ALGEBRA SEMINAR

NIKO NAUMANN AND JUSTIN NOEL

1. General advice

Unless otherwise stated, you will generally be expected to supply proofs for claims made during your talk. If a text makes a claim without proof, then you need to supply your own proof. Be especially aware of the phrases: "It is easy to see", "clearly", and "obviously". Organize your talk into definitions and stated theorems, propositions, and lemmas. For the proofs and examples make sure that *every* claim is justified.

If the proof for a claim seems to take much longer than you have time for then bring this to the attention of Prof. Naumann or Justin Noel *before* your talk is expected to be prepared.

2. A course in arithmetic

(1) Polynomial equations over finite fields [Ser73, §I.2].
  (a) The proof of Theorem 3 is missing a couple of details; fill them.
  (b) Supply the definitions of homogeneous polynomials and quadratic forms.

(2) Supporting lemmas for the quadratic reciprocity theorem [Ser73, §I.3.1-I.3.2].
  (a) Proof all of the statements in Theorem 5.
  (b) Find numerous examples for the remark in 3.2.

(3) Quadratic reciprocity [Ser73, §I.3.3].
  (a) Check all computations carefully.
  (b) Work through more examples as in the remark in 3.3.
  (c) In particular when $\left(\frac{p}{q}\right) = 1$ find a solution to $x^2 \equiv p \pmod{q}$.

(4) Quadratic forms [Ser73, §IV.1.1-IV.1.2]
  (a) Give explicit examples of quadratic forms, their associated matrices, and identify their radicals.
  (b) Apply Prop. 3 and its corollary to a specific example.

(5) Isotropic spaces and bases [Ser73, §IV.1.3-IV.1.4]

(6) Witt's theorem and Translations [Ser73, §IV.1.5-IV.1.6]

(7) Quadratic forms over $\mathbb{F}_q$ [Ser73, §IV.1.7] and quaternions [Sti03, §8.1-8.3].
  (a) This talk will conclude our discussion of quadratic forms as well as recall the a basics of the quaternions.
  (b) Include specific (non-trivial) examples illustrating [Ser73, §IV.1.7. Prop. 5].

(8) The four square theorem [Sti03, §8.4.-8.8].
  (a) If time permits, do exercise 8.8.4.

3. Integral solutions to $a^n + b^n = c^n$ for $2 \leq n \leq 4$

(9) Pythagorean triples
  (a) The goal of this lecture is to find all triples $(a, b, c) \in \mathbb{N}$ such that $a^2 + b^2 = c^2$. (a nice overview is available at `https://en.wikipedia.org/wiki/Pythagorean_triple`.

(b) Reduce to the case of where each pair $(a, b), (a, c)$, and (b, c) are relatively prime (such a triple is called primitive).
(c) As time permits:
 (i) Derive Euclid's formula again using unique factorization in $\mathbb{Z}[i]$ ([Sti03, §6.1]).
 (ii) Derive Euclid's formula again using the chord method of Diophantus ([Sti03, §1.7]).
 (iii) Use elementary algebra to derive Euclid's formula for the primitive triples.

(10) First cases of Fermat's last theorem
 (a) The goal of this lecture is to show that there are no triples $(a, b, c) \in \mathbb{N}$ such that $a^n + b^n = c^n$ for $n \in \{3, 4\}$.
 (b) First handle the case of $n = 4$. This problem is equivalent to showing $a^4 - b^4 = c^2$ has no solutions.
 (c) This uses the method of infinite descent, which shows that if one has a solution then one can always construct a 'smaller' solution. Since this can not be done indefinitely there is no solution (see [IR82, §17.2]).
 (d) As a corollary, show that the area of any right triangle with whose legs have integer length is not the square of an integer.
 (e) For the case $n = 3$ follow [IR82, §17.8].

4. Applications of number theory to classical geometry

(11) Trisecting an angle, squaring the circle, and doubling the cube (follow [Bos06, §6.4]).
 (a) Recall compass and straightedge constructions.
 (b) Show that any rational length can be constructed.
 (c) Show that any length constructed in one step from given lengths is the solution to a quadratic equation whose coefficients are in a rational field containing the given lengths.
 (d) As time permits:
 (i) Show that a constructible angle θ can be trisected if and only if $4t^3 - 3t - \cos(\theta)$ is reducible over $\mathbb{Q}(\cos(\theta))$ (see `https://en.wikipedia.org/wiki/Angle_trisection`).
 (ii) Show that $\pi/3$ is a constructible angle which can not be trisected.
 (iii) Using the fact that $\sqrt{\pi}$ is not an algebraic integer show that one can not construct a square with area equal to the circle with radius 1.
 (iv) Show that there is a cube C with constructible side lengths such that there is no cube D with constructible side lengths such that $\text{Vol}(D) = 2\text{Vol}(C)$.

5. Impossibility of solving every quintic by radicals

(12) Solvable groups and the insolvability of A_n and S_n for $n \geq 5$ [Bos06, §5.4].
 (a) Include the definition of A_n and S_n.

(13) Solvable field extensions and iterated extensions (follow [Bos06, §6.1] go up to Satz 5 and its proof.)
 (a) The goal of this lecture is to show that an extension of fields $E \subset F$ is solvable (i.e., there is an extension $F \subset L$ with $E \subset L$ Galois with solvable Galois group), precisely when the extension can be constructed as a sequence of very elementary extensions.
 (b) Feel free to restrict to characteristic 0 fields.

(14) Solving polynomial equations by radicals (follow [Bos06, §6.1] continuing the previous lecture.)
   (a) The goal of this lecture is to show that in general the quintic over $\mathbb{Q}$ is not solvable by radicals.
   (b) Assume the Hauptsatz on symmetric polynomials.

References

[Bos06] Siegfried Bosch. *Algebra*. Springer-Lehrbuch. Berlin: Springer, 6. auflage edition, 2006.

[IR82] Kenneth F. Ireland and Michael I. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1982. Revised edition of ıt Elements of number theory.

[Ser73] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[Sti03] John Stillwell. *Elements of number theory*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2003.

[Tha00] Dinesh S. Thakur. Fermat's last theorem for regular primes. In *Cyclotomic fields and related topics (Pune, 1999)*, pages 165–173. Bhaskaracharya Pratishthana, Pune, 2000. Available at `http://www.bprim.org/cyclotomicfieldbook/d3f.pdf`.