Math 4281, Spring 2019: **Introduction to Modern Algebra**
– Syllabus –
Darij Grinberg, VinH 203B, dgrinber@umn.edu
last update: May 31, 2019

##
WARNING! You are reading the syllabus of a class that lies in the past. If you're looking for the current iteration of Math 4281, you are in the wrong place.
##

1. Time & Place

Lectures:	**Section 001:** MWF 9:05–9:55, Vincent Hall 211. **Section 002:** MWF 11:15–12:05, Vincent Hall 211.
Office hours:	Monday 14:35–15:35. Tuesday 10:00–11:00. Tuesday 12:00–13:00. Friday 14:30–15:00 (half an hour).

This class has a website: http://www.cip.ifi.lmu.de/~grinberg/t/19s/ and two Canvas boards:
Section 001: https://canvas.umn.edu/courses/99199.
Section 002: https://canvas.umn.edu/courses/99188.

Homework will usually be due on **Wednesday** (sometimes weekly, sometimes every other week) **at the beginning of class**. You can also submit your homework electronically via Canvas (see above) **provided that the problem set is submitted as 1 single PDF file**. See "Grading" and "Coursework" below for details.

Midterms (3 in total) are like homework, but they count for more, and collaboration is not allowed (see below for details). There will be **no final exam**.

2. Requirements

This is a pure mathematics class and relies heavily on proofs. You have to feel at home reading and writing mathematical proofs. You can catch up on this from:

- [LeLeMe] Eric Lehman, F. Thomson Leighton, Albert R. Meyer, *Mathematics for Computer Science*, https://courses.csail.mit.edu/6.042/spring18/mcs.pdf . (You should know the material from Chapters 1–5, minus the CS parts.)

- [Hammack] Richard Hammack, *Book of Proof*,
`http://www.people.vcu.edu/~rhammack/BookOfProof/`
- [Day] Martin V. Day, *An Introduction to Proofs and the Mathematical Vernacular*,
`https://www.math.vt.edu/people/day/ProofsBook/IPaMV.pdf` .

You should also know some linear algebra: Gaussian elimination, linear independence, vector spaces, dimension, rank of matrices. The more you know, the better. One of the best texts to learn linear algebra from is:

- [Hefferon] Jim Hefferon, *Linear Algebra*, 2017,
`http://joshua.smcvt.edu/linearalgebra/`

if you have the time for it (it is long and thorough). If not, make sure you know at least the topics named above. We won't start using linear algebra until a few weeks into this class.

3. Texts

3.1. required:

There is no required textbook if you attend class. I won't follow a text directly anyway. I will post lecture notes on the class website. These will not be as polished as a book, but will contain everything needed to do homeworks and midterms.

3.2. recommended:

Here are some good texts I know:[1]

- [Goodman] Frederick M. Goodman, *Algebra: Abstract and Concrete*, edition 2.6.
This is a long book going beyond what we will do in this class. We won't follow it directly either, but it has a lot of the material we care about.
- [Siksek] Samir Siksek, *Introduction to Abstract Algebra*, 2015.
This is probably the most amusing (though occasionally overdoing the goofiness) book on abstract algebra I've ever seen. It is also really good at motivating definitions.
- [Pinter] Charles C. Pinter, *A book of abstract algebra*, 2nd edition, Dover 2010.
The link goes to an ebook version that doesn't look very good, but you can get the original for less than $20.

[1] The bracketed names (such as "[Goodman]") are the abbreviations by which I will refer to the texts in class.

- [Armstrong] Drew Armstrong, *Abstract Algebra I*, 2018.
  (Click on "Course Notes" for the main text.) This is new and I haven't had much experience with it, but Armstrong is a good expositor. Note that this only goes until group theory.

On specific topics:

- [Conrad-Gauss] Keith Conrad, *The Gaussian integers*.
  This is a topic we'll spend some time with early on in this course. And Conrad is a really good writer; check out his expository papers for various other pieces of algebra.
- [Strickland] Neil Strickland, *Linear mathematics for applications*.
  Would you have guessed by the title that these lecture notes have one of the most rigorous treatments of determinants I've seen in the linear algebra literature?
- [Gallier-RSA] Jean Gallier, Jocelyn Quaintance, *Notes on Primality Testing And Public Key Cryptography, Part 1*.
  This contains most of the elementary number theory we'll be going through (modular arithmetic, RSA, groups), plus a lot that we won't (primality checking).

For the sake of completeness, here are links to some old editions of this class: Fall 2018, Spring 2018, Fall 2017, Spring 2017. Note that they were structured differently from mine and used different texts.

4. Contact

All material regarding the course (including homework) can be found on

`http://www.cip.ifi.lmu.de/~grinberg/t/19s/`

The best way to reach me is by email to `dgrinber@umn.edu` .

After I leave UMN (in Summer), the best way to reach me will be by email to `darijgrinberg@gmail.com` , and the class materials will migrate to `http://www.cip.ifi.lmu.de/~grinberg/t/19s/` .

5. Topics (tentative)

This is still far from finished and decided.

Topics marked with an * **may** be excluded. Topics marked with an ** probably **will** be excluded.

1. Introduction and motivating questions.

a) $n = x^2 + y^2$.

b) Algebraic vs. transcendental numbers; sums of algebraics.

c) Shamir's secret sharing scheme and the need for finite fields.

d) * Angle trisection, cube duplication, circle squaring.

e) * Solving degree-3 equations; higher orders.

2. Elementary number theory.

a) Divisibility.

b) Congruences mod n.

c) Division with remainder.

d) gcd, Bezout, Euclidean algorithm.

e) Primes and prime factorization.

f) Modular inverses & cancellation mod n.

g) Fermat's little theorem.

h) Euler's ϕ-function and its properties.

i) Chinese Remainder Theorem.

3. $\mathbb{Z}/n$.

a) Equivalence relations.

b) Equivalence classes and quotient sets.

c) $\mathbb{Z}/n$.

d) RSA and applications of the Chinese Remainder Theorem.

e) Primitive roots (no proofs).

4. Complex numbers and Gaussian integers.

a) Complex numbers (the very basics).

b) Gaussian integers (follow Keith Conrad).

c) $n = x^2 + y^2$ (follow Keith Conrad).

d) Finish with discussion of other quadratic and higher-order number rings.

5. Rings and fields I.

a) Define rings, commutative rings and fields.

b) Examples (but no structure or homomorphisms). Include $\mathbb{Z}/p$, $\mathbb{Z}[i]$, dual numbers, etc. Also $\mathbb{Z}\left[\sqrt[3]{2}\right]$, but note that just adding $\sqrt[3]{2}$ does not work.

c) General properties (e.g., finite sums).

6. Linear algebra.
   a) Modules and vector spaces.
   b) Linear algebra (crash course, following Hefferon? Charlier? Artin? whoever does it most slickly).
   c) Direct sums/products of vector spaces.
   d) Quotient vector spaces.
   e) Linear algebra over $\mathbb{Z}/p$.
   f) XOR as vector addition over $\mathbb{Z}/2$.
   g) Solve lights-out using $\mathbb{Z}/2$-linear algebra.
   h) What works and what fails over the base ring $\mathbb{Z}$? (Leave some harder stuff unproven.)
   i) * $\mathbb{Z}/26$ and affine ciphers as 2×2-matrices (follow Conrad).
   j) The Smith normal form over $\mathbb{Z}$, proven by merging Gaussian elimination with the Euclidean algorithm.
7. Permutations and determinants.
   a) Permutation basics (follow [detnotes]).
   b) Lengths and signs (follow [detnotes]).
   c) Cycles and transpositions (follow [detnotes]).
   d) Cycle decompositions (follow Loeh?).
   e) Determinants.
   f) Properties of determinants.
   g) $\det(AB)$.
   h) Adjugate matrices.
8. Groups.
   a) Definition of a group.
   b) Subgroups.
   c) Homomorphisms.
   d) Direct products.
9. Group actions. (Include necklace counting.)
10. Quotient groups and homomorphism theorems.
11. Rings.

a) Recalling the definition.
b) Subrings.
c) Ring homomorphisms.
d) Ideals and quotient rings.

12. Polynomials and their rings.
    a) Define formal power series.
    b) Define polynomials.
    c) Polynomials over a field as vector space.
    d) Division with remainder modulo monic (or invertible-LT) polynomial.
    e) Use as generating functions.
    f) Lucas's theorem reproved.
    g) Companion matrices.
    h) Cayley-Hamilton theorem.
    i) Application: sums/products of algebraic integers.
13. Fields.
14. Field extensions and angle trisection.
15. Finite fields. (Prove existence by counting irreducible polys.)
16. * Properties of rings (PID, UFD, etc.).
17. * Symmetric polynomials and the Fundamental Theorem.
18. * Galois theory introduction. (Apply to deg-3 maybe.)
19. * Modules and their basic applications. (Apply to algebraic integers again?)

6. Schedule (tentative)

The due dates with question marks are not set in stone.

week	**material**	**due**
Jan 23, 25		
Jan 28, 30, 1		
Feb 4, 6, 8		hw1
Feb 11, 13, 15		hw2
Feb 18, 20, 22		hw3
Feb 25, 27, 1		
Mar 4, 6, 8		MT1
Mar 11, 13, 15		hw4
Mar 18–24	*break*	
Mar 25, 27, 29		
Apr 1, 3, 5		hw5 (Mon)
Apr 8, 10, 12		MT2
Apr 15, 17, 19		hw6?
Apr 22, 24, 26		
Apr 29, 1, 3		MT3
May 5		

7. Grading

The grade will be computed based on three take-home **midterms** (totalling to **60%** of the final grade, each giving 20% of the final grade) and somewhere between 5 and 10 **homework sets** (totalling to **40%** of the final grade, but the lowest score will be dropped).

Points will be deducted if your proofs are ambiguously worded or otherwise hard to understand. Writing readable arguments is part of mathematics; you can learn this from the references in the "Requirements" section above and you can practice it on math.stackexchange.

8. Coursework

Collaboration on homework is allowed, as long as:

- you **write** up the solutions autonomously and in your own words (in particular, this means that you have to **understand** them), and
- you **list the names of your collaborators** (there will be no penalties for collaboration, so you don't lose anything doing this!).

On the midterms, you have to **work alone** (you can **read** whatever you want, but you must **not contact** anyone about the midterm problems[2]; in particular, you must **not ask** them on the internet).

Homework and midterms should be submitted either in person during class, or via Canvas.

If you handwrite your solutions:

- Make sure that your writing is legible.
- If you submit your solutions by email, make sure that your submission is **1 single PDF file** for a given homework set (not many 1-page JPGs!). Double-check that your scans are readable and aren't missing any relevant text near the margins.

If you type up your solutions:

- Again, make sure that your submission is **1 single PDF file** for a given homework set.
- Double-check that your text doesn't go over the margins (something that often happens when using LaTeX). If something is not on the page, we cannot grade it...

Calculators and computer algebra systems may be used, but are not necessary (and you are responsible for any resulting errors).

Late homework or late midterms are **not accepted** in any situation; if you are not finished, submit whatever you have before the deadline. If you want to update your submission, you can do so (before the deadline!) by sending me an email that includes the whole updated submission (not just the parts you want changed).

See also the following university policies:

- https://policy.umn.edu/education/gradingtranscripts
- https://policy.umn.edu/research/academicmisconduct

[2] It is OK to contact **me** with questions.