Topics for a bachelor's thesis

Leandro Vendramin

In this document, you will find a selection of topics suitable for preparing your bachelor's thesis under my supervision. Each topic includes a brief explanation and a few references. If you need more information, please feel free to contact me.

FIGURE 1. Here is the list of theses I have supervised.

1. Representations of (some) Lie algebras

The Lie algebra

$$\mathfrak{sl}_2(\mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a + d = 0 \right\}$$

is a fundamental object in the study of Lie algebras and plays a crucial role in understanding more complicated structures. In addition to its significance in physics, it possesses a rich representation theory that serves as a blueprint for understanding more general cases.

2. The Cauchy—Davenport theorem in finite groups

Let p be a prime number. If A and B are non-empty subsets of the set $\mathbb{Z}/p$ of integers modulo p, then

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

This sharp bound is known as the Cauchy—Davenport theorem [**40**]. Remarkably, the theorem can be generalized to any finite group! Reference: [**2, 25**].

3. Chebyshev's curves and singular points

A classical theorem in the theory of plane curves states an irreducible algebraic curve C of degree n in $\mathbb{P}_2(\mathbb{C})$ has at most $\frac{1}{2}(n-1)(n-2)$ singularities. It is a very natural question to ask whether, for each n, there exists irreducible curves of degree n that have such maximal number of singularities. A concrete family of curves reaching that maximal number of singularities can be constructed using Chebyshev's polynomials. References: [**11, 43**].

4. The Schur–Zassenhaus theorem

Given a normal subgroup N of G, can we reconstruct the structure of G from that of N and G/N? In general, no. However, there is a crucial case where this problem has a beautiful solution: If the orders of N and G/N are coprime, then G is a semidirect product of N and G/N. This is the celebrated Schur—Zassenhaus theorem. The proof is also enjoyable. It reduces the problem to the case where N is abelian; in that case, one uses some basic group cohomology! Reference: [**21**].

DEPARTMENT OF MATHEMATICS AND DATA SCIENCE, VRIJE UNIVERSITEIT BRUSSEL, PLEINLAAN 2, 1050 BRUSSELS, BELGIUM.
E-mail address: `Leandro.Vendramin@vub.be`.
Date: August 20, 2025.

5. Dedekind-finite rings

A ring is said to be a *Dedekind-finite* ring if $ab = 1$ implies $ba = 1$ for any two elements a and b. Several classes of rings are known to be Dedekind-finite. There is a beautiful theorem of Kaplansky that states that if an element of a ring has more than one right inverse, then it in fact has infinitely many. References: [**26, 27, 46**].

6. It is all about actions

The idea is to study an elementary theorem (yet compelling) proved not so long ago by Deaconescu and Walls about divisibility relations among the set of orbits of actions by group automorphisms. The theorem is very elementary and has friendly and highly non-trivial applications. References: [**8, 9, 22**].

7. Hall's Marriage theorem

Suppose that n persons apply to m jobs. Assume that each person applied to some jobs. When do we know that every person will get a job? Hall's theorem [**16**] answers the question. The result has several equivalent formulations and almost infinitely many applications! References: [**10, 17**].

8. Permutation polynomials

Let K be a finite field (e.g., the field of integers modulo a prime number p). The project is about "permutation polynomials". A permutation polynomial $f(X) \in K[X]$ such that the associated function $x \mapsto f(x)$ is bijective. In 1966, Carlitz presented a conjecture that motivated around 30 years of intensive research in permutation polynomials. Although there was an immediate success in some special cases, progress was made slowly over the next three decades until Carlitz's conjecture was finally resolved in the affirmative by Fried, Guralnick, and Saxl in 1993. References: [**31, 32, 33**].

9. Combinatorial Nullstellensatz

An algebraic approach to combinatorial problems involves capturing some combinatorial structures using polynomials and arguing about their algebraic properties. This has led to simple solutions to several long-standing open problems. One of the main tools in this context is Alon's combinatorial NullStellensatz [**38**]. Examples of problems that can be solved with Alon's theorem are the Cauchy—Davenport theorem, and Kakeya's conjecture for finite fields. References: [**14, 37**].

10. Cross products only in dimensions three and seven

This astonishing claim follows quickly from a theorem of Hurwitz about the possibility of writing products of a sum of squares as a sum of squares. There is a proof of the theorem based on linear algebra [**7**]. There is another proof that uses the representation theory of finite groups [**19**].

11. Zsigmondy's theorem

Zsigmondy's theorem is a result that often proves useful in various number theory problems. It proves the existence of primitive divisors of numbers of the form $a^n - b^n$. And while this is an interesting result in itself, it is also a powerful trick for solving mathematical contest problems. Reference: [**54**].

12. The Brauer–Fowler theorem

There are (at most) finitely many simple groups with a centralizer of involutions of order n. The theorem is the starting point for the classification of simple groups. References: [**3, 23**].

13. The Golod–Shafarevich theorem

Golod and Shafarevich proved this significant result in 1964. It results in non-commutative algebra, which solves several challenging problems (e.g., the class field tower problem). In combinatorial group theory, finding a counterexample to the generalized Burnside problem is crucial: For each prime p, there is an infinite group G generated by three elements in which each element has order a power of p. Reference: [**19**].

14. Kaplansky's conjectures in group rings

There are several open problems in ring theory known as Kaplansky's conjectures [**24**]. Recently, Giles Gardam found a two-page counterexample [**12**] to the celebrated conjecture on units of group algebras. This is just the story's beginning: several other open problems exist! References: [**26, 42**].

15. Far beyond the Cayley—Hamilton theorem

The Cayley–Hamilton theorem states that every square matrix satisfies its characteristic equation. The Amitsur–Levitzki theorem deals with products of $2k$ matrices of size k^2. The theorem is the starting point of a rich theory of rings with polynomial identities. (Interesting note: As a young man, Levitzki went to Göttingen to study chemistry, but attending a lecture by Emmy Noether converted him to mathematics.) References: [**4, 47**].

16. Graph theory and the Amitsur–Levitski theorem

The Amitsur—Levitzki theorem states that

$$\sum_{\sigma \in \mathbb{S}_{2n}} \operatorname{sign}(\sigma) A_{\sigma(1)} \cdots A_{\sigma(2n)} = 0$$

for all $A_1, \ldots, A_{2n} \in M_n(\mathbb{C})$. There is a beautiful graph-theoretic proof of this surprising result. References: [**52, 53**].

17. Prime number generators and the FRACTRAN programming language

FRACTRAN is a Turing-complete programming language invented by the mathematician John Conway. A FRACTRAN program is an ordered list of positive rational numbers and an initial positive integer. In this fantastic language, Conway learned how to write an astonishing prime number generator. Surprisingly, this FRACTRAN program is just a list of 14 rational numbers! Reference: [**6, 15**].

18. The Jones polynomial

In 1984 Jones discovered a new invariant of knots. The invariant assigns to each oriented knot (or link) a Laurent polynomial with integer coefficients. This invariant is surprisingly simple and extremely powerful. And Jones' discovery was crucial in solving some old-and-famous 200-years-old conjectures. References: [**1, 30**].

19. The (curious history of the) Schwartz–Zippel lemma

The fundamental question of identity testing is: given a polynomial $P(X_1, \ldots, X_n)$ of degree d, when is this polynomial identically zero? An interesting approach to this question appeared independently in the works of Schwartz [**48**], Zippel [**55**], De Millo and Lipton [**34**], and others. According to [**33**], the first instance of this result was proven by Ore in 1922. The lemma also appears in the PhD thesis of Daniel Erickson from 1974. This lemma now has several applications in pure mathematics.

20. Herstein's theorem

A very nice theorem proved by Herstein in 1957 states that a finite group with an abelian maximal subgroup is always solvable. The original proof uses Frobenius' groups [**18**]. Alternatively, one can present a more elementary proof using the transfer map; see [**35**, Theorem 5.53].

21. An example of a P.I.D. that is not a Euclidean domain

It turns out that $R = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-19})]$ is such an example. A simple proof appears in [**5, 29**]. To show that R has the desired properties, Campoli proves that the ring R is, in his words, *almost euclidean*. It turns out that a ring is almost euclidean if and only if it is a principal ideal domain [**13**].

22. Dirichlet's theorem

Dirichlet's theorem states that for any two positive coprime integers a and d, there are infinitely many primes of the form $a + nd$, where $n \geq 1$. In other words, there are infinitely many primes that are congruent to a modulo d. Reference: [**49**].

23. Lagrange's theorem

Lagrange's theorem states that every non-negative integer can be represented as a sum of four non-negative integer squares. A particularly elegant proof of this result can be found using ideas from the geometry of numbers, specifically Minkowski's theorem. It can also be proved using ideas similar to those we studied in the bachelor course *Ring and Module Theory*. References: [**41, 51**].

24. The inverse Galois problem for abelian groups

The Inverse Galois Problem is a fundamental question in mathematics that seeks to determine whether every finite group can be realized as the Galois group of some field extension over the rational numbers. The case of abelian groups is the perfect place to start studying this fascinating topic. References: [**36, 50**].

25. Ore's theorem

This important, though not very well-known, theorem states that any finite solvable group G is isomorphic to a quotient of a group of the form $U \rtimes S$, where U is nilpotent and S is a solvable group of order less than $|G|$. This result is a consequence of Frattini's work and has applications in Galois theory Reference: [**50**].

26. Using wreath products to prove theorems

Wreath products are formed through a specific combination of groups, similar in spirit to the construction of semidirect products. Despite their significant applications, wreath products are often overlooked in introductory courses. The goal of this project is to define wreath products, provide examples, and use them to prove easily some nice theorems. Reference: [**45**].

27. Semisimple rings

Semisimple rings are rings where every module is a direct sum of simple modules. By Wedderburn's theorem, they're isomorphic to finite products of matrix rings over division rings. Examples include group algebras over fields of characteristic zero. Reference: [**20**].

28. Projective modules

Projective modules generalize free modules in algebra. A module P is projective if homomorphisms from P can be "lifted" through surjective maps. They're direct summands of free modules and essential for homological algebra, representation theory and algebraic topology. [**28**].

29. What is a pointed Hopf algebra?

Pointed Hopf algebras are Hopf algebras generalize group algebras and enveloping algebras of Lie algebras, and many quantum groups like quantized enveloping algebras. Reference: [**39, 44**].

References

[1] C. C. Adams. *The knot book*. American Mathematical Society, Providence, RI, 2004. An elementary introduction to the mathematical theory of knots, Revised reprint of the 1994 original.

[2] P. Balister and J. P. Wheeler. The Erdös-Heilbronn problem for finite groups. *Acta Arith.*, 140(2):105–118, 2009.

[3] R. Brauer and K. A. Fowler. On groups of even order. *Ann. of Math. (2)*, 62:565–583, 1955.

[4] M. Brešar. *Introduction to noncommutative algebra*. Universitext. Springer, Cham, 2014.

[5] O. A. Cámpoli. A principal ideal domain that is not a Euclidean domain. *Amer. Math. Monthly*, 95(9):868–871, 1988.

[6] J. H. Conway. FRACTRAN: a simple universal programming language for arithmetic [reprinted from mr0922073]. In *The ultimate challenge: the* $3x+1$ *problem*, pages 249–264. Amer. Math. Soc., Providence, RI, 2010.

[7] M. L. Curtis. *Abstract linear algebra*. Universitext. Springer-Verlag, New York, 1990. With revisions by Paul Place, With a preface by John Hempel.

[8] M. Deaconescu and G. L. Walls. On orbits of automorphism groups. *Sib. Mat. Zh.*, 46(3):533–537, 2005.

[9] M. Deaconescu and G. L. Walls. On orbits of automorphism groups. II. *Arch. Math.*, 92(3):200–205, 2009.

[10] R. Diestel. *Graph theory*, volume 173 of *Graduate Texts in Mathematics*. Springer, Berlin, fifth edition, 2018. Paperback edition of [MR3644391].

[11] G. Fischer. *Plane algebraic curves*, volume 15 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2001. Translated from the 1994 German original by Leslie Kay.

[12] G. Gardam. A counterexample to the unit conjecture for group rings. *Ann. of Math. (2)*, 194(3):967–979, 2021.

[13] J. Greene. Principal ideal domains are almost Euclidean. *Amer. Math. Monthly*, 104(2):154–156, 1997.

[14] L. Guth. *Polynomial methods in combinatorics*, volume 64 of *University Lecture Series*. American Mathematical Society, Providence, RI, 2016.

[15] R. K. Guy. Conway's prime producing machine. *Math. Mag.*, 56(1):26–33, 1983.

[16] P. Hall. On Representatives of Subsets. *J. London Math. Soc.*, 10(1):26–30, 1935.

[17] P. R. Halmos and H. E. Vaughan. The marriage problem. *Amer. J. Math.*, 72:214–215, 1950.

[18] I. N. Herstein. A remark on finite groups. *Proc. Amer. Math. Soc.*, 9:255–257, 1958.

[19] I. N. Herstein. *Noncommutative rings*, volume 15 of *Carus Mathematical Monographs*. Mathematical Association of America, Washington, DC, 1994. Reprint of the 1968 original, With an afterword by Lance W. Small.

[20] T. W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.

[21] I. M. Isaacs. *Finite group theory*, volume 92 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008.

[22] I. M. Isaacs. Group actions and orbits. *Arch. Math. (Basel)*, 98(5):399–401, 2012.

[23] G. James and M. Liebeck. *Representations and characters of groups*. Cambridge University Press, New York, second edition, 2001.

[24] I. Kaplansky. Problems in the theory of rings. In *Report of a conference on linear algebras, June, 1956*, pages 1–3. Nat. Acad. Sci., Washington, DC, 1957. Publ. 502.

[25] G. Károlyi. The Erdös-Heilbronn problem in abelian groups. *Israel J. Math.*, 139:349–359, 2004.

[26] T. Y. Lam. *A first course in noncommutative rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001.

[27] T. Y. Lam. *Exercises in modules and rings*. Problem Books in Mathematics. Springer, New York, 2007.

[28] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[29] A. Lemos and P. H. A. de Oliveira. Suggested corrections for "A principal ideal domain that is not a Euclidean domain". *Amer. Math. Monthly*, 125(5):425, 2018.

[30] W. B. R. Lickorish. *An introduction to knot theory*, volume 175 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1997.

[31] R. Lidl and G. L. Mullen. Unsolved Problems: When Does a Polynomial Over a Finite Field Permute the Elements of the Field? *Amer. Math. Monthly*, 95(3):243–246, 1988.

[32] R. Lidl and G. L. Mullen. Unsolved Problems: When Does a Polynomial over a Finite Field Permute the Elements of the Field?, II. *Amer. Math. Monthly*, 100(1):71–74, 1993.

[33] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[34] R. J. Lipton and R. E. Miller. A batching method for coloring planar graphs. *Inform. Process. Lett.*, 7(4):185–188, 1978.

[35] A. Machì. *Groups*, volume 58 of *Unitext*. Springer, Milan, 2012. An introduction to ideas and methods of the theory of groups.

[36] G. Malle and B. H. Matzat. *Inverse Galois theory*. Springer Monographs in Mathematics. Springer, Berlin, 2018. Second edition [MR1711577].

[37] J. Matoušek. *Thirty-three miniatures*, volume 53 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2010. Mathematical and algorithmic applications of linear algebra.

[38] M. Michał ek. A short proof of combinatorial Nullstellensatz. *Amer. Math. Monthly*, 117(9):821–823, 2010.

[39] S. Montgomery. *Hopf algebras and their actions on rings*, volume 82 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 1993.

[40] M. B. Nathanson. *Additive number theory*, volume 165 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996. Inverse problems and the geometry of sumsets.

[41] I. Niven, H. S. Zuckerman, and H. L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, Inc., New York, fifth edition, 1991.

[42] D. S. Passman. *The algebraic structure of group rings*. Robert E. Krieger Publishing Co., Inc., Melbourne, FL, 1985. Reprint of the 1977 original.

[43] D. Pecker. Simple constructions of algebraic curves with nodes. *Compositio Math.*, 87(1):1–4, 1993.

[44] D. E. Radford. *Hopf algebras*, volume 49 of *Series on Knots and Everything*. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2012.

[45] L. Ribes and B. Steinberg. A wreath product approach to classical subgroup theorems. *Enseign. Math. (2)*, 56(1-2):49–72, 2010.

[46] I. Rosenholtz. A pigeonhole proof of Kaplansky's theorem. *Amer. Math. Monthly*, 99(2):132–133, 1992.

[47] S. Rosset. A new proof of the Amitsur-Levitski identity. *Israel J. Math.*, 23(2):187–188, 1976.

[48] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. Assoc. Comput. Mach.*, 27(4):701–717, 1980.

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

[50] J.-P. Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, second edition, 2008. With notes by Henri Darmon.

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

[52] R. G. Swan. An application of graph theory to algebra. *Proc. Amer. Math. Soc.*, 14:367–373, 1963.

[53] R. G. Swan. Correction to "An application of graph theory to algebra". *Proc. Amer. Math. Soc.*, 21:379–380, 1969.

[54] M. Teleuca. Zsigmondy's theorem and its applications in contest problems. *Internat. J. Math. Ed. Sci. Tech.*, 44(3):443–451, 2013.

[55] R. Zippel. Probabilistic algorithms for sparse polynomials. In *Symbolic and algebraic computation (EUROSAM '79, Internat. Sympos., Marseille, 1979)*, volume 72 of *Lecture Notes in Comput. Sci.*, pages 216–226. Springer, Berlin-New York, 1979.