Commutative Algebra MAS439
Lecture 1

Paul Johnson
paul.johnson@sheffield.ac.uk
Hicks J06b

September 28th

Assessment is entirely via problem sets

- Problems are due *every* Wednesday at the *beginning* of class
- Each semester, the two lowest scores (out of ten) can be dropped
- You are encouraged, but not required, to write your solutions in LaTeX
- You are encouraged, but not required, to work together in groups of 2 or 3

Wait, groupwork?! How does that work?

- Each group member writes up and hands in their own solution
- If you do work in groups, please write who you worked with on every assignment

What is/isn't allowed:

- You should NOT be writing up identical solutions, or even writing up your solutions sitting together.
- Rather, in the group digest what the problem is actually asking, come up with an informal / pseudo-formal solution
- LATER, on your own, write up the full, rigorous solution

Rigour and intuition, proof and understanding

- Mathematics is all in our heads. Giving formal definitions and rigorous proofs make sure we're not just making up nonsense
- However, humans don't think very well in this rigorous structure. We have our own intuitive pictures
- Most of the work of doing mathematics is translating back and forth between rigorous and intuitive modes.

The *Oral tradition* in mathematics

Mathematics is written down in full rigor, but informal discussion of "how to think about this" or "what's really going on" aren't written down

- Terry Tao, There's more to mathematics than rigour and proofs
- William Thurston, On proof and progress in mathematics

Lectures and Notes

- Primary text: Tom Bridgeland's notes (rigor)
- I won't provide lecture notes (intuition)

Weekly webpage

- Terse description of what was covered in lecture
- Slides
- Problem set
- Feedback on problem set?
- Comment section

Please *Please* read Tom's notes

I will be assuming you are

The first 3-4 weeks should be somewhat review

MAS220 Syllabus from 2014

conjugacy classes. Conjugation in $GL_2(\mathbb{R})$, O_2 and S_n. The class equation, application to p-groups.

3. Group Homomorphisms

(3 lectures)

Homomorphisms, image subgroups and kernel normal subgroups. First Isomorphism Theorem for groups. Representations, Buckminsterfullerene.

4. Introduction to Rings

(3 lectures)

Basic laws of arithmetic of natural numbers. Invention of the integers, rational numbers, real numbers and complex numbers. Ring axioms. Commutative and non-commutative rings. Division rings, fields. Hamilton's quaternions, **H**. Polynomial rings, matrix rings, Weyl algebra.

5. Ring Homomorphisms

(4 lectures)

Subrings. Norm and determinant as group homomorphisms. Rotations, quaternions and computer graphics. Ring homomorphisms, inclusion and evaluation examples. Image subrings and kernel ideals. Modular arithmetic revisited. Quotient rings. First Isomorphism Theorem for rings.

6. Divisibility and Factorisation

(6 lectures)

Divisibility, integral domains, units, irreducibles. Unique factorisation domains. Euclidean domains and their quotient rings. The field $\mathbf{F}_4$ with four elements, solitaire. Unique factorisation in Euclidean domains. Criterion for squareness of −1 mod p. Irreducibles in the Gaussian

MAS439 Table of Contents

MAS 439

COMMUTATIVE ALGEBRA AND ALGEBRAIC GEOMETRY

TOM BRIDGELAND

CONTENTS

- You've forogtten a lot of this not having used it for two years
- We do everything more in depth and sophisticated

I AM DEPENDING ON YOU TO LET ME KNOW IF I'M GOING TOO FAST (or too slow)

A Quiz

Answer on the paper provided

1. What's the formal definition of a ring homomorphism? Give an example.
2. What's the formal definition of an ideal? What's the *point* of this definition?
3. Give at least 5 examples of rings.

Up to you whether you put your name on them or not; I'm just using these as a quick gauge of our background.

Definition of a ring, ugly version

A *ring* is a set R with two binary operations $+, \cdot$ satisfying:

1. $\forall x, y, z \in R, (x+y)+z = x+(y+z)$
2. $\exists 0_R \in R$ such that $\forall x \in R, 0_R + x = x + 0_R = x$
3. $\forall x \in R, \exists -x \in R$ such that $x + (-x) = (-x) + x = 0_R$
4. $\forall x, y \in R, x + y = y + x$
5. $\forall x, y, z \in R, (x \cdot y) \cdot z = x \cdot (y \cdot z)$
6. $\exists 1_R \in R$ such that $\forall x \in R, 1_r \cdot x = x \cdot 1_R = x$
7. $\forall x, y, z \in R$:
$$x \cdot (y+z) = x \cdot y + x \cdot z$$
$$(y+z) \cdot x = y \cdot x + y \cdot z$$

What are the names of the axioms?

Definition of a ring, take two

A *ring* is a set R with two binary operations $+, \cdot$ satisfying:

1. $(R, +)$ is an abelian group
2. $(R, \cdot)$ is a monad
3. Multiplication $(\cdot)$ distributes over addition $(+)$

A *monad* satisfies all the axioms of a group except perhaps the existence of inverses.

Back to the Quiz:
Let's list examples of rings

How'd we do?

1. The trivial ring has one element
2. The integers $\mathbb{Z}$
3. Any field $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_2, \cdots$
4. "clock arithmetic" $\mathbb{Z}/12\mathbb{Z}$ and more generally $\mathbb{Z}/n\mathbb{Z}$
5. Polynomial rings $\mathbb{R}[x], \mathbb{Z}[y, z]$
6. The set $M_n(\mathbb{R})$ of $n \times n$ matrices with real coefficients
7. The quaternions $\mathbb{H}$
8. The Gaussian integers $\mathbb{Z}[i] = \{z = a + bi \in \mathbb{C} | a, b \in \mathbb{Z}\}$
9. The set $\mathrm{Fun}(\mathbb{R}, \mathbb{R})$ of all functions from $\mathbb{R}$ to itself, under pointwise addition and multiplication (e.g., $(f \cdot g)(x) = f(x) \cdot g(x)$)
10. The set $C(\mathbb{R})$ of all *continuous* functions from $\mathbb{R}$ to itself

Commutative algebra is the study of commutative rings

Definition

A ring R is *commutative* if multiplication is commutative, i.e. $x \cdot y = y \cdot x$

Convention:

Unless otherwise specified, all rings R will be assumed to be commutative.

Types of elements

Definition

We say $r \in R$ is a *unit* if there exists an element $s \in R$ with $rs = 1_R$

Definition

We say that $r \in R$ is a *zero divisor* if there exists $s \in R, s \neq 0_R$ with $rs = 0_R$

Definition

We say that $r \in R$ is *nilpotent* if there exists some $n \in \mathbb{N}$ with $r^n = 0_R$

Examples?

Types of rings

Definition

We say R is *field* if every nonzero element is a unit.

By convention, the trivial ring is not a field.

Definition

We say R is an *integral domain* if it has no zero divisors.

Definition

We say that R is *reduced* if it has no nilpotent elements.

Examples?