

Project guidelines

1. The project is meant to be a fun way for you to learn some topics outside of the main syllabus, work in a team, and develop your expository skills in mathematics.
2. Your project group will be either three or four people. I will assign groups based on topic preferences, and I will also take into account a (mutual) desire to work with specific people.
3. You may divide the work among your group however you like, but every group member should understand (and be able to answer questions about) any part of the project.
4. Each group will submit one write-up, due on the last day of classes (Wednesday, December 12). The write-up must be typed in LaTeX (see the LaTeX suggestions on the course website, or feel free to ask me for help). There is no page requirement, as long as you adequately cover the project topics. As a rough guideline, most write-ups will likely be between three and five pages, single spaced.
5. Your write-up should be written with the goal of explaining the topic to someone with a similar math background to you, such as another student in Math 350. Be sure to define your terms carefully, explain any notation you use, and try to motivate the ideas and give intuition wherever possible.
6. Your write-up should cite any sources you used, including books or webpages.
7. Each project group will give a 10-minute presentation during the last week of classes. The presentation should be aimed at your fellow students, with the goal of surveying the topic and highlighting the most important ideas or techniques. After the presentation, I will ask each group member a question about the topic.
8. The grading will be based on both the correctness of the mathematics and the quality of your exposition.
9. Please feel free to ask me for help or advice, individually or as a group, during office hours or by appointment!

Topics

If there is another topic related to abstract algebra that you'd like to explore, please feel free to suggest it to me and discuss the possibility!

1. Groups of order $2p$.

This project will prove that there are exactly two non-isomorphic groups of order $2p$, with p an odd prime number: every such group is either cyclic or dihedral. There is no specific reading attached to this project; rather it is an extended exercise that will involve putting together several of the main theorems and techniques from the group theory unit.

- (a) Let G be a group of order $2p$. Show that if G contains an element of order $2p$ then G is cyclic.
- (b) Show that if G is a non cyclic group of order $2p$ then it must have an element of order p .

- (c) Show that if G is a non cyclic group of order $2p$, r is an element of G of order p , and m is an element of G that is not a power of r , then
- $G = \{e, r, r^2, \dots, r^{p-1}, m, rm, r^2m, \dots, r^{p-1}m\}$.
 - $\langle r \rangle m = m \langle r \rangle$.
 - $o(m) = 2$. [**Hint:** Remember that $m^2 \in G$. What could m^2 be?].
 - $o(rm) = 2$. [**Hint:** rm must be equal to mr^i for some $1 \leq i \leq p-1$, why? Then recall that $o(rm) = p$ or $o(rm) = 2$, why? Why $o(rm) = p$ can't happen?]
 - Conclude that $o(r^j m) = 2$ for all $1 \leq j \leq p-1$.
- (d) Conclude that if G is a group of order $2p$ then either G is isomorphic to either \mathbb{Z}_{2p} or D_p .

2. Groups of order pq are always cyclic, for certain pairs of primes p, q

This project concerns groups of order pq , where p and q are distinct primes. How many groups like this exist depends on the primes, but it turns out that in many cases there is actually only one possible group of order pq (up to isomorphism). Specifically, this project will show that if the order of a group, G , is pq with p, q primes, $p < q$ and $p \nmid (q-1)$ then G is isomorphic to \mathbb{Z}_{pq} . There is no specific reading for this project; rather it is an extended exercise that will involve putting together several of the main theorems and techniques from the group theory unit.

In each part below, assume that p, q are primes as described above, and G is a group of order pq .

- Prove that if G is abelian, then it is cyclic. Deduce that if G is abelian, then it is isomorphic to \mathbb{Z}_{pq} . [**Hint:** use Theorem 11.7, together with a problem from a homework assignment about the order of a product of two elements.]
- Read pages 93 to 95 in Saracino, about the Class Equation (Theorem 10.9). Summarize the proof, including the key ideas, in your write-up, and make sure you understand the details.
- Prove that G must be abelian, using a proof by contradiction. Assume that G is non-abelian, and deduce a contradiction as follows.
 - Show that $|Z(G)|$ must be equal to 1, p , or q .
 - Show that if $|Z(G)| = q$ and $g \notin Z(G)$ then $|Z(g)| > q$. Explain why this is impossible.
 - Show that if $|Z(G)| = p$ and $g \notin Z(G)$ then $|Z(g)| = q$. Explain why this is impossible.
 - Show that if $|Z(G)| = 1$ then
 - there are $g_1, g_2 \in G$ such that $|Z(g_1)| = p$ and $|Z(g_2)| = q$. [**Hint:** Use the Class Equation].
 - if $P = \{g \in G : o(g) = p\}$, then $p-1$ and q both divide $|P|$.
 - if $Q = \{g \in G : o(g) = q\}$, then $q-1$ and p both divide $|Q|$.
 - Show that $|Z(G)| = 1$ cannot happen. [**Hint:** $|G| = 1 + |P| + |Q|$].
- Conclude that if G is a group of order pq with p, q primes, $p < q$ and $p \nmid (q-1)$ then $G \cong \mathbb{Z}_{pq}$.

3. Finite abelian groups are always direct products

This project concerns the classification of finite abelian groups, which is discussed in §14 of Saracino (which we did not cover in class). The purpose of this project is to read and understand this chapter, and write a self-contained proof of some of the results from it (in your own words).

- (a) Read and understand §14 of Saracino. In your write-up, state the fundamental theorem on finite abelian groups (14.2), and describe at least two of its consequences (which you can choose among the Corollaries in the section, or the exercises following it).
- (b) Write a self-contained proof that every finite abelian group is isomorphic to a direct product of cyclic groups (this is essentially Steps 1 and 2 as described on page 138, although those give slightly more information: that these cyclic groups can be assumed to have prime-power order). Be sure to define and terminology that you use, and refer clearly to any previous results that you make use of in the proof. Don't follow the textbook's proof verbatim; try to organize and explain it in a way that makes sense to you.

4. Sylow subgroups

This project will present a few aspects of the Sylow Theorems. The Sylow theorems concern finite groups, and give information about the subgroups of a finite group whose orders are powers of prime numbers. These theorems have been instrumental in determining how many non-isomorphic groups are there for a given order. The Sylow Theorems are discussed in §15 of the textbook, but you do not need to read and completely understand everything in that chapter.

Throughout the questions we will always assume that G is a group of order n and that p is a prime number such that $p \mid n$.

- (a) Read pages 93 to 95 in Saracino, about the Class Equation (Theorem 10.9). Summarize the proof, including the key ideas, in your write-up, and make sure you understand the details.
- (b) Show that G contains a subgroup of order p .
[**Remark:** We proved this in class for the case when G is abelian; it is Theorem 11.7]
[**Hint:** The proof is by induction and the inductive step requires the Class Equation.]
- (c) Suppose that $r \in \mathbb{Z}^+$, and $p^r \mid n$. Prove that G has a subgroup of order p^r , as follows.
 - i. Prove that if N is a normal subgroup of G , and the quotient group G/N has a subgroup of order m , then G has a subgroup of order $|N| \cdot m$.
 - ii. Prove that if $p^r \mid n$, then either $p \mid |Z(G)|$ or $p^r \mid Z(g)$ for some element $g \in G$ (make sure you understand the distinction between $Z(G)$, the center of the group, and $Z(g)$, the centralizer of a single element).
 - iii. Prove, by induction on n , that if $p^r \mid n$ and G is a group of order n , then G has a subgroup of order p^r .
- (d) Read the first two pages of §15 in Saracino. In your write-up, define a p -Sylow subgroup, and state the three Sylow theorems. You do not need to worry about the proofs, just understand the statements.
- (e) Prove, using the Sylow theorems, that any group of order 91 necessarily has a normal subgroup of order 13.

5. Burnside's theorem

This project concerns a method from group theory for answering certain types of counting problems that involve symmetry. An example of this sort of problem is: how many distinguishable ways are there to color the faces of a tetrahedron black or white? Here, two colorings are “indistinguishable” if you can obtain one by rotating the other.

The reference for this topic is Judson's online Abstract Algebra textbook, chapter 14. You may find this chapter at the link below.

<http://abstract.ups.edu/aata/actions.html>

- (a) Read sections 14.1 and 14.3 in the online textbook above. In your write-up, carefully state Burnside's theorem (Theorem 14.19), and prove it. Try to write the proof in your own terms, rather than repeating the proof in the textbook verbatim.
- (b) Solve the problem in the first paragraph: how many indistinguishable ways are there to color the faces of a tetrahedron black or white? Recall from earlier in the semester that the symmetry group of the tetrahedron is A_4 .
- (c) How many indistinguishable ways are there to color the faces of a tetrahedron with three possible colors, e.g. red, blue, or green?
- (d) Solve exercise 16 from section 4.4 in the online textbook above (about counting Benzene compounds using Burnside's theorem).

6. Structure of finite fields

In this project, you will prove some basic facts about the structure of finite fields. In class and on the homework, we've discussed a few ways to make finite fields of order p (a prime number), 4, and 9. There are many more finite fields, and they are fairly well understood, due to some nice structure. In particular, the number of elements is always a power of a prime number, and they always have a rather curiously defined automorphism.

Below, assume that F is a field with a finite number of elements.

- (a) Define a ring homomorphism $\mathbb{Z} \rightarrow F$ by $\phi(n) = n \cdot 1_F$. Prove that the image of \mathbb{Z} is a subfield, and that this subfield has a prime number of elements. This is called the *prime subfield* of F .

In the parts below, denote this prime subfield by P , and denote by p the number of elements in P .

- (b) Read and understand the definitions of *linearly independent*, *span*, and *basis* on page 231 of Saracino. It may also be helpful to read the following two pages, to get a feel for the terminology. These terms match the corresponding terms from Math 271/2, except that we have replaced \mathbb{R} by a new field. Summarize these definitions in your own words in your write-up, as well as your presentation.
- (c) Prove that if $\{s_1, s_2, \dots, s_n\} \subseteq F$ is a linearly independent over P , then the set

$$\{c_1 s_1 + c_2 s_2 + \dots + c_n s_n : c_1, c_2, \dots, c_n \in P\}$$

has exactly p^n elements in it.

- (d) Prove that there exists a basis $\{s_1, \dots, s_n\}$ for F over P . [*Hint*: argue by contradiction. If there is no basis, then find the largest possible linearly independent set; show that adding any element not in the span of this set would produce an even larger linearly independent set.]
- (e) Deduce from the previous two parts that the number of elements in F is a power of p .
- (f) Define a function $\phi : F \rightarrow F$ by $\phi(x) = x^p$. This is called the *Frobenius map*. Look up a statement of the binomial theorem, and use it to show the following curious identity (sometimes jokingly called the “Freshman’s dream” in reference to common algebra errors in calculus class): for all $x, y \in F$,

$$(x + y)^p = x^p + y^p.$$

Deduce from this identity that ϕ is a homomorphism of fields, and prove that in fact ϕ is an *automorphism*. This is often called the “Frobenius automorphism,” and is a crucial tool in algebra over finite fields.

7. Unique factorization in $\mathbb{Z}[i]$

This project concerns the ring of Gaussian integers $\mathbb{Z}[i]$ discussed in class, and one particularly surprising way in which it resembles the usual ring \mathbb{Z} of integers: it has its own version of prime numbers and unique factorization. The main source for this topic is §21 of Saracino, which we will not cover in class.

- (a) Read and understand §21 of Saracino, with particular emphasis on the main definitions (especially UFD, Euclidean domain, and PID), and any mention of $\mathbb{Z}[i]$.
- (b) In your write-up, state Theorem 21.4 (you do not need to write out a proof of it), and explain all of the terminology used in the statement.
- (c) Write a proof that $\mathbb{Z}[i]$ is a PID and a UFD, defining any terminology that you need. You can follow the same method as the book uses, but try not to mimic the book verbatim; write the proof in a way that makes sense to you.
- (d) Prove that if p is a prime number and $p \equiv 1 \pmod{4}$, then p is *not* irreducible in $\mathbb{Z}[i]$. Explain why this implies that p can be written as a sum of two squares (this is part of Theorem 21.8 in Saracino).
- (e) Prove that if p is a prime number with $p \equiv 3 \pmod{4}$, then p is irreducible in $\mathbb{Z}[i]$. Use this to prove that the quotient ring $\mathbb{Z}[i]/p\mathbb{Z}[i]$ is a *field*, and show that this field has p^2 elements.

8. Construction by straight-edge and compass

In this project, you will learn about an ancient geometry problem: if your only drafting tools are a straightedge and a compass, which figures is it possible to draw with them? The main source for this topic is §23 of Saracino. The main idea is to relate the constructible figures to a certain subfield of \mathbb{C} .

One challenging aspect of this project is that you’ll need to get some working familiarity of some of the preceding sections of Saracino (especially about degrees of field extensions) in order to understand §23; my suggestion is to try to learn just enough about these earlier topics to understand the arguments in §23, even if you do not learn all of the proofs in the earlier sections. Please do not hesitate to ask me for help.

- (a) In your write-up, explain the definition of \mathbb{C}_c (as defined in §23), and how to understand it in terms of compass and straightedge constructions.
- (b) Explain what the Greeks meant when they asked if you could “double the cube,” and explain why it is in fact impossible to do so.
- (c) Explain what the Greeks meant when they asked if you “trisection the angle,” and explain why it is in fact impossible to do so.
- (d) Explain why the Saracino text has a 17-sided polygon on its cover.
- (e) Solve exercises 23.8 and 23.11 in Saracino (include the solution in your write-up).

9. Public key cryptography

This project will give some fundamentals of public key cryptography. As source material, read Chapter 7 of the Judson’s free online textbook on abstract algebra, which you may find at the following link:

<http://abstract.ups.edu/aata/crypt.html>

- (a) Give a description of the following private key cryptography methods:
 - i. *monoalphabetic cryptosystem*.
 - ii. *affine cryptosystem*.
 - iii. *polyalphabetic cryptosystem*.
- (b) Provide an example of how the message “GROUPS RINGS AND FIELDS ROCKS” would be encoded by a:
 - i. monoalphabetic cryptosystem. (Using $b = 7$)
 - ii. affine cryptosystem. (Using $a = 7$ and $b = 10$. Could we use $a = 10$ and $b = 7$? Explain why or why not.)
 - iii. polyalphabetic cryptosystem. (Using $A = \begin{bmatrix} 3 & 5 \\ 2 & 3 \end{bmatrix}$ and $\vec{b} = [5 \ 11]$. Could we use $A = \begin{bmatrix} 4 & 7 \\ 1 & 5 \end{bmatrix}$ $\vec{b} = [3 \ 2]$? Explain why or why not.)
- (c) Explain how the public key cryptography RSA method works. Be sure to explain the following:
 - i. How a message is encoded.
 - ii. How a message is decoded.
 - iii. How do we know the process properly decodes a message that was encoded using a public key?
 - iv. How does message verification work?
 Explain using an example with the message N (13) and the sender having $n' = 77$ and $E' = 7$ as the public key, (what must D' be in this case?) and the receiver having $n = 65$ and $E = 11$, (what must D be in this case?)
Remark: I recommend you also read *The method of repeated squares* in the book, pages 65-67, so you can do this efficiently.
- (d) Create your own example with n and E (do not reveal E to me), encode the message “NO” (by encoding each letter, ‘N’ is 13 and ‘O’ is 14, separately). Provide me the result of the encoding, n and D so I can decode the message and verify that you understand the process.

10. **Historical project**

This project idea is fairly open-ended. If you choose it, please meet with me in your group beforehand to discuss your ideas and what you'd like to do. The basic parameters: write a paper of approximately 2000 words describing the historical development of some of the concepts that we've discussed in this class. For example: you might choose a concept (such as normal subgroups, or ideals, or fields), and ask: when where they first defined? How closely does the original definition match the one that we use today, and what problems was it intended to solve? What is some of the contemporary research on the topic?

11. **Algorithms for \mathbb{Z}_n (coding project; requires programming experience)**

In this project, you will learn about several important algorithms for working with the ring \mathbb{Z}^n in an applied context, and implement them in a programming language of your choice. Such algorithms are crucial in applications such as cryptography and coding theory.

Your write-up should consist of brief explanations of the algorithms and the main ideas that make them work, as well as your source code. In your presentation, you should explain the basic ideas behind the algorithms, and why they work efficiently.

Use the book *An Introduction to Mathematical Cryptography* as your reference. You can find it online for free (with your Amherst login) online at the link below.

<https://link.springer.com/book/10.1007%2F978-0-387-77993-5>

Note that all of these problems have relatively easy “guess-and-check” implementations, but the purpose of this project is to understand how to make efficient algorithms. For example, your implementations should finish their computation nearly instantaneously when given 32-bit integers as input.

- (a) (Addition and multiplication) In your preferred programming language, write functions `add` and `multiply` that accept three arguments: a positive integer n (the modulus), and two integers a, b , which you may assume to lie in the set \mathbb{Z}_n , and return $a \oplus b$ and $a \odot b$ (respectively).
- (b) (Multiplicative inverses) Read Section 1.2 in the textbook linked above, and implement the Extended Euclidean Algorithm. That is: write a program that accepts integers a, b and returns integers u, v such that $au + bv = (a, b)$. Use this algorithm to implement a function `modinverse` that accepts an integer n (the modulus) and an integer a (which you may assume is chosen from \mathbb{Z}_n^\times), and returns the multiplicative inverse of a in the ring \mathbb{Z}_n .
- (c) (Exponentiation) Read section 1.3.2 in the textbook linked above, and implement the fast-powering algorithm. That is, write a function `modpow` that accepts an integer n (the modulus), an integer a (which you may assume is chosen from \mathbb{Z}_n), and a positive integer k , and returns the element $a^k \in \mathbb{Z}_n$.
- (d) (k th roots modulo a prime) Read Proposition 3.2 and its proof in the textbook linked above. Combine the functions implemented so far to implement a function `kthroot` that takes arguments p, a, k , where you may assume that p is prime, $a \in \mathbb{Z}_p$, and $(k, p-1) = 1$, and returns the solution $x \in \mathbb{Z}_p$ to the equation $x^k = a$.

12. Coding theory

In this project, you will learn about a topic called *coding theory*, which applies finite fields to solve the following problem: how do you send a digital transmission across a noisy channel that may corrupt some of the bits?

The source for this project will be chapters 2 and 4 of Finston and Morandi's Abstract Algebra textbook. You may access this book free online (with your Amherst login) at the following link.

<https://link.springer.com/book/10.1007%2F978-3-319-04498-9>

For this project, you should read chapters 2 and 4 of the textbook linked above, and write a paper summarizing the main ideas, with particular emphasis on the Hamming code, in a manner that would be accessible to another student in Math 350. Your write-up should describe codes in general and linear codes in particular, and should also describe the notions of vector spaces and subspaces over the field \mathbb{Z}_2 . Include several examples (a good source of example would be to choose a few exercises from the textbook and solve them).