MATH 252: ABSTRACT ALGEBRA II
RESEARCH TOPICS

The paper should be **6-8 pages in length**; if your paper is slightly shorter or substantially longer, you will not be penalized. It should have an introduction and a conclusion, and clearly-written proofs and examples. Your target audience for the paper should be your peers; imagine coming back to this paper after two years, will you still be able to follow it from start to finish?

You must choose a topic by Friday, March 21. An e-mail will suffice, but if a topic seems interesting to you, please talk to me about it and I can suggest further reading and directions. A good place to start will be consulting what the text has to say, but I will push you to look beyond this resource.

It is recommended that you turn in a rough draft of your paper to me sometime in April—even one only partially finished—so that I can give you feedback. The quality of my comments will be proportional to the amount of time that you give me to look at it.

The paper is due at the time of the final exam, **Monday, May 5, from 8:00 a.m.–11:00 a.m.** You will be asked to present a 15-minute presentation on your topic for the class.

The paper must be typed. For your convenience, there is a TeXable template at:

`http://www.cems.uvm.edu/~voight/252/252-PROJ-template.tex`

Feel free to adjust this template however you wish. If you have never used TeX before—or have a particular question about how to get TeX to behave—please come talk to me and I will be happy to sit down with you. For other hints and tricks, you can check out the TeXed versions of the homework solutions available at the course website.

Here are some possible topics.

- **Class number 1 problem**. The class number of a number field is an abelian group which measures how far the ring of integers is from being a principal ideal domain. Which imaginary quadratic fields $\mathbb{Q}(\sqrt{D})$ have class number 1?
- **Euclidean number fields**. Some number rings are Euclidean, some are not. What is known?
- **Sum of two squares**. Give the nicest proof that a prime p can be written as the sum of two squares $p = x^2 + y^2$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$.
- **Euclidean algorithm for quadratic fields**. Find all imaginary quadratic fields which are Euclidean. Implement in Sage an extended Euclidean algorithm for one or more of these fields.
- **The exceptional automorphism of S_6**. Give a description of the exceptional automorphism of S_6.
- **The monster group**. What is the monster group? How can it be described, and from where does it arise?
- **Rubik's cube group**. Describe the Rubik's cube group in terms of simpler, smaller groups.
- **Origami**. Describe some interesting relationships between origami and group theory. For example, show that using origami one can trisect an angle.
- **Subgroup lattices**. Finish in Sage an algorithm for computing the subgroup lattice of a group. (The algorithm has already been implemented; you just need to connect the group theory to the graph theory.)

Date: 27 February 2008.

- **Finite simple groups**. Discuss a class of finite simple groups. For example, prove that the groups $PSL_n(\mathbb{F}_q)$ are simple whenever $q > 4$.
- $SL_2(\mathbb{Z})$. What can you say about the group $SL_2(\mathbb{Z})$? What are generators and relations?
- **Exact sequences**. What is an exact sequence? Do some diagram chasing, maybe prove the snake lemma.
- **Applications**. Interested in applications of group theory? Check out *Applied Abstract Algebra* by Rudolf Lidl and Günter Pilz (available through Google books) and find a topic like the relationship between semigroups and biology...
- **Inseparable extensions**. What is an inseparable extension of a field?
- **Profinite groups**. A profinite group is a group which is the inverse limit of finite groups. It carries a topology, and for example the Galois group of the algebraic closure of $\mathbb{Q}$ (over $\mathbb{Q}$) is such a group.
- **Coding theory**. Error-correcting codes allow the transmission of information over a noisy channel. A linear code is a finite-dimensional vector space over a field. Describe some simple linear codes and their relationship to group theory.
- **Cylotomic polynomials**. The cyclotomic polynomials give the factorization of $x^n - 1$ in terms of polynomials which are irreducible over $\mathbb{Q}$. What are these polynomials, and how do they bear on the arithmetic of the number field $\mathbb{Q}(\zeta_n)$ obtained by adjoining a primitive nth root of unity ζ_n?
- **Kronecker-Weber theorem**. Any abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field. Discuss some aspects of the proof.
- **Frobenius' theorem**. Prove that any finite-dimensional division algebra over $\mathbb{R}$ is isomorphic to $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$.
- **Wedderburn's theorem**. Prove that any finite-dimensional central simple algebra over a finite field k is isomorphic to $M_n(k)$ for some $n \in \mathbb{Z}_{>0}$.
- **Group extensions**. Given two groups N, H, how many possible ways are there to put them together in a group G such that N is a normal subgroup of G and $G/N \cong H$? Describe the (nonabelian) groups of order 16 (for example) in terms of group extensions.
- **Real fields**. A real field is a generalization of $\mathbb{R}$ over which many of the same theorems apply. What can you say about real fields?
- **Infinite abelian groups**. Under what circumstances is an (infinite) abelian group a direct sum of cyclic groups?