MATH 417

Iwan Duursma

January 19, 2022

Week 1 - Wednesday

Course outline

Math 417 Introduction to Abstract Algebra [43 hrs]

(a) Integers [4 hrs]

(b) Permutations [3hrs]

(c) Groups [10 hrs]

(d) Group actions [10 hrs]

(e) Rings [12 hrs]

(*) Exams and leeway [4hrs]

Text

Main text:

Fraleigh, A First Course in Abstract Algebra (7th edition)

With a few sections from:

Rotman, A First Course in Abstract Algebra (3rd edition)

Optional, not expected to be used:

Goodman, Algebra: Abstract and Concrete (free online)

Other:

Artin, Algebra (2nd edition)

Dummit and Foote, Abstract Algebra (3rd edition) (covers Math 500)

Rotman, Advanced Modern Algebra (2002 ed.) (covers Math 500)

Looking ahead at (c) Groups

$a * b$	$b = 1$	2	3	4	5	6	7	8	9	10	11	12
$a = 1$	1	2	3	4	5	6	7	8	9	10	11	12
2	2	1	4	3	7	8	5	6	12	11	10	9
3	3	4	1	2	8	7	6	5	10	9	12	11
4	4	3	2	1	6	5	8	7	11	12	9	10
5	5	6	7	8	9	10	11	12	1	2	3	4
6	6	5	8	7	11	12	9	10	4	3	2	1
7	7	8	5	6	12	11	10	9	2	1	4	3
8	8	7	6	5	10	9	12	11	3	4	1	2
9	9	10	11	12	1	2	3	4	5	6	7	8
10	10	9	12	11	3	4	1	2	8	7	6	5
11	11	12	9	10	4	3	2	1	6	5	8	7
12	12	11	10	9	2	1	4	3	7	8	5	6

Questions (Homework, due Monday 1/31)

1. Collect all pairs (a, b) with $a * b = 7$.

2.. Compute each of the following. What do you observe?

$$\begin{array}{ccc} (2*3)*7 & (7*2)*3 & (3*7)*2 \\ 7*(2*3) & 3*(7*2) & 2*(3*7) \end{array}$$

3. Find a subset $H \subset G$ of size four such that $a * b \in H$ for all $a, b \in H$.

4. Find all subsets $H \subset G$ of size three such that $a * b \in H$ for all $a, b \in H$.

5. For $a \in G$ define $\ell_a : G \to G$ as the function $\ell_a(x) = a * x$.
Determine the composition $\ell_4 \circ \ell_5 : G \to G$.

6. For $b \in G$ define $r_b : G \to G$ as the function $r_b(x) = x * b$.
Determine the composition $r_4 \circ r_5 : G \to G$.

First topic: (a) Integers [4hrs]

[Rotman-1.3-1.5]

The Integer division algorithm (p.35)

  optional: Euclidean algorithm (pp.43-45)

Greatest common divisor (pp.37-38)

Fundamental theorem of arithmetic (pp.53-55)

Congruence arithmetic (pp.57-59)

  optional: Application to RSA-cryptosystem (handout or homework)

Integer division algorithm

Theorem

Given integers a and b with $a \neq 0$,

there exist unique integers q and r with

$$b = qa + r \quad \text{and} \quad 0 \leq r < |a|.$$

Example

$a = 7$ and $b = 60$: $60 = 8 \cdot 7 + 4$ with $q = 8$ and $r = 4$.

$a = 7$ and $b = -60$: $-60 = (-9) \cdot 7 + 3$ with $q = -9$ and $r = 3$.

Greatest common divisor

Definition

The integer a divides the integer b, notation $a \mid b$,

if there exists an integer d with $b = d \cdot a$.

We also say a is a divisor of b or b is a multiple of a.

The integer c is a common divisor of a and b if $c \mid a$ and $c \mid b$.

For a and b not both zero, the greatest common divisor of a and b,

notation $\gcd(a, b)$, is the largest common divisor of a and b.

Example: $\gcd(120, 300) = 60$, $\gcd(119, 301) = ?$.

Euclidean algorithm

Lemma

Let $b = q \cdot a + r$. Then $\gcd(b, a) = \gcd(a, r)$.

Proof

The pair b, a has the same set of common divisors as the pair a, r.

To compute $\gcd(119, 301)$ we use the lemma repeatedly.

$$\begin{aligned}
301 &= 2 \cdot 119 + 63 \ : \ \gcd(301, 119) = \gcd(119, 63). \\
119 &= 1 \cdot 63 + 56 \ : \ \gcd(119, 63) = \gcd(63, 56). \\
63 &= 1 \cdot 56 + 7 \ : \ \gcd(63, 56) = \gcd(56, 7). \\
56 &= 8 \cdot 7 + 0 \ : \ \gcd(56, 7) = \gcd(7, 0) = 7.
\end{aligned}$$