fields

- Construction
- Uniqueness
- Multiplicative group is cyclic
- Applications: coding theory, LFSR,...