Algebra, Coding Theory and Cryptography
Lecture Notes

Lior Silberman

These are rough notes for the spring 2009 course. Solutions to problem sets were posted on an internal website.

Contents

CHAPTER 1

Introduction (8/9/2011)

Lior Silberman, `lior@Math.UBC.CA`, `http://www.math.ubc.ca/~lior`
Office: Math Building 229B
Phone: 604-827-3031

1.1. First impressions

1.1.1. Practical side.

Uses of error-correcting codes.

- CDs
- Ethernet; IP; TCP
- Cellular networks
- Satellite & Space probe communications

Uses of Cryptography.

- Secure communication
  - Web browsers
  - IP Telephony
- Digital signatures
  - Website certificates
  - Software downloads

1.1.2. Abstract algebra. Generalize specific examples of algebraic constructions to a theory of abstract objects.

1.1.3. Course plan. 5 weeks of arithmetic in the integers and in $\mathbb{Z}/m\mathbb{Z}$, leading up to RSA.
7 weeks of abstract structures with coding theory applications.

1.2. Microcosm: Vector spaces over $\mathbb{F}_2$

1.2.1. $\mathbb{F}_2$. Computers work best with bits (zeroes and ones) and strings of bits. Any stream of data can be encoded into binary. Would be nice to impose algebraic structure on these strings. Start with arithmetic of $0,1$. Clearly we must have:

$$\begin{aligned} 0+0 &= 0 \\ 0+1 &= 1 \\ 1+0 &= 1 \end{aligned}$$

Question: What about $1+1$?

DEFINITION 1. A set A together with a binary operation $+$ and a distinguished element $0 \in A$ is called an *abelian group* if:

(1) $\forall x,y,z \in A : (x+y)+z = x+(y+z)$
(2) $\forall x \in A : 0+x = x$.
(3) $\forall x \in A \exists x' \in A : x+x' = 0$.
(4) $\forall x,y \in A : x+y = y+x$.

These are the usual laws one would expect, and they hold for the structure we defined provided $1+1=0$.

Question: What about multiplication?

The usual laws of arithmetic then hold (including multiplicative inverses), and the resulting structure is called a *field*.

We call $\mathbb{F}_2 = (\{0,1\},+,\cdot,0,1)$ *the field with* 2 *elements*. Compare it with $\mathbb{R} = (\mathbb{R},+,\cdot,0,1)$, the field of real numbers.

1.2.2. Vector spaces over $\mathbb{F}_2$. For the use of computers it is natural to encode data as strings of zeroes and ones, that is elements of $\{0,1\}^n$. Many applications involves transforming the data. For example:

- Error-correcting encoding: we may want to represent the message $\underline{v} \in \{0,1\}^n$ as a long bit string $C(\underline{v}) \in \{0,1\}^m$ adding some redundancy. This can be done in such a way that even if $C(\underline{v})$ is modified at a few bits it's possible to reconstruct $\underline{v}$.
- Encryption: we may want to replace $\underline{v}$ with a message $E(\underline{v})$ with a function E which is hard to invert.

Giving *structure* to the space of messages allows us to look for maps that are easy to compute and describe (such as linear maps). Here, instead of thinking of $\{0,1\}^n$ we will think of $\mathbb{F}_2^n$, the n-dimensional vector space of *column vectors with entries in* $\mathbb{F}_2$. Addition of vectors is defined component-wise, as is multiplication by scalars (elements of $\mathbb{F}_2$).

To get used to the way arithmetic works here and to the idea of vectors spaces, we use:

Question: Let $\mathbb{F}_2$ act on $\mathbb{R}^n$ as follows: multiplication by $0 \in \mathbb{F}_2$ will map the vector to zero; multiplication by $1 \in \mathbb{F}_2$ will map the vector to itself. What's wrong with this definition?

Answer: This definition is inconsistent with having the ordinary laws of arithmetic, basically since $1+1=0$ in $\mathbb{F}_2$ but not in $\mathbb{R}$. Formally, take $\underline{v} \in \mathbb{R}^n \setminus \{\underline{0}\}$. Then we have by definition

$$1_{\mathbb{F}_2} \cdot \underline{v} = \underline{v}.$$

Adding this equation to itself, and using the distributive law, we get:

$$(1_{\mathbb{F}_2} + 1_{\mathbb{F}_2}) \cdot \underline{v} = \underline{v} + \underline{v} = 2_{\mathbb{R}} \cdot \underline{v}.$$

But in $\mathbb{F}_2$ $1+1=0$ so we get $\underline{v}+\underline{v}=0$ which in $\mathbb{R}^n$ only happens for $\underline{v} = \underline{0}$. The moral is that $\mathbb{R}^n$ is not a vector space over $\mathbb{F}_2$ since we can't make the distributive law hold. Of course $\mathbb{R}^n$ is a vector space over $\mathbb{R}$.

1.2.3. Application: one-time pad. Alice and Bob would like to communicate privately. The message they want to send will be encoded in a long string of bits, that is a vector $\underline{v} \in \mathbb{F}_2^n$. In order to do this they generate a vector of random bits $\underline{p} \in \mathbb{F}_2^n$, share it, and keep it secret. $\underline{p}$ is called the "pad".

Encryption: Alice sends to Bob the vector $\underline{x} = E_{\underline{p}}(\underline{v}) = \underline{v} +_{\mathbb{F}_2} \underline{p}$.

Decryption: Bob calculates the vector $D_{\underline{p}}(\underline{x}) = \underline{x} +_{\mathbb{F}_2} \underline{p}$. Since $\underline{x}+\underline{p} = \underline{v} + \left(\underline{p}+\underline{p}\right) = \underline{v} + \underline{0} = \underline{v}$, Bob can successfully recover $\underline{v}$.

REMARK 2.

1. The transmitted vector $\underline{x}$ is indistinguishable from random noise, since every bit in it was mingled with a totally random bit from the pad. Only knowing the pad allows you to recover the information transmitted.
2. We need one random bit in the pad for each bit we want to send. In particular, this is very expensive in terms of communicated the pad itself. Sending special couriers with CDs burned with random noise is ok for the Foreign Office, but not for private people.
3. It's important to have a *one-time* pad, that is use every bit of the pad only once. If we every encode two messages with the same pad, then the difference $E_{\underline{p}}(\underline{u}) - E_{\underline{p}}(\underline{v})$ does not depend on $\underline{p}$ and so leaks information.

Math 342 Lecture 1 Worksheet.

PROBLEM. (Arithmetic) Fill in the tables using only $\{0,1\}$ while preserving the rules of arithmetic.

$+$	0	1
0		
1		

$\times$	0	1
0		
1		

Specific checks: what is $0+x$? does your table achieve $0+1=1+0$?
what about $(0+1)+1=0+(1+1)$?

PROBLEM. Encode the message 01101101 using the following pad, then decode your result.

Plaintext								
PAD	1	1	0	0	0	0	1	0
Cyphertext								

Cyphertext								
PAD	1	1	0	0	0	0	1	0
Plaintext								

PROBLEM. (Linear algebra) Are the vectors $(1,0,1),(1,1,0)$ a linearly independent in $\mathbb{F}_2^3$? What about $(1,0,1,0,1),(0,1,0,1,0),(1,1,1,1,1)$ in $\mathbb{F}_2^5$?

PROBLEM. (Arithmetic mod 3) Now try the first problem using $\{0,1,2\}$. Start by figuring out why $1+1=0$ and $1+1=1$ can't work, so that $1+1=2$.

$+$	0	1	2
0			
1		2	
2			

$\times$	0	1	2
0			
1			
2			

Math 342 Problem set 1 (due 13/9/11)

Linear algebra over $\mathbb{F}_2$

1. Solve the system of equations

$$\begin{cases} x+y &= 1 \\ x+y+z &= 0 \\ y+z &= 0 \end{cases}$$

   over $\mathbb{F}_2$ (that is, with $x,y,z \in \{0,1\}$ and subject to the rules of addition and multiplication we obtained in class).

2. Can the bit vector $(0,1,1,1,0) \in \mathbb{F}_2^5$ be represented as a linear combination of the vectors $\{(1,0,0,0,0),(0,1,0,0,0),(1,0,1,0,1)\}$?
   Hint: the coefficients in the combination must also come from $\mathbb{F}_2$.

Induction

3. Use induction to show that among every three consecutive positive integers there is one that is divisible by 3.

4. Show that for every $n \geq 0$, $x-y$ divides $x^n - y^n$ as polynomials.

5. §2A.E23.

6. (Bernoulli's inequality) Show that $(1+x)^n \geq 1+nx$ for any natural number n and real $x > -1$.

Divisibility

An integer a is said to *divide* the integer b if there is a third integer c such that $ac = b$. For example, 2 divides 6 since $2 \cdot 3 = 6$, but 5 does not divide 6.

7. For each integer $n \in \{6,12,17\}$:
   (a) List the positive integers which divide n.
   (b) Find the sum of the divisors of n which are different from n (that is, for each n add all the numbers you got in part (a) except for n itself).
   (c) Is n *abundant* (the sum is bigger than n), *deficient* (the sum is less than n) or *perfect* (the sum is equal to n)?
8. Using the lists of divisors from the previous problem:
   (a) What is the largest number that divides both 6 and 12?
   (b) What is the largest number that divides both 12 and 17?

REMARK. (Aside) Perfect numbers are rare and only finitely many are known. It is believed that there are infinitely many even perfect numbers, but this is not known. It is not known if there exist any odd perfect numbers.

Problem set 0

1. Let $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \in M_3(\mathbb{F}_2)$. Let $\underline{v} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \in \mathbb{F}_2^3$.
   (a) Calculate $A\underline{v}$.
   (b) Is A invertible? If so, find A^{-1}.
2. (§2A.E5) Show that $\frac{1-x^{n+1}}{1-x} = 1 + x + \cdots + x^n = \sum_{k=0}^{n} x^k$.

Solution examples

1.
   (a) $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1\cdot 1 + 0\cdot 1 + 1\cdot 0 \\ 0\cdot 1 + 0\cdot 1 + 1\cdot 0 \\ 1\cdot 1 + 1\cdot 1 + 1\cdot 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.

   (b) Expanding in the first row, $\det A = 1 \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} - 1 \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = 1 \neq 0$, so A is invertible.

   We already know that $A \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ and that $A \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ (this is the second column of A) so $A^{-1} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ and $A^{-1} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$. Finally, since the first and last columns of A add to $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ we have $A \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ so $A^{-1} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ and the matrix of A^{-1} is $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

2. For $n = 0$ we need to show $\frac{1-x}{1-x} = \sum_{k=0}^{0} x^k$ and indeed both sides equal 1. We continue by induction. Assuming the truth of the claim for some n, we have

$$\begin{aligned} \sum_{k=0}^{n+1} x^k &= \sum_{k=0}^{n} x^k + x^{n+1} \\ &= \frac{1-x^{n+1}}{1-x} + x^{n+1} && \text{by the induction hypothesis} \\ &= \frac{1-x^{n+1}+x^{n+1}-x^{n+2}}{1-x} \\ &= \frac{1-x^{(n+1)+1}}{1-x}. \end{aligned}$$

CHAPTER 2

The Integers: Foundations (13-22/9/2011)

2.1. The natural numbers (13/9)

$\mathbb{N} = (\{0,1,2,3,\dots\},0,1,+,\cdot)$. How to make formal sense of our intuitive concept?

DEFINITION 3. (Peano arithmetic)

(1) For all $n \in \mathbb{N}$, $n+1 \neq 0$.
(2) For all $n,m \in \mathbb{N}$, if $n+1 = m+1$ then $n = m$.
(3) ("induction") Let $S \subset \mathbb{N}$. If $0 \in S$, and whenever $n \in S$ we also have $n+1 \in S$, then $S = \mathbb{N}$.
(4) (addition) For all $n,m \in \mathbb{N}$,
  (a) $n+0 = n$, $0+1 = 1$.
  (b) $n+(m+1) = (n+m)+1$.
(5) (multiplication) For all $n,m \in \mathbb{N}$,
  (a) $n \cdot 0 = 0$;
  (b) $n \cdot (m+1) = n \cdot m + n$.

PROPOSITION 4. *(addition) For all $l,m,n \in \mathbb{N}$:*

(1) *(Associativity)* $(n+m)+l = n+(m+l)$.
(2) *(Zero and one)* $0+n = n$, $1+n = n+1$.
(3) *(Commutativity)* $m+n = n+m$.
(4) *(Cancellation) If* $n+l = m+l$ *then* $n = m$.

PROOF. We prove each statement by induction.

(1) Let S be the set of $l \in \mathbb{N}$ such that the identity holds for all $n,m \in \mathbb{N}$. Using axiom (4a) twice gives $(n+m)+0 = n+m = n+(m+0)$, in other words that $0 \in S$. Now assume that $l \in S$. Then

$$\begin{aligned}(n+m)+(l+1) &= ((n+m)+l)+1 \text{ [axiom (4b)]}\\ &= (n+(m+l))+1 \text{ [induction hypothesis]}\\ &= n+((m+l)+1) \text{ [axiom (4b)]}\\ &= n+(m+(l+1)) \text{ [axiom (4b)],}\end{aligned}$$

and we conclude that $l+1 \in S$ as well.
(2) Let S be the set of $n \in \mathbb{N}$ such that $0+n = n$ and $1+n = n+1$. Then $0 \in S$ by axiom (4a), and if $n \in S$ then by axiom (4b), $0+(n+1) = (0+n)+1$ which equals $n+1$since $n \in S$, and similarly $1+(n+1) = (1+n)+1 = (n+1)+1$.

(3) Let S be the set of $m \in \mathbb{N}$ such that for all $n \in \mathbb{N}$, $n+m = m+n$. We have just shown that $0,1 \in S$. Assume now that $m \in S$. Then

$$\begin{aligned} n+(m+1) &= (n+m)+1 \text{ [axiom (4b)]} \\ &= 1+(n+m) \text{ [part (2)]} \\ &= 1+(m+n) \text{ [induction hypothesis]} \\ &= (1+m)+n \text{ [part (1)])} \\ &= (m+1)+n \text{ [part (2)].} \end{aligned}$$

(4) Let S be the set of $l \in \mathbb{N}$ for which the claim holds for all $n,m \in \mathbb{N}$. $0 \in S$ by axiom (4a). If $l \in S$ and $n,m \in \mathbb{N}$ satisfy $n+(l+1) = m+(l+1)$ then by axiom (4b), we have $(n+l)+1 = (m+l)+1$. By axiom (2) this implies $n+l = m+l$ and we now use the induction hypothesis to conclude $n = m$.

□

PROPOSITION 5. *(multiplication) For all $l,m,n \in \mathbb{N}$:*

(1) *(Distributivity) $l \cdot (m+n) = l \cdot m + l \cdot n$.*
(2) *(Associativity) $(l \cdot m) \cdot n = l \cdot (m \cdot n)$.*
(3) *(Identity) $1 \cdot n = n \cdot 1 = n$.*
(4) *(Commutativity) $m \cdot n = n \cdot m$.*
(5) *(Cancellation) If $n \cdot l = m \cdot l$ and $l \neq 0$ then $n = m$.*

PROOF. Exercise. □

DEFINITION 6. (Order) For $m,n \in \mathbb{N}$ say that $m \leq n$ if these exists $a \in \mathbb{N}$ such that $n = m+a$.

PROPOSITION 7. *(Order) For all $k,l,m,n \in \mathbb{N}$:*

(1) *If $n \neq 0$ then $n = m+1$ for some $m \in \mathbb{N}$.*
(2) *$m+l = 0$ iff $m = l = 0$.*
(3) *(Addition) $m \leq n$ iff $m+l \leq n+l$, and if $m \leq n$ and $k \leq l$ then $m+k \leq n+l$.*
(4) *(Discreteness) If $m \leq n$ and $m \neq n$ then $m+1 \leq n$.*
(5) *(Reflexivity) $n \leq n$.*
(6) *(Transitivity) If $l \leq m$ and $m \leq n$ then $l \leq n$.*
(7) *(Trichotomy I) At least one of $m \leq n$ and $n \leq m$ holds.*
(8) *(Trichotomy II) If $m \leq n$ and $n \leq m$ then $n = m$.*
(9) *(Multiplication) If $l \neq 0$ then $m \leq n$ iff $m \cdot l \leq n \cdot l$.*

PROOF.

(1) Let S be the set of $n \in \mathbb{N}$ such that either $n = 0$ or n is a successor of an element of $\mathbb{N}$. Then $0 \in S$ by definition, also $n+1 \in S$ for all $n \in S$ since this holds for n whatsoever. We conclude that $S = \mathbb{N}$.
(2) If $l \neq 0$ then $l = t+1$. Then $(m+l) = (m+t)+1 \neq 0$ by axiom (1). If $m \neq 0$ then $m+l = l+m \neq 0$ for the same reason. If $m = l = 0$ then indeed $m+l = 0$.
(3) If $n = m+a$ iff $n+l = m+l+a$ by associativity, commutativity and cancellation. If $n = m+a$ and $l = k+b$ then $n+l = (m+k)+(a+b)$.
(4) Say $n = m+a$. If $a = 0$ then $n = m$. Otherwise, by part (1) we have $a = b+1$, so that $n = m+(b+1) = (m+1)+b$.

(5) For all n we have $n = n+0$.
(6) If $m = l+a$ and $n = m+b$ then $n = (l+a)+b = l+(a+b)$ by associativity of addition.
(7) Let S be the set of m such that all $n \in \mathbb{N}$ satisfy either $m \leq n$ or $n \leq m$. Since $0 \leq n$ for all n, $0 \in S$. Assume next that $m \in S$, and let $n \in \mathbb{N}$. Then either $n \leq m$ or $n \geq m$. In the first case we have $n \leq m+1$ by transitivity since $m \leq m+1$ holds by definition. In the second case either $n = m$, at which point $n \leq m+1$, or $n \neq m$, as which point $n \geq m+1$ by part (4). We conclude that $m+1 \in S$.
(8) Say that $m+a = n$ and $n+b = m$. It follows that $m+(a+b) = m$, and by the cancellation property that $a+b = m$. Now use part (2).
(9) Let S be the set of l for which either $l = 0$ or, for all $m,n \in \mathbb{N}$, $m \leq n$ implies $m \cdot l \leq n \cdot l$. Assume that $l \in S$. If $l = 0$ then clearly $l+1 = 1 \in S$. Otherwise, for every $m \leq n \in \mathbb{N}$, $m \cdot l \leq n \cdot l$ and $m \leq n$ imply $m \cdot (l+1) \leq n \cdot (l+1)$ by part (3) and the distributive law. Finally, assume $m,n \in \mathbb{N}$ and $l \in \mathbb{N} \setminus \{0\}$ satisfy $m \cdot l \leq n \cdot l$. If $m \leq n$ we are done and otherwise by part (7) we have $n \leq m$ and hence $n \cdot l \leq m \cdot l$. By part (8) we then have $m \cdot l = n \cdot l$ and by the cancellation property of multiplication we have $m = n$, hence $m \leq n$ anyway.

□

THEOREM 8. *(Well-ordering principle) Every non-empty $S \subset \mathbb{N}$ has a least element (an element $l \in S$ such that for all $n \in S$, $n \geq l$).*

PROOF. Let T be the set of integers m with the property that if $m \in S \subset \mathbb{N}$ then S has a least element. $0 \in T$ since if $0 \in S$ then clearly 0 is the least element of S. Now assume $m \in T$ and let $(m+1) \in S \subset \mathbb{N}$. If $m \in S$ also then S has a least element and we are done. Otherwise consider the set $S' = S \cup \{m\}$. By the induction hypothesis it has a least element, say l, and clearly $l \leq m$. If $l \neq m$ then $l \in S$, and it is smaller than any other element of S since $S \subset S'$. If m is the least element of S' then every element of S is at least m but distinct from m, hence at least $m+1$ by the Proposition. It follows that $(m+1) \in S$ is the least element. □

LEMMA 9. *Let $T \subset \mathbb{Z}$ be non-empty and bounded below (above). Then T has a least (greatest) element.*

PROOF. Let m be a lower bound for T, and consider the set $T - m = \{t - m \mid t \in T\}$. This is a set of natural numbers, hence has a least element $t_0 - m$. But then t_0 is a least element of T. Similarly, if M is an upper bound for T we use a least element of $M - T = \{M - t \mid t \in T\}$. □

2.2. Aside: From natural numbers to integers

2.2.1. Quick-and-dirty construction.

- Let $\mathbb{N}_{\geq 1} = \mathbb{N} \setminus \{0\}$, and define $\mathbb{Z}$ as the union:

$$\mathbb{Z} = \mathbb{N}_{\geq 1} \bigcup \{0\} \bigcup \left\{n' \mid n \in \mathbb{N}_{\geq 1}\right\} .$$

  In other words, if n is a positive natural number then $\mathbb{Z}$ contains two elements, denoted n and n' (read “n prime”). Of course later n' will be the negative of n.
- Next, define two unary operations for $z \in \mathbb{Z}$:

- "negation"

$$-z \overset{\text{def}}{=} \begin{cases} n' & z = n, n \in \mathbb{N}_{\geq 1} \\ 0 & z = 0 \\ n & z = n', n \in \mathbb{N}_{\geq 1} \end{cases}.$$

- "magnitude" or "absolute value"

$$|z| \overset{\text{def}}{=} \begin{cases} n & z = n, n \in \mathbb{N}_{\geq 1} \\ 0 & z = 0 \\ n & z = n', n \in \mathbb{N}_{\geq 1} \end{cases}.$$

- "sign"

$$\operatorname{sgn}(z) \overset{\text{def}}{=} \begin{cases} 1 & z = n, n \in \mathbb{N}_{\geq 1} \\ 0 & z = 0 \\ 1' & z = n', n \in \mathbb{N}_{\geq 1} \end{cases}$$

- Next, for natural numbers a,b with $a \leq b$ define $b -_{\mathbb{N}} a$ to be the integer c such that $a+c = b$ (exists since $a \leq b$).
- Now, for $w,z \in \mathbb{Z}$ we define their sum as follows: first, order them so that $|w| \geq |z|$. Then set:

$$w +_{\mathbb{Z}} z \overset{\text{def}}{=} \begin{cases} w +_{\mathbb{N}} z & w,z \in \mathbb{N} \\ w -_{\mathbb{N}} (-z) & w \in \mathbb{N}, -z \in \mathbb{N} \\ -((-w) -_{\mathbb{N}} z) & -w \in \mathbb{N}, z \in \mathbb{N} \\ -((-w) +_{\mathbb{N}} (-z)) & -w, -z \in \mathbb{N} \end{cases}.$$

- Similarly, set

$$w \cdot_{\mathbb{Z}} z \overset{\text{def}}{=} \begin{cases} |w| \cdot_{\mathbb{N}} |z| & \operatorname{sgn}(w) = \operatorname{sgn}(z) \\ -|w| \cdot_{\mathbb{N}} |z| & \operatorname{sgn}(w) \neq \operatorname{sgn}(z) \end{cases}.$$

- Finally, say that $z \geq w$ if $z +_{\mathbb{Z}} (-w) \in \mathbb{N}$.
- Then one deduces all the properties of addition, multiplication, and order by dividing into cases according to the signs and relative magnitudes of the arguments and going back to the proofs of the properties for $\mathbb{N}$.

2.2.2. Systematic construction.

- Let $D = \mathbb{N} \times \mathbb{N}$ be the set of all pairs of natural numbers (to be thought of as *differences*, that is think of the pair (a,b) as the difference $a-b$.
- Define the following operations on pairs:

$$-(a,b) \overset{\text{def}}{=} (b,a),$$

$$\operatorname{sgn}(a,b) \overset{\text{def}}{=} \begin{cases} (1,0) & a > b \\ (0,0) & a = b \\ (0,1) & a < b \end{cases},$$

$$(a,b) + (c,d) \overset{\text{def}}{=} (a+c, b+d),$$

$$(a,b) \cdot (c,d) \overset{\text{def}}{=} (ac+bd, ad+bc),$$

$$|(a,b)| = \operatorname{sgn}(a,b) \cdot (a,b).$$

- Prove the associative and commutative laws for addition and multiplication and the distributive law from the properties of the natural numbers. Check that $(0,0)$ is a neutral element for addition and that $(a,b)+(-(a,b)) = (0,0)$. Check that $(1,0)$ is a neutral element for addition.
- Now say Say that $(a,b) \geq (c,d)$ iff $a+d \geq b+c$. In particular, we call two pairs $(a,b),(a',b') \in \mathbb{N} \times \mathbb{N}$ *equivalent* if $a+b' = a'+b$ (note that this only uses addition of natural numbers).
- Check that the operations above respect equivalence. For example, if you replace (a,b) and (c,d) by equivalent pairs (a',b') and (c',d') then $(a,b)+(c,d)$ and $(a',b')+(c',d')$ are equivalent.
- Let $\mathbb{Z}$ be the set of *equivalence classes* of pairs. In other words, every element $z \in \mathbb{Z}$ in this construction is the set of all pairs that are equivalent to a given pair. Define operations on $\mathbb{Z}$ by taking representatives.
- Identify every $n \in \mathbb{N}$ with the equivalence class of the pair $(n,0)$. Check that this is an embedding respecting all operations of arithmetic, and that for every element of $\mathbb{Z}$ either it or its negative corresponds to a natural number.

Math 342 Problem set 2 (due 20/9/11)

The natural numbers

1. Prove parts (1),(2),(3) of Proposition 5 on page 12 of the lecture notes.
   Hint: In each case you need to choose which variable you want to use for your induction.

Division with remainder

2. (Parity)
   (a) Show that every integer m is of one of the forms $2n$, $2n+1$ for another integer n by quoting the Division Theorem. We call integers of the first form *even*, of the second *odd*, and call this property *parity* (for example, you can say that 5 has *odd parity*).
   (b) What is the parity of 10? 17? -9?
   (c) Show that the parity of the sum of two integers only depends on the parity of these integers, not on their values. Make an addition table for parities and compare it with the addition table of $\mathbb{F}_2$.

   [You should now figure out for yourself how to use the usual properties of addition in $\mathbb{Z}$ such associativity and commutativity to deduce the corresponding properties in $\mathbb{F}_2$.]

3. (PS1 problem 5, again)
   (a) What are the possible remainders when dividing an integer by 3?
   (b) By writing an arbitrary integer m in the form $3n+r$, show that one of $m, m+1, m+2$ is divisible by 3.
   Hint: divide into cases depending on the value of r.
   (c) Is this solution fundamentally different from the one given in Problem Set 1? In other words, where did we use induction to get this solution?

The Fibonacci sequence

Let $\{a_n\}_{n=0}^{\infty}$ be the sequence of integers defined as follows: $a_0 = 0$, $a_1 = 1$, and for $n \geq 1$, $a_{n+1} = a_n + a_{n-1}$. (Story: at month 1 we introduce a pair of newborn rabbits into the country; every pair of rabbits takes one month to mature, after which they spawn another pair every month; thus the number of pairs of rabbits at any month equals the number of pairs the previous month, plus one new pair for each pair that was alive the month before).

4. Calculate a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 and check that $a_{10} = 55$.

5. For $1 \leq n \leq 10$ calculate the ratio $\frac{a_n}{a_{n-1}}$ to three decimal digits.

6. Let $R > 1$ be a solution of $x^2 - x - 1 = 0$. Calculate R to three decimal digits.

7. (§3D.E70(i)) Show that $a_n = \frac{R^n - r^n}{R - r}$ for all n, where r is the other solution to the equation.
   Hint: Check the cases $n = 0$, $n = 1$ by hand and use induction.

REMARK. We will return to this sequence in the next problem set.

2.3. Division with remainder

Let n, a be integers, $a \geq 1$. Let T be the set of natural numbers k such that $n-k$ (an element of $\mathbb{Z}$) is divisible by a. T is non-empty since $|n|\,a \geq |n|$. Let r be the smallest element of T. Then $n-r$ is divisible by a, and we conclude that

$$n = qa + r\,.$$

If $r \geq a$ then $r - a \geq 0$ and $(r-a) \in T$, a contradiction, so $0 \leq r \leq a-1$.

If we also had $n = q'a + r'$ with $r' \geq r$ then $0 \leq r' - r \leq r' < a$ would be divisible by a. Conclude $r = r'$ and hence $q' = q$.

DEFINITION 10. Call r the *remainder* of dividing n by a.

2.4. gcd and lcm

DEFINITION 11. An integer a is said to *divide* the integer b if there is a third integer c such that $ac = b$.

EXAMPLE 12. Every integer is divisible by 1 and itself. 0 is divisible by every integer (including itself).

Let $a, b \in \mathbb{Z}$ be non-zero. Let D be the set of common divisors of a and b (non-empty since $1 \in D$). D is bounded since every divisor of a is no larger than $|a|$. Let M be the set of positive common multiples of a, b (non-empty since $|ab| = \pm ab \in M$).

DEFINITION 13. $(a,b) \overset{\text{def}}{=} \gcd\{a,b\} = \max D$; $[a,b] \overset{\text{def}}{=} \operatorname{lcm}\{a,b\} = \min M$. Also, for all $a \in \mathbb{Z}$, set $(a,0) = a$ and $[a,0] = 0$.

FACT 14. *Every common divisor of a, b divides (a,b). Every common multiple of a, b is divisible by $[a,b]$.*

LEMMA 15. *(Euclid) Let $x, y \in \mathbb{Z}$. Then $(x,y) = (x-y, y)$.*

PROOF. We prove that both pairs have the same set of common divisors. Indeed, let d divide y. If d also divides x then d divides $x-y$. Conversely, if d divides $x-y$ then d divides $x = (x-y)+y$. □

Since $(x,0) = x$ for all x, and since changing the signs of x,y does not change their gcd (why?) we get a method for calculating the gcd of any two integers. For example:

$$\begin{aligned}
(24,-153) &= (153,24) \\
&= (129,24) \\
&= (105,24) \\
&= (81,24) \\
&= (57,24) \\
&= (33,24) \\
&= (24,9) \\
&= (15,9) \\
&= (9,6) \\
&= (6,3) \\
&= (3,3) \\
&= (3,0) \\
&= 3\,.
\end{aligned}$$

ALGORITHM 16. *(Euclid) Given two integers x,y, output their* gcd*:*

1. *Replace x with $|x|$, y with $|y|$.*
2. *If $x < y$ exchange x and y.*
3. *If $y = 0$, terminate and output x.*
4. *Else, replace x with $x - y$ and go to step* 2.

THEOREM 17. *The algorithm terminates after finitely many steps and outputs the* gcd *of* (x,y).

PROOF. Consider the changes in the quantity $|x| + |y|$ during the course of the algorithm. Every time we reach step 4, we know that $x \geq y > 0$. It follows that at the conclusion of step 4, the quantity has decreased by at least $y \geq 1$. Since there is no infinite strictly decreasing sequence of natural numbers (well-ordering), we can reach step 4 only finitely many times. In particular, at some point $y = 0$ and we terminate. Finally, by Lemma 15, the replacements and exchanges never change the gcd of the two numbers. □

In fact, more can be said.

CLAIM 18. (Bezout) Every intermediate value considered by Euclid's Algorithm is of the form $ax + by$ for some $a,b \in \mathbb{Z}$.

PROOF. We prove this by induction on the steps of the algorithm. Certainly this is true at the start, and also changing signs and exchanging x,y doesn't matter. Now assume that at the nth time we reach step 3, we are looking at the numbers $x' = ax + by > y' = cx + dy$, where x,y are the initial values and $a,b,c,d \in \mathbb{Z}$. At step 4 we will then replace x' with

$$x' - y' = (a-c)x + (b-d)y$$

which is indeed also of this form, so the situation will hold when we reach step 3 for the $(n+1)$st time. □

We have thus proven (by algorithm) the following fact:

THEOREM 19. *(Bezout) Given $x,y \in \mathbb{Z}$ the exist $a,b \in \mathbb{Z}$ such that $(x,y) = ax + by$.*

There is a second, direct, proof of this fact which is instructive in its own right and does not use Euclid's algorithm.

COROLLARY 20. *Every common divisor of x,y divides their* gcd – *since every common divisor divides every number of the form $ax + by$.*

REMARK 21. Euclid's algorithm allows us to compute the coefficients, by writing each intermediate value in terms of the original x and y. For example:

$$\begin{array}{rcll}
(24,-153) & = & (153,24) & \\
 & = & (129,24) & 129 = -(-153) - 24 \\
 & = & (105,24) & 105 = -(-153) - 2 \cdot 24 \\
 & = & (81,24) & 81 = -(-153) - 3 \cdot 24 \\
 & = & (57,24) & 57 = -(-153) - 4 \cdot 24 \\
 & = & (33,24) & 33 = -(-153) - 5 \cdot 24) \\
 & = & (24,9) & 9 = -(-153) - 6 \cdot 24 \\
 & = & (15,9) & 15 = 24 - 9 = (-153) + 7 \cdot 24 \\
 & = & (9,6) & 6 = 15 - 9 = 2 \cdot (-153) + 13 \cdot 24 \\
 & = & (6,3) & 3 = 9 - 6 = (-3) \cdot (-153) - 19 \cdot 24 \\
 & = & (3,3) & \\
 & = & (3,0) & \\
 & = & 3\,. &
\end{array}$$

Math 342 Problem set 3 (due 27/9/11)

The natural numbers

1. Using the division Theorem, prove that if a,b are two non-zero integers then every common multiple of a,b is divisible by the least common multiple $[a,b]$.
   Hint: Show that the remainder obtained when dividing one common multiple by another is also a common mulitple.

2. Prove Bezout's Theorem as follows: Given $a,b \in \mathbb{Z}$ not both zero let $I = \{xa+by \mid x,y \in \mathbb{Z}\}$. Show that the smallest positive member of I is the gcd of a,b.
   Hint: You need to show that I has positive members. To show that the number your produced divides a and b use the idea of problem 1.

Using Euclid's Algorithm

DEFINITION. We say that two integers a,b are *relatively prime* (or *coprime*) if $(a,b) = 1$.

3. For every integer n show that n and $n+1$ are relatively prime.

4. Find the gcd of 98 and 21 using subtractions only (list your intermediate steps).

5. (§3A.E7) Improving Euclid's algorithm with the idea of division with remainder, find the gcd of 21063 and 43137, listing your intermediate steps (you may want to use a calculator). How many remainders did you calculate?

Using Bezout's Theorem

6.
   (a) Using Euclid's Algorithm, find integers r,s such that $12r+17s = 1$.
   (b) Find integers m,n such that $12m+17n = 8$.
   (c) You take a 12-quart jug and a 17-quart jug to a stream. How would you bring back exactly 8 quarts of water?

The efficiency of Euclid's Algorithm

Let $a > b > 0$ be two integers, and let $0 = r_0 < r_1 < r_2 < \cdots < r_{T-1}$ be the remainders calculated by the improved algorithm using remainders (starting with a,b), *in reverse order*. In other words, $r_0 = 0$ is the remainder of the final, exact, division of r_2 by r_1. r_1 is the remainder when dividing r_3 by r_2 and so on, all the way to r_{T-1} which is the remainder of dividing a by b (which we denote r_T). Note that T is the number of divisions performed during the run.

Let $\{a_n\}_{n=0}^{\infty}$ be the Fibonacci sequence from Problem Set 2.

7. Prove by induction on n that, for $0 \le n \le T$, we have $a_n \le r_n$.
   Hint: For the induction step, express r_{n+1} using r_n, r_{n-1} and the quotient in the division, and use the defining property of the Fibonacci sequence.

8. The case $n = T$ of what you just proved reads: $a_T \leq b$. In the previous problem set you showed that for $T \geq 1$, $a_T \geq \frac{1}{3}R^T$ where $R = \frac{1+\sqrt{5}}{2}$. Conclude that, when running the improved algorithm on (a,b) one needs at most $C \log b + D$ divisions, where C, D are two constants. What are C, D?

Solving congruences

9. For each $a \in \{0,1,2\}$ find all $x \in \mathbb{Z}$ such that x^2 leaves remainder a when divided by 3.
Hint: first show that the remainder of x^2 only depends on that of x, and then divide into cases based on the latter remainder.

2.5. Unique Factorization

DEFINITION 22. Call $p \in \mathbb{N}$ *prime* if the only positive divisors of p are $\{1, p\}$, in other words if whenever $ab = p$ with $a, b \in \mathbb{N}$ we have $a = 1$, $b = p$ or $a = p$, $b = 1$.

REMARK 23. If p is prime and $n \in \mathbb{Z}$ then either $(n, p) = 1$ or $p|n$, depending on which divisor of p is the greatest common divisor.

THEOREM 24. *(Euclid) Every integer ≥ 2 can be written as a product of primes.*

PROOF. Let a be the smallest integer ≥ 2 that cannot be written as a product of primes. Then a cannot be prime. Thus we have $a = bc$ with $1 < b, c < a$. But then b, c can be written as a product of primes, and hence so can their product. □

LEMMA 25. *If $p \mid ab$ then $p|a$ or $p|b$.*

PROOF. Assume $(p, a) = 1$. By Bezout's Theorem there exists x, y such that $xp + ya = 1$. Multiply this identity by b to conclude

$$b = xpb + yab\,.$$

Now $p|xpb$ and $p|yab$ since $p|ab$. We conclude that $p|b$. □

THEOREM 26 (Fundamental Theorem of Arithmetic). *Every positive integer can be written as a (potentially empty) product of primes,* uniquely up to reordering the factors. *More formally, if $\{p_i\}_{i=1}^{n}$ and $\{q_j\}_{j=1}^{m}$ are sequences of not necessarily distinct primes such that*

$$\prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_j$$

then $n = m$ and each prime number ℓ appears in both lists exactly the same number of times.

PROOF. Let a be the smallest number for which the statement fails. Since any non-empty product of primes is at least 1, $a \geq 2$. By Euclid's Theorem, we know that a can be written as a product of primes in at least one way, so n must have more than one representation as a product of primes, say:

$$a = \prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_j\,.$$

Then $p_n \mid a$ and hence $p_n \mid \prod_j q_j$. From Lemma 25, we must have $p_n \mid q_j$ for some j. Reordering the factors we may assume $p_n \mid q_m$. Since q_m is prime this means $p_n = q_m$. Dividing both sides by this prime we conclude:

$$\prod_{i=1}^{n-1} p_i = \frac{a}{p_n} = \frac{a}{q_m} = \prod_{j=1}^{m-1} q_j\,.$$

Now $\frac{a}{p_n} < a$. Thus this number has a *unique* factorization. It follows that $n - 1 = m - 1$ (in particular $n = m$) and that the lists of both sides are the same up to reordering. Adding the extra prime $p_n = q_m$ shows that the original lists were also the same. □

NOTATION 27. We sometimes write the factorization as $n = \prod_p p^{e_p}$. The product ranges over all primes, but $e_p = 0$ for all but finitely many. The Theorem then states that e_p depend only on n, that is there is only one choice of e_p that makes this an equality. We sometimes write this as $v_p(n)$. This is the largest e such that $p^e|n$. We sometimes write this fact as $p^e \| n$ and say that p^e divides n *exactly*.

Applications of unique factorization.

PROPOSITION 28. *Let $n = \prod_p p^{e_p}$and $m = \prod_p p^{f_p}$, $l = \prod_p p^{g_p}$with $e_p, f_p, g_p \in \mathbb{N}$ and almost all are zero. Then*

(1) *$n|m$ iff $e_p \leq f_p$ for all p;*
(2) *$(n,m) = \prod_p p^{\min\{e_p,f_p\}}$ and every common divisor of $\{n,m\}$ divides the gcd;*
(3) *$[n,m] = \prod_p p^{\max\{e_p,f_p\}}$ and every common multiple of $\{n,m\}$ is divisible by the lcm;*
(4) *$(n,m) \cdot [n,m] = nm$.*

PROOF. If $e_p \leq f_p$ for all p then $m = \prod_p p^{(f_p - e_p)}$ (for almost all p, we have $f_p - e_p = 0 - 0$ so this is an integer). Conversely, if $m = nl$ then $f_p = e_p + g_p \geq e_p$. It follows that l is a common divisor of m and n iff $g_p \leq e_p$ and $g_p \leq f_p$ for all p, that is iff $g_p \leq \min\{e_p, f_p\}$. It follows that the stated product is the gcd and that every common divisor divides it. Part (3) follows by a similar argument. To check the last claim we compare the factorizations of both sides. The exponent at p on the LHS is $\min\{e_p, f_p\} + \max\{e_p, f_p\}$, on the RHS it is $e_p + f_p$, and the two are clearly equal. □

LEMMA 29. *$n = \prod_p p^{e_p}$ is a d-th power iff $d|e_p$ for all p.*

PROOF. Let $m = \prod_p p^{f_p}$ and assume $n = m^d$. Then $e_p = d \cdot f_p$ for all p and hence is divisible by d. Conversely, if e_p is divisible by d for all p then $n = \left(\prod_p p^{(e_p/d)}\right)^d$ (note that e_p/d is zero for almost all p). □

THEOREM 30 (Irrationality of $\sqrt{2}$). *$n = \prod_p p^{e_p}$is a d-th power of a rational number iff $d|e_p$ for all p.*

PROOF. One direction is contained in the Lemma. For the converse, assume that $n = \left(\frac{a}{b}\right)^d$ for some non-zero $a, b \in \mathbb{N}$. Say that $a = \prod_p p^{f_p}$ and $b = \prod_p p^{g_p}$. We write the prime factorization of a^d in two forms:

$$\prod_p p^{df_p} = a^d = nb^d = \prod_p p^{e_p + dg_p}.$$

The uniqueness of the factorization shows $df_p = e_p + dg_p$, and hence that $e_p = d(f_p - g_p)$ is divisible by d. □

COROLLARY 31. *There is no rational number $r \in \mathbb{Q}$ such that $r^2 = 2$.*

Math 342 Problem set 4 (due 4/10/11)

The natural numbers

1. Show, for all $a,b,c \in \mathbb{Z}$ with $c > 0$:
   (a) (cancellation from both sides) $(ac,bc) = c\,(a,b)$.
   (b) (cancellation from one side) If $(a,c) = 1$ then $(a,bc) = (a,b)$
   Hint: can either do these directly from the definitions or using Prop. 28 from the notes.

2. ($\sqrt{15}$ and friends)
   (a) Show that $\sqrt{3}$ and $\sqrt{15}$ are irrational.
   Hint: Use a Theorem from class.
   (*b) Show that $\sqrt{5}$ is not of the form $a + b\sqrt{15}$ for any $a,b \in \mathbb{Q}$.
   Hint: Assuming that $\sqrt{5} = a + b\sqrt{15}$ start by squaring both sides and using that $\sqrt{15} \notin \mathbb{Q}$ to learn something about a,b (but that's not the end of the problem ...)
   SUPP For any $a,b \in \mathbb{Q}$ show that $a\sqrt{2} + b\sqrt{3}$ is irrational unless $a = b = 0$.

Factorization in the integers and the rationals

3. Let $r \in \mathbb{Q} \setminus \{0\}$ be a non-zero rational number.
   (a) Show that r can be written as a product $r = \varepsilon \prod_p p^{e_p}$ where $\varepsilon \in \{\pm 1\}$ is a sign, all $e_p \in \mathbb{Z}$, and all but finitely many of the e_p are zero.
   Hint: Write $r = \varepsilon a/b$ with $\varepsilon \in \{\pm 1\}$ and $a,b \in \mathbb{Z}_{\geq 1}$.
   (b) Write $\frac{58}{493}$, $-\frac{105}{99}$ as products of integral powers of primes.
   (c) Prove that the representation from (a) is unique, in other words that if we also have $r = \varepsilon' \prod_p p^{f_p}$ for $\varepsilon' \in \{\pm 1\}$ and $f_p \in \mathbb{Z}$ almost all of which are zero, then $\varepsilon' = \varepsilon$ and $f_p = e_p$ for all p.
   Hint: Start by separating out the prime factors with positive and negative exponents on each side.

Ideals (an exercize with definitions)

DEFINITION. Call a non-empty subset $I \subset \mathbb{Z}$ an *ideal* if it is closed under addition (if $x,y \in I$ then $x + y \in I$) and under multiplication by elements of $\mathbb{Z}$ (if $x \in I$ and $z \in \mathbb{Z}$ then $xz \in I$).

4. For $a \in \mathbb{Z}$ let $(a) = \{ca \mid c \in \mathbb{Z}\}$ be the set of multiples of a. Show that (a) is an ideal. Such ideals are called *principal*.
   Hint: This rephrases facts that you know about divisibility. You need to show, for example, that if x and y are multiples of a then $x + y$ is also a multiple.

5. Let $I \subset \mathbb{Z}$ be an ideal. Show that I is principal.
   Hint: Use the argument from the second proof of Bezout's Theorem.

6. For $a,b \in \mathbb{Z}$ let (a,b) denote the set $\{xa + yb \mid x,y \in \mathbb{Z}\}$. Show that this set is an ideal. By problem 5 we have $(a,b) = (d)$ for some $d \in \mathbb{Z}$. Show that d is the GCD of a and b. This justifies using (a,b) to denote both the gcd of the two numbers and the ideal generated by the two numbers.

SUPP Let $I,J \subset \mathbb{Z}$ be ideals. Show that $I \cap J$ is an ideal, that is that the intersection is non-empty, closed under addition, and closed under multiplication by elements of $\mathbb{Z}$.

8. For $a,b \in \mathbb{Z}$ show that the set of common multiples of a and b is precisely $(a) \cap (b)$. Use the previous problem and problem 5 to show that every common multiple is a divisible by the least common multiple.

Congruences

9. Using the fact that $10 \equiv -1\,(11)$, find a simple criterion for deciding whether an integer n is divisible by 11. Use your criterion to decide if 76443 and 93874 are divisible by 11.

10. For each integer a, $1 \leq a \leq 10$, check that $a^{10} - 1$ is divisible by 11.

Supplmenetary problems: The p-adic distance

For an rational number r and a prime p let $v_p(r)$ denote the exponent e_p in the unique factorization from problem 3. Also set $v_p(0) = +\infty$ (∞ is a formal symbol here).

A. For $r,s \in \mathbb{Q}$ show that $v_p(rs) = v_p(r) + v_p(s)$, $v_p(r+s) \geq \min\left\{v_p(r), v_p(s)\right\}$ (when r, s, or $r+s$ is zero you need to impose rules for arithmetic and comparison with ∞ so the claim continues to work).

For $a \neq b \in \mathbb{Q}$ set $|a-b|_p = p^{-v_p(a-b)}$ and call it the p-adic *distance* between a,b. For $a = b$ we set $|a-b|_p = 0$ (in other words, we formally set $p^{-\infty} = 0$). It measure how well $a-b$ is divisible by p.

B For $a,b,c \in \mathbb{Q}$ show the *triangle inequality* $|a-c|_p \leq |a-b|_p + |b-c|_p$.
Hint: $(a-c) = (a-b) + (b-c)$.

C. Show that the sequence $\{p^n\}_{n=1}^{\infty}$ converges to zero in the p-adic distance (that is, $|p^n - 0|_p \to 0$ as $n \to \infty$).

REMARK. The sequence $\{p^{-n}\}_{n=1}^{\infty}$ cannot converge in this notion of distance: if it converged to some A then, after some point, we'll have $|p^{-n} - A|_p \leq 1$. By the triangle inequality this will mean $|p^{-n}|_p \leq |A|_p + 1$. Since $|p^{-n}|_p$ is not bounded, there is no limit. The notion of p-adic distance is central to modern number theory.

Supplmenetary problems: Divisors

Let $\tau(n)$ denote the number of divisors of n (e.g. $\tau(2) = 2$, $\tau(4) = 3$, $\tau(12) = 6$). Let $\sigma(n)$ denote the sum of divisors of n (e.g. $\sigma(2) = 3$, $\sigma(4) = 7$, $\sigma(12) = 28$).

D. Let $n = \prod_p p^{e_p}$. Show that $\tau(n) = \prod_p (e_p + 1)$, and from this that if $(n,m) = 1$ then $\tau(nm) = \tau(n)\tau(m)$ (we say "$\tau(n)$ is a *multiplicative function*").

E. Find a formula for $\sigma(n)$ in terms of the prime factorization, and show that $\sigma(n)$ is also multiplicative.

CHAPTER 3

Congruence in the Integers (27/9-13/10)

3.1. Congruence and Congruence Classes

DEFINITION 32. (Gauss) Let $a,b,m \in \mathbb{Z}$ with $m \neq 0$. We say that *a is congruent to b modulu m* if m divides $a-b$, that is if $a-b=km$ for some $k \in \mathbb{Z}$. This is also denoted:

$$a \equiv b\,(m)$$

and

$$a \equiv b \mod (m)\,.$$

Note that, by definition, $a \equiv b\,(m)$ iff $a = b+km$ for some $k \in \mathbb{Z}$.

DEFINITION 33. The set $[b]_m = \{b+km \mid k \in \mathbb{Z}\}$ of all integers congruent to $b \mod m$ is called the *congruence (*or *residue) class of b (modulu m).*

LEMMA 34. *Let $m \in \mathbb{Z} \setminus \{0\}$. Then congruence $\mod m$ is an equivalence relation. In other words:*

(1) *(Reflexivity) For all $a \in \mathbb{Z}$, $a \equiv a\,(m)$.*
(2) *(Symmetry) For all $a,b \in \mathbb{Z}$, if $a \equiv b\,(m)$ then $b \equiv a\,(m)$.*
(3) *(Transitivity) For all $a,b,c \in \mathbb{Z}$, if $a \equiv b\,(m)$ and $b \equiv c\,(m)$ then $a \equiv c\,(m)$.*

PROOF. In order:

(1) $a-a=0$ is divisible by all m.
(2) If m divides $a-b$ then it also divides $(-1)\cdot(a-b) = b-a$.
(3) If $a=b+km$ and $b=c+lm$ then $a=c+km+lm=c+(k+l)m$. Alternatively, $a-c=(a-b)+(b-c)$.

□

PROPOSITION 35. *(Arithmetic only depends on the congruence class) Let $a \equiv a'\,(m)$, $b \equiv b'\,(m)$. Then:*

(1) $a+b \equiv a'+b'\,(m)$.
(2) $-a \equiv -a'\,(m)$.
(3) $ab \equiv a'b'\,(m)$.

PROOF. In order:

(1) $(a+b)-(a'+b') = (a-a')+(b-b')$ and both summands on the right are divisible by m.
(2) $(-a)-(-a') = (-1)\cdot(a-a')$ so is divisible by m.

(3) Say $a = a' + km$, $b = b' + lm$. Then

$$\begin{aligned} ab &= (a'+km)(b'+lm) \\ &= a'b' + a'lm + kmb' + kmlm \\ &= a'b' + (a'l + b'k + klm)m \\ &\equiv a'b'\,(m)\,. \end{aligned}$$

□

EXAMPLE 36. Let $n = \sum_{i=0}^{d} a_i \cdot 10^i$ with $a_i \in \mathbb{Z}$. Then $n \equiv S(n) \overset{\text{def}}{=} \sum_{i=0}^{d} a_i\,(9)$. In particular, n is divisible by 9 iff the sum-of-digits $S(n)$ is.

PROOF. $10 \equiv 1\,(9)$. It follows by induction that $10^i \equiv 1\,(9)$ for all i, and hence that $a_i 10^i \equiv a_i\,(9)$ for all i. □

EXAMPLE 37. Let $n = \sum_{i=0}^{d} a_i \cdot 10^i$. Then $n \equiv a_0\,(10)$. In particular, $n \equiv a_0\,(2)$ and $n \equiv a_0\,(5)$. In other words, to check if n is divisible by 2 or 5 it suffices to check its last digit.

DEFINITION 38. We say that an integer r *represents* its congruence class $[r]_m$. A set S of integers is called a *complete set of representatives* or a *system of residues* $\mod m$ if it contains exactly one representative from every congruence class $\mod m$.

THEOREM 39. *(Sets of representatives)*

(1) *Every two congruence classes are either disjoint of equal. (no partial intersection)*
(2) *The set $S_m = \{0, 1, \dots, |m| - 1\}$ is a complete set of representative $\mod m$.*
(3) *There are exactly $|m|$ congruence classes modulu m, hence every system of residues contains exactly $|m|$ elements.*
(4) *(Gauss) Every sequence of $|m|$ consecutive integers is a system of residues $\mod m$.*

PROOF. In order.

(1) Assume that $c \in [a]_m \cap [b]_m$. Then $c \equiv a\,(m)$ and $c \equiv b\,(m)$ hence $a \equiv b\,(m)$. It follows that $[a]_m = [c]_m = [b]_m$.
(2) By the Division Theorem, every integer is congruent $\mod m$ to an element of S_m. To see that it is a system of residues it suffices to make sure that no two elements of S_m belong to the same residue class. Indeed, given $r, s \in S_m$ we may assume that $0 \le r \le s < m$. Then $0 \le s - r < m - r \le m$. It follows that $0 \le (s - r) < m$. Thus $s - r$ is divisible by m iff $s - r = 0$, that is iff $s = r$.
(3) All systems of residues have the same number of elements (this is the number of residue classes). In particular, they have the same number of elements as S_m.
(4) Exercise.

□

COROLLARY 40. *Let $m' \mid m$. Then every congruence class modulu m' is a union of $\frac{m}{m'}$ congruence classes modulu m.*

PROOF. We first note that if $a \equiv b\,(m)$ then $a \equiv b\,(m')$. Thus $[a]_m \subset [a]_{m'}$ so that every congruence class modulu m' is a union of congruence classes modulu m. Now let $[a]_{m'}$ be such a class, and enumerate its members as $\{a + qm' \mid q \in \mathbb{Z}\}$. Then $a + qm' \equiv a + rm'\,(m)$ iff $m \mid (q - r)m'$. Dividing both sides by m' we see that this is the case iff $\frac{m}{m'} \mid q - r$, that is iff $q \equiv r\,(\frac{m}{m'})$. In other words, the congruence class of $a+qm'$ modulu m is determined by the congruence class of q modulu $\frac{m}{m'}$. Since there are $\frac{m}{m'}$ such classes (and we are going over all $q \in \mathbb{Z}$) we are done. □

3.2. Solving Congruences

Equal -> Equation. Similarly, Congruent -> Congruence.

LEMMA 41. *Let $a,b \in \mathbb{Z}$ and $m \in \mathbb{Z} \setminus \{0\}$. Then:*

1. *The set of solutions to the congruence $a+x \equiv b\,(m)$ is precisely the congruence class $[b-a]_m$.*
2. *If $(a,m)=1$ then there exists $\bar{a} \in \mathbb{Z}$ such that $a\bar{a} \equiv 1\,(m)$, and the set solutions to $ax \equiv 1\,(m)$ is the the congruence class $[\bar{a}]_m$, also denoted $[a]_m^{-1}$.*
3. *If $(a,m)>1$ then there is no $\bar{a} \in \mathbb{Z}$ as above.*
4. *Assume that $(a,m)=1$. Then the set of solutions to the congruence $ax \equiv b\,(m)$ is the single congruence class $[a]_m^{-1}[b]_m = [\bar{a}b]_m$.*
5. *Let $d=(a,m)$. The set of solutions to $ax \equiv b\,(m)$ is empty if $d \not| b$, and is otherwise equal to the congruence class $\left[\frac{a}{d}\right]_{m/d}^{-1}\left[\frac{b}{d}\right]_{m/d}$ modulu m/d, which is a union of d congruence classes modulu m.*

3.2.1. Example: Luhn's Algorithm. We'd like to check that a sequence of decimal digits has been typed correctly. The idea is similar to the tests for divisibility by 11, and is sensitive to both digits being changed and digits being transposed.

DEFINITION 42. For $n = \sum_{i=0}^{d} a_i 10^i$ write

$$L(n) = \sum_{i=0}^{d} \ell_i(a_i)$$

where

$$\ell_i(a) = \begin{cases} a & i \text{ even} \\ 2a & i \text{ odd}, 0 \le a \le 4 \\ 2a-9 & i \text{ odd}, 5 \le a \le 9 \end{cases}.$$

For example, we have

$$L(45802147) = 7+8+1+4+0+(6+1)+5+8 = 40.$$

Note that for i odd, $l_i(n)$ is not quite $2a_i$ mod 10: if $2a_i \ge 10$ we take the sum of the digits.

The effectiveness of $L(n)$ for checking that the number n was written correctly is given by the following:

PROPOSITION 43. *If n,n' differ only at one digit, or by transposition of adjacent digits except for* 90 ↔ 09 *then $L(n) \not\equiv L(n')\,(10)$.*

PROOF. Assume $n' = \sum_{i=0}^{d} a_i' 10^i$. Assume first that $a_i' = a_i$ except if $i=j$. And that $L(n) \equiv L(n')\,(10)$. Then

$$\begin{aligned} L(n) - L(n') &= \sum_{i=0}^{d} \left(\ell_i(a_i) - \ell_i(a_i')\right) \\ &= \ell_j(a_j) - \ell_j(a_j') \end{aligned}$$

That is

$$\ell_j(a_j) \equiv \ell_j(a'_j)\,(10)\,.$$

since for $i \neq j$ the two terms are the same. Now if j is even then we have $a_j - a'_j$. Since the two are digits this is a number between -9 and 9 and hence is divisible by 10 iff it vanishes. If j is odd then use the fact that congruence mod 10 implies congruence mod 2 to see that either both a_j, a'_j are between 0 and 4 ($l_j(a_j)$ even) or both are between 5 and 9 ($l_j(a_j)$ odd). In either case we have $2a_j \equiv 2a'_j\,(10)$, hence $a_j \equiv a'_j\,(5)$, and this gives equality since both range over the same interval of size 5.

Assume now that $a'_i = a_i$ except that we transpose a_j and a_{j+1}. Then

$$L(n) - L(n') = \ell_{j+1}(a_{j+1}) + \ell_j(a_j) - \ell_{j+1}(a_j) - \ell_j(a_{j+1})\,.$$

Calling one of the numbers a and the other b we have:

$$\ell_{\text{odd}}(a) - \ell_{\text{even}}(a) \equiv \ell_{\text{odd}}(b) - \ell_{\text{even}}(b)\,(10)\,.$$

We now consider the function $\ell_{\text{odd}}(a) - \ell_{\text{even}}(a)$. When $0 \leq a \leq 4$, this is just $2a - a = a$. When $5 \leq a \leq 9$ this is $a+1$. Thus the only way for a, b to give the same value modulu 10 is either $a = b$ or $\{a,b\} = \{0,9\}$ where both give residue 0. We can see this in the table:

a	0	1	2	3	4	5	6	7	9
$\ell_{\text{odd}}(a) - \ell_{\text{even}}(a)$	0	1	2	3	4	6	7	8	0

□

Math 342 Problem set 5 (due 11/10/11)

Congruences

1. We will calculate 15^{321} modulu 121 by a method called "repeated squaring".
   (a) Find a small representative for 15^2 modulu 121.
   (b) Find a small representative for 15^4 modulu 121 (hint: $15^4 = (15^2)^2$)
   (c) Find a small representative for 15^8 modulu 121 (hint: $15^8 = (15^4)^2$)
   (d) Find small representatives for 15^{16}, 15^{32}, 15^{64}, 15^{128} and 15^{256} modulu 121.
   (e) Write 321 as a sum of powers of two.
   (f) Using the formula $15^{a+b} \equiv 15^a \cdot 15^b \,(121)$, find a small representative for 15^{321} modulu 121 by multiplying some of the numbers you got in parts (a)-(d) (as well as $15^1 = 15$) . You should only need to use each intermediate result at most once.

2. Solve the following congruences:
   (a) $x+7 \equiv 3\,(18)$.
   (b) $5x \equiv 12\,(100)$.
   (c) $5x \equiv 15\,(100)$.
   (d) $x^2+3 \equiv 2\,(5)$.

3. For each pair of a, m belonew-york/nba/story/_/id/7088249/amare-stoudemire-new-york-knicks-nba-labor-get-deal-donew use Euclid's algorithm to find $\bar{a}$ so that $a \cdot \bar{a} \equiv 1\,(m)$.
   (a) $m = 5$, $a = 2$.
   (b) $m = 12$, $a = 5$.
   (c) $m = 30$, $b = 7$.

4. Multiplying by the inverses from the previous problem, solve the following congruences:
   (a) $2x \equiv 9\,(5)$.
   (b) $5x+3 \equiv 11\,(12)$.
   (c) $14x \equiv 28\,(60)$.

Luhn's Algorithm

5. Replace x with an appropriate final digit so that the following digit sequences satisfy Luhn's Algorithm:
   (a) $45801453x$.
   (b) $6778312x$.

6. Show that adding zero digits *on the left* to a digit sequence does not affect whether it passes the check.

7. Let $n = \sum_{i=0}^{d} a_i 10^i$ be a number written in base 10.
   (a) Show that changing any single digit, or transposing any two neighbouring digits, will change the residue class of n modulu 11.
   (b) Starting with the number 15, one of the numbers $150, 151, 152, \cdots, 159$ is divisible by 11 (which?). Find an example of a number n such that adding a digit to n on the right will never give a number divisible by 11.
   (c) Explain why the previous example rules out using the 'mod 11' algorithm in place of Luhn's algorithm.

Foundations of Modular arithmetic

8. Show that arithmetic in $\mathbb{Z}/m\mathbb{Z}$ satisfies the distributive law for multiplication over addition.

Supplementary problem

A. Explain how to use the idea of problem 1 to calculate the residue class $[a^b]_m$ using only $2(1+\log_2 b)$ multiplications instead of b multiplications. This algorithm is known as "exponentiation by repeated squaring".

3.3. $\mathbb{Z}/m\mathbb{Z}$

We give an abstract way to package modular arithmetic: we transfer the operations from the numbers to the *congruence classes*.

Fix $m > 0$.

DEFINITION 44. $\mathbb{Z}/m\mathbb{Z}$ will denote the set of congruence classes modulu m, together with the operations of addition: $[a]_m + [b_m] \overset{\text{def}}{=} [a+b]_m$ and multiplication: $[a]_m + [b_m] \overset{\text{def}}{=} [a+b]_m$, and the distinguished elements $[0]_m$ and $[1]_m$.

REMARK 45. We say "$\mathbb{Z}$ mod $m\mathbb{Z}$". Here $m\mathbb{Z}$ is the ideal (m) of multiples of $\mathbb{Z}$, and the "division" operation is of identifying two numbers if their difference belongs to $m\mathbb{Z}$ (recall the definition of residue classes).

PROPOSITION 46. *(Arithmetic in $\mathbb{Z}/m\mathbb{Z}$)*

1. *The arithmetic operations are well-defined.*
2. *The associative and commutative laws hold for both addition and multiplication.*
3. *(neutral elements) For every residue class $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ we have $[a]_m + [0]_m = [a]_m$, $[a]_m \cdot [1]_m = [a]_m$.*
4. *(additive inverse) Every residue class $[a]_m$ has an additive inverse, the residue class $[-a]_m$: $[a]_m + [-a]_m = [0]_m$.*
5. *The distributive law holds.*
6. *(units) $[a]_m$ is invertible in $\mathbb{Z}/m\mathbb{Z}$ iff $(a,m) = 1$.*

PROOF. The first statement is Proposition 35. Properties (2)-(5) follows from the same properties in $\mathbb{Z}$. We prove the associative law for addition as an example: for all $a,b,c \in \mathbb{Z}$, we have:

$$\begin{aligned}
([a]_m + [b]_m) + [c]_m &= [a+b]_m + [c]_m && \text{(by definition)} \\
& [(a+b)+c]_m && \text{(by definition)} \\
&= [a+(b+c)]_m && \text{(arithmetic in } \mathbb{Z}) \\
&= [a]_m + [b+c]_m \\
&= [a]_m + ([b]_m + [c]_m) \,.
\end{aligned}$$

Statement (6) is Lemma 41(2),(3). □

EXAMPLE 47. $\mathbb{Z}/2\mathbb{Z}$ is precisely $\mathbb{F}_2$.

EXAMPLE 48. Multiplication table of $\mathbb{Z}/6\mathbb{Z}$.

Discussion: can solve equations in $\mathbb{Z}/m\mathbb{Z}$ just like any other arithmetical system. We can use subtraction freely, and divide by any a such that $(a,m) = 1$, where division means multiplying by a number $\bar{a}$ such that $a\bar{a} \equiv 1$.

3.4. $\mathbb{Z}/m\mathbb{Z}^{\times}$

DEFINITION 49. Call $[a]_m \in \mathbb{Z}$ a *unit* (or $a \in \mathbb{Z}$ a *unit modulu m) if* $(a,m) = 1$, that is if $[a]_m$ is invertible in $\mathbb{Z}/m\mathbb{Z}$.

Call $[a]_m \in \mathbb{Z}$ a *zero-divisor* if for some $[b]_m \neq [0]_m$ we have $[a]_m[b]_m = 0$.

LEMMA 50. *(units)*

(1) *If $[a]_m$, $[b]_m$ are units then so is $[ab]_m$ and their inverses.*
(2) *If $[a]_m$ is a zero-divisor then so is $[ac]_m$ for any c.*
(3) *Every element of $\mathbb{Z}/m\mathbb{Z}$ is either a unit or a zero-divisor.*
(4) *Every non-zero element of $\mathbb{Z}/m\mathbb{Z}$ is invertible iff m is prime.*

PROOF.

(1) Say $a\bar{a} \equiv b\bar{b} \equiv 1\,(m)$. Then $[\bar{a}]_m$ is a unit (its inverse is $[a]_m$!) and we have $(ab)(\bar{a}\bar{b}) \equiv 1\,(m)$.
(2) If $[a]_m[b]_m = [0]_m$ then $([a]_m[c]_m)\,[b]_m = 0$ too.
(3) Given $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ let $r = (a,m)$. If $r = 1$ then $[a]_m$ is a unit. Otherwise, $1 \leq \frac{m}{r} < m$ so $\left[\frac{m}{r}\right]_m$ is non-zero, but $[r]_m[\frac{m}{r}]_m = [m]_m = [0]_m$, so $[r]_m$ is a zero-divisor. Since a is a multiple of r, $[a]_m$ is a zero-divisor.
(4) When m is prime we only have the two possibilities $(a,m) = 1$ and $(a,m) = m$. In the first case a is invertible, in the second divisible by m hence congruent to zero mod m.

□

DEFINITION 51. $(\mathbb{Z}/m\mathbb{Z})^{\times}$ is the multiplicative system of units. It contains $[1]_m$, is closed under multiplication and taking inverses and satisfies the associative law and the commutative law. The size of $(\mathbb{Z}/m\mathbb{Z})^{\times}$ is denoted $\varphi(m)$. This is *Euler's totient function.*

EXAMPLE 52. For primes p,q we have: $\varphi(p) = p-1$; $\varphi(pq) = (p-1)(q-1)$.

PROPOSITION 53. *Let $x = [a]_m \in (\mathbb{Z}/m\mathbb{Z})^{\times}$. Then:*

(1) *There exists $r \neq 0$ such that $x^r = [1]_m$.*
(2) *(Euler's Theorem) $x^{\varphi(m)} = [1]_m$. In other words, if $(a,m) = 1$ then $a^{\varphi(m)} \equiv 1\,(m)$.*
(3) *The set of r such that $x^r = 1$ is a non-trivial ideal of $\mathbb{Z}$. Its generator is called the* order *of a mod m.*
(4) *In particular, the order of x divides $\varphi(m)$.*

PROOF.

(1) Consider the sequence $\{x^n\}_{n\in\mathbb{Z}} \subset \mathbb{Z}/m\mathbb{Z}$ (we can take about x^{-k} since x is a unit). This is an infinite list while $\mathbb{Z}/m\mathbb{Z}$ is finite. It follows that there exists $n \neq m$ so that $x^n = x^m$. Multiplying by x^{-m} we see $x^{n-m} = [1]_m$.
(2) Consider the set $S = (\mathbb{Z}/m\mathbb{Z})^{\times} = \left\{xy \mid y \in (\mathbb{Z}/m\mathbb{Z})^{\times}\right\}$. In other words, look at the row of x in the multiplication table of $(\mathbb{Z}/m\mathbb{Z})^{\times}$. We claim that S has exactly the same elements as $\mathbb{Z}/m\mathbb{Z}$ (just presented in a different order). Indeed, every $z \in \mathbb{Z}/m\mathbb{Z}^{\times}$ appears as $x(x^{-1}z)$ and if $xy = xy'$ then multiplying by x^{-1} shows $y = y'$ so we get every element once. Now let P be the product of all the elements of $\mathbb{Z}/m\mathbb{Z}^{\times}$. This is also the product of all elements of S, so :
$$P = \prod_{y\in(\mathbb{Z}/m\mathbb{Z})^{\times}} y = \prod_{z\in S} z = \prod_{y\in(\mathbb{Z}/m\mathbb{Z})^{\times}} (xy) = x^{\varphi(m)} \prod_{y\in(\mathbb{Z}/m\mathbb{Z})^{\times}} y = x^{\varphi(m)}P\,.$$
Finally, we cancel P from both sides.
(3) Let I be the set of $r \in \mathbb{Z}$ such that $x^r = 1$. Then $0 \in I$. Also, if $r,s \in I$ and $t \in \mathbb{Z}$ then $x^{r+s} = x^r x^s = 1$ and $x^{tr} = (x^r)^t = 1$ so $r+s, tr \in I$.
(4) In part (2) we showed $\varphi(m) \in I$. It follows that $\varphi(m)$ is a multiple of the generator of this ideal.

□

COROLLARY 54. *(Fermat's Little Theorem) Let p be prime. Then for any number $a \in \mathbb{Z}$ we have $a^p \equiv a\,(p)$.*

PROOF. If $a \equiv 0\,(p)$ then $a^p \equiv 0^p \equiv 0\,(p)$. Otherwise, a is a unit mod p. Since $\varphi(p) = p-1$, we have

$$a^{p-1} \equiv 1\,(p)\,.$$

Now multiply both sides by a. □

3.5. RSA = Rivest-Shamir-Adelman

LEMMA 55. *Let $d, e \in \mathbb{Z}$ satisfy $de \equiv 1\,(\varphi(m))$. Then for any $x \in (\mathbb{Z}/m\mathbb{Z})^\times$, $\left(x^d\right)^e \equiv x\,(m)$ and $(x^e)^d \equiv x\,(m)$.*

PROOF. Say $de = 1 + T\varphi(m)$. Then $\left(x^d\right)^e = (x^e)^d = x^{de} = x^{1+T\varphi(m)} = x \cdot (x^{\varphi(m)})^T \equiv x \cdot 1\,(m)$ By Euler's Theorem. □

Let's say Alice wants to send a message to Bob. Bob secretly generates a large number m, in such a way that he knows $\varphi(m)$. He also picks a number d relatively prime to $\varphi(m)$, and uses Euclid's Algorithm to find e such that $de \equiv 1\,(m)$.

Bob now advertises the pair (m, d) keeping the additional information $(\varphi(m), e)$ secret.

RSA Encryption: Alice takes a message, encodes it as a number $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, and sends Bob a^d modulu m.

RSA Decryption: If Bob receives a number b from Alice, he calculates b^e modulu m. By the Lemma, the number he gets is exactly the message a.

Breaking the encryption requires solving the following problem: given $b \in (\mathbb{Z}/m\mathbb{Z})^\times$, find a so that $a^d = b$.

REMARK 56. In practice, Bob takes $m = pq$ where $p \neq q$ are large primes. Then $\varphi(m) = (p-1)(q-1)$. Knowing $m, \varphi(m)$ one can calculate p, q since we can solve the pair of equations $p + q = m + 1 - \varphi(m)$ and $pq = m$, but since factorization is believed to be hard, it should also be hard to find $\varphi(m)$.

REMARK 57. To account for non-uniformity in the choice of messages, it is better for Alice to randomize the message somewhat.

RSA Digital Signature: Bob writes a message $b \in (\mathbb{Z}/m\mathbb{Z})^\times$. He then publishes the pair (b, b^e).

RSA Signature Verification: Alice sees the pair (b, s). She then calculates $s^d \mod m$ using the public value d, and verifies that $s^d \equiv b\,(m)$.

No-one but Bob can generate valid signatures since only Bob knows e (inverses are unique!)

Math 342 Problem set 6 (due 18/10/11)

$(\mathbb{Z}/m\mathbb{Z})^\times$

1. Let p be a prime. We saw in class that $\varphi(p) = p-1$. Now let $k \geq 1$ be an integer.
   (a) What are the positive divisors of p^k? Find a simple way to express the condition "$(a, p^k) > 1''$.
   (b) How many integers between 0 and $p^k - 1$ are multiples of p?
   (c) (§9C.E51(ii)) Show that $\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$ for all k.
   (d) Show that $\varphi(p \cdot p) \neq \varphi(p)\varphi(p)$.

2. Let p, q be distinct primes. Let $m = pq$.
   (a) What are the positive divisors of m?
   (b) Which integers a, $0 \leq a \leq m-1$ have a common factor with m?
   (c) Show that $\varphi(pq) = (p-1)(q-1)$.
   (d) The conclusion of part (c) can be rephrased as $\varphi(p \cdot q) = \varphi(p)\varphi(q)$. Given the conclusion of part 1(d), your proof of 2(c) must have at some point used the fact that $p \neq q$. Where was it?

3. (§9C.E58) For each integer n below, list the positive divisors of n. For each divisor d find $\varphi(d)$ [by definition, $\varphi(1) = 1$]. Calculate the sum $\sum_{d|n} \varphi(d)$.
   (a) $n = 16$ (you may want to use 1(c)),
   (b) $n = 15$ (you may want to use 2(c)),
   (c) $n = 45$.

RSA

- Download the paper by Rivest, Shamir and Adelman from the course website and read it.

Section II describes the idea (novel at the time) of the whole world knowing the encryption method but nevertheless only the receiver knowing the decryption method. In this description the keys (the various integers $d, e, m, \varphi(m)$) are considered part of the functions D, E of the second lecture.

5. Explain why on the top of page 123, e is chosen to be *relatively prime* to $\varphi(pq)$. This was not emphasized in class, but it is essential.
   Hint: How do we know that d exists?

6. The algorithm in section VII.A has appeared in a previous problem set; it requires about $2\log_2 d$ multiplications to raise a number to the dth power. Could you guess why it was important enough to be mentioned?
   Hint: In applications, d and e will have hundreds of digits.

7. We will verify the numerical example in part VIII: for $m = 2773$, $\varphi(m) = 2668$, $d = 157$, $e = 17$.
   (a) Check that $de \equiv 1\,(\varphi(m))$.
   (b) Consider the word "GREEK" from the example, encoded as the three decimal numbers 0718, 0505, 1100. Here $G = 07$, $R = 18$, $E = 05$, $K = 11$. For each of the three numbers x calculate $x^e \mod m$ and compare with the "encyphered" values given.
   (c) Take your resulting three numbers y, calculate $y^d \mod m$ and see that you get your starting values back.

Rings

Let $M_2(\mathbb{Z})$ be the set of 2×2 matrices. We write $A \in M_2(\mathbb{Z})$ as $\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$. We define addition component-wise, and multiplication by the usual rule of matrix multiplication:

$$A \cdot B = \begin{pmatrix} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12}A_{12}B_{22} \\ A_{21}B_{11} + A_{22}B_{21} & A_{21}B_{12} + A_{22}B_{22} \end{pmatrix}.$$

Let $I = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$ denote the identity matrix, 0 the everywhere zero matrix.

8. Using the usual laws of arithmetic in $\mathbb{Z}$, prove that:
   (a) Addition in $M_2(\mathbb{Z})$ is associative.
   (b) I is a neutral element for multiplication in $M_2(\mathbb{Z})$: for all $A \in M_2(\mathbb{Z})$, $I \cdot A = A \cdot I = A$.
   (c) Show that multiplication in $M_2(\mathbb{Z})$ is not commutative. In other words, find 2×2 matrices A, B with integer entries so that $A \cdot B \neq B \cdot A$

Optional

A. Continuing problem 8, prove that multiplication in $M_2(\mathbb{Z})$ is associative.

CHAPTER 4

Abstract Algebra I: Rings, Fields and Vector Spaces (18/10-27/10)

4.1. Rings (18/10/11)

DEFINITION 58. A *ring* is a quintuple $(R,1,0,+,\cdot)$ consisting of a set R, two elements $0,1\in R$ and two binary operations $+,\cdot\colon R\times R\to R$, such that:

(1) Addition is associative: $\forall x,y,z\in R:\ (x+y)+z=x+(y+z)$.
(2) Additive identity: $\forall x\in R:\ 0+x=x+0=x$.
(3) Additive inverses: $\forall x\in R\exists\bar{x}\in R:\ x+\bar{x}=\bar{x}+x=0$.
(4) Addition is commutative: $\forall x,y\in R:\ x+y=y+x$.
(5) Multiplication is associative: $\forall x,y,z\in R:\ (x\cdot y)\cdot z=x\cdot(y\cdot z)$.
(6) Multiplicative identity: $\forall x\in R:\ 1\cdot x=x\cdot 1=x$.
(7) Distributive law: $\forall x,y,z\in R:\ x\cdot(y+z)=x\cdot y+x\cdot z\wedge(y+z)\cdot x=y\cdot x+z\cdot x$.

If, in addition, multiplication is commutative ($\forall x,y\in R:\ x\cdot y=y\cdot x$), we say R is a *commutative ring*.

EXAMPLE 59. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all rings. $\mathbb{Z}/m\mathbb{Z}$ is also a ring (Proposition 46).

LEMMA 60. *Let R be a ring. Then its neutral elements are unique.*

PROOF. Let $0'$ be another netural element for addition. Then $0=0+0'=0'$ where the left equality following from $0'$ being a neutral element, the right one from 0 being a netural element. Similarly for multiplicatin. □

What this lemma means is that after we define the operations, if we are to get a ring then the choices of 0 and 1 are forced on us: given the set R and the operations $+,\cdot$ there is at most one choice of distinguished elements $0,1\in R$ that will give us a ring.

LEMMA 61. *Let R be a ring, $a,b\in R$. Then the equation $a+x=b$ has a unique solution.*

PROOF. Let $\bar{a}$ be an additive inverse to a. If x is a solution then additing $\bar{a}$ on the left to both sides of the equation shows:

$$\begin{aligned}\bar{a}+b &= \bar{a}+(a+x)\\ &= (\bar{a}+a)+x \qquad \text{(associativity)}\\ &= 0+x \qquad \text{(definition of inverse)}\\ &= x \qquad \text{(definition of zero)}\,.\end{aligned}$$

Conversely, we have $a+(\bar{a}+b)=(a+\bar{a})+b=b$ so indeed $\bar{a}+b$ is a solution. □

COROLLARY 62. *Every $a\in R$ has a unique additive inverse, which we will from now on denote $-a$. Indeed the additive inverse is a solution to the equation $a+x=0$.*

LEMMA 63. *Let R be a ring. Then the equation $x+x=x$ has the unique solution* 0.

PROOF. Clearly $0+0=0$. For the converse add $-x$ to both sides of the equation. □

LEMMA 64. *Let R be a ring, and let $r \in R$. Then $0 \cdot r = r \cdot 0 = 0$.*

PROOF. Let $x = 0 \cdot r$. We then have $x + x = 0 \cdot r + 0 \cdot r = (0+0) \cdot r$ by the distributive law. Now $0+0=0$ so we find $x+x=x$ and hence $x=0$. The same calculation shows that if $y = r \cdot 0$ then $y+y=y$ and again $y=0$. □

LEMMA 65. *Let R be a ring and let $r \in R$. Then $-r = (-1) \cdot r = r \cdot (-1)$.*

PROOF. We have $r + (-1) \cdot r = 1 \cdot r + (-1) \cdot r = (1 + (-1)) \cdot r = 0 \cdot r = 0$, and the claim follows by Corollary 62. The ot her side is proved the same way. □

4.1.1. Example: Rings of functions. Let X be a non-empty set, R a ring. Let R^X denote the set of functions from X to R. We define operations on fuctions pointwise: given functions $f, g \colon X \to R$ we define their sum and product as the functions $f+g$, $f \cdot g$ where:

$$(f+g)(x) \overset{\text{def}}{=} f(x) +_R g(x),$$
$$(f \cdot g)(x) \overset{\text{def}}{=} f(x) \cdot_R g(x).$$

Let , $\mathbb{1}$ denote the constant functions $(x) = 0_R$, $\mathbb{1}(x) = 1_R$.

LEMMA 66. $\left(R^X, , \mathbb{1}, +, \cdot\right)$ *is a ring. It is commutative if and only if R is.*

PROOF. Let $f, g, h \in R^X$. Then for all x we have:

$$\begin{aligned} ((f+g)+h)(x) &= (f+g)(x) +_R h(x) \\ &= (f(x) +_R g(x)) +_R h(x) \\ &= f(x) +_R (g(x) +_R h(x)) \\ &= f(x) +_R (g+h)(x) \\ &= (f + (g+h))(x). \end{aligned}$$

Thus the two functions $((f+g)+h)$ and $(f+(g+h))$ agree at every x – they are the same function.

All the ring axioms hold for the same reason: they hold in R pointwise for every x. We also illustrate with the existence of additive inverses. Given $f \in R^X$ we define a function $-f$ by

$$(-f)(x) = -(f(x)).$$

It is an additive inverse since

$$(f + (-f))(x) = f(x) +_R (-(f(x))) = 0 = (x).$$

□

4.1.2. Example: Rings of matrices. Let R be a ring. Let $M_n(R)$ denote the set of $n \times n$ matrices with entries in R. For $A \in M_n(R)$ we write A_{ij} for the jth element of the ith row of A. We define addition co-ordinatewise and multiplication by the usual rule:

$$(A+B)_{ij} \overset{\text{def}}{=} A_{ij} +_R B_{ij},$$

$$(A \cdot B)_{ik} \overset{\text{def}}{=} \sum_{j=1}^{n} A_{ij} \cdot B_{jk}.$$

We let 0_n, I_n denote the $n \times n$ zero matrix and identity matrix respectively: $(0_n)_{ij} = 0_R$ for all i, j while $(I_n)_{ij} = \begin{cases} 1_R & i = j \\ 0_R & i \neq j \end{cases}$.

PROPOSITION 67. *$(M_n(R), 0_n, I_n, +, \cdot)$ is a ring. It is not commutative unless $n = 1$ and R is commutative.*

PROOF. The axioms about addition are proved the same way as for rings of functions (think of a matrix A as a function on a set of size n^2). The distributive law is proved the same way – we give one half of it:

$$\begin{aligned}
(A \cdot (B + C))_{ik} &= \sum_j A_{ij} \cdot_R (B + C)_{jk} && \text{(definition of matrix multiplication)} \\
&= \sum_j A_{ij} \cdot_R \left(B_{jk} +_R C_{jk} \right) && \text{(definition of matrix addition)} \\
&= \sum_j \left(A_{ij} \cdot_R B_{jk} +_R A_{ij} \cdot C_{jk} \right) && \text{(the distributive law in } R\text{)} \\
&= \left(\sum_j A_{ij} \cdot_R B_{jk} \right) + \left(\sum_j A_{ij} \cdot_R C_{jk} \right) && \text{(the commutative law of addition in } R\text{)} \\
&= (A \cdot B)_{ik} + (A \cdot C)_{ik} && \text{(definition of matrix multiplication)} \\
&= (A \cdot B + A \cdot C)_{ik} && \text{(definition of matrix addition)}\,.
\end{aligned}$$

Associativity of multiplication and the multiplicative identity property are proved the same way. In the problem set we will see an example of matrices $A, B \in M_2(R)$ defined for any ring R so that $AB \neq BA$. This example clearly works in $M_n(R)$ for any $n \geq 2$, so these are never commutative. $M_1(R)$ is essentially the same as R, so it's commutative exactly when R is. □

4.1.3. Maps of ring; isomorphism. Let R be a ring. Then $M_2(R)$ is a ring, so $\mathcal{R} = M_2(M_2(R))$ is also a ring. Its elements are "2×2 matrices, the entries of which are 2×2 matrices". These look similar to the elements of the ring $\mathcal{S} = M_4(R)$, which are "4×4 matrices". We write two typical elements of the two rings:

$$\begin{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \begin{pmatrix} e & f \\ g & h \end{pmatrix} \\ \begin{pmatrix} i & j \\ k & l \end{pmatrix} & \begin{pmatrix} m & n \\ o & p \end{pmatrix} \end{pmatrix} \mapsto \begin{pmatrix} a & b & e & f \\ c & d & g & h \\ i & j & m & n \\ k & l & o & p \end{pmatrix}.$$

Consider the map $f \colon \mathcal{R} \to \mathcal{S}$ given by the arrow above.

PROPOSITION 68. *The map f respects the ring operations. In other words, it has the following properties:*

(1) $f(0_{\mathcal{R}}) = 0_{\mathcal{S}}$.
(2) $f(1_{\mathcal{R}}) = 1_{\mathcal{S}}$.
(3) *For all $x, y \in \mathcal{R}$, $f(x +_{\mathcal{R}} y) = f(x) +_{\mathcal{S}} f(y)$.*
(4) *For all $x, y \in \mathcal{R}$, $f(x \cdot_{\mathcal{R}} y) = f(x) \cdot_{\mathcal{S}} f(y)$.*
(5) *f is a bijection of the underlying sets. In other words, f is $1 - 1$ and onto.*

PROOF. (1), (2), (3) are immediate by the definitions. (4) requires a calculation (omitted). (5) is also clear – both sets are basically the set of 16-tuples of elements from R. □

DEFINITION 69. Let $\mathcal{R},\mathcal{S}$ be a rings. A map $f\colon \mathcal{R}\to\mathcal{S}$ is called a (ring) *homomorphism* if it satisfies properties (1)-(4) of the proposition. If, in addition, it satisfies condition (5) then it is called an *isomorhpism*. If there is an isomorphism between $\mathcal{R},\mathcal{S}$ we say that $\mathcal{R},\mathcal{S}$ are *isomorphic*.

LEMMA 70. *Isomorphism is an equivalence relation (most importantly, if $f\colon \mathcal{R}\to\mathcal{S}$ is an isomorphism then the inverse map $f^{-1}\colon \mathcal{R}\to\mathcal{S}$ is also an isomorphism)*

REMARK 71. The concepts *homomorphism* and *isomorphism* are very important. The second one is the mathematician's word for "the same for all practical purpopses". In out example, $M_2(M_2(R))$ and $M_4(R)$ are not the same ring, but they are the same for the purpopse of any question of algebra.

LEMMA 72. *Let $f\colon \mathcal{R}\to\mathcal{S}$ be a map of rings, and assume that it preserves addition (property (3) above). Then it preserves zero (property (1) above).*

PROOF. Since $0_{\mathcal{R}}+_R 0_{\mathcal{R}}=0_{\mathcal{R}}$ we have $f(0_{\mathcal{R}})+_{\mathcal{S}}f(0_{\mathcal{R}})=f(0_{\mathcal{R}})$. In other words, $f(0_{\mathcal{R}})$ is a solution to the equation $x+x=x$ in $\mathcal{S}$. Now Lemma 63 shows that $0_{\mathcal{S}}$ is the unique solution to that equation. □

Math 342 Problem set 7 (due 27/10/11)

Coding Theory: The Hamming Distance

Let Σ be a set ("alphabet"). Let $X = \Sigma^n$ be the set of sequences of length n ("words") consisting of elements of Σ. Given two words $\underline{w}, \underline{v} \in X$ we define their *Hamming distance* to be the number of positions at which they differ. That is, if $\underline{w} = (w_1, \ldots, w_n)$, $\underline{v} = (v_1, \ldots, v_n)$ we set:

$$d_{\mathrm{H}}(\underline{w}, \underline{v}) = \#\{i, 1 \le i \le n \mid w_i \neq v_i\} .$$

Example: if $\Sigma = \{0,1,2\}$, $n = 6$, $\underline{w} = 012212$, $\underline{v} = 022210$ then $d_{\mathrm{H}}(\underline{w}, \underline{v}) = 2$ (they differ in the 2nd and 6th letters).

1. Let $\Sigma = \{0,1\}$, $X = \Sigma^8$ (bit strings of length 8). Let $\underline{a} = 00000000$, $\underline{b} = 11110000$, $\underline{c} = 01001010$, $\underline{d} = 01001000$. Make a 4x4 table with rows and columns corresponding to these four vectors, and fill in each entry with the distance of the corresponding pair of vectors (there are 16 distances to find in total).

2. Going back to the general case of the Hamming distance on any $X = \Sigma^n$, show that d_{H} is a distance function:
   (a) Show that for any $\underline{w}, \underline{v} \in X$, $d_{\mathrm{H}}(\underline{w}, \underline{v}) = d_{\mathrm{H}}(\underline{v}, \underline{w})$.
   Hint: Convert the claimed assertion to words: "The number of positions at which $\underline{w}$ differs from $\underline{v}$ is equal to ..."
   (b) Show that for any $\underline{w}, \underline{v} \in X$, $d_{\mathrm{H}}(\underline{w}, \underline{w}) = 0$ but if $\underline{w} \neq \underline{v}$ then $d_{\mathrm{H}}(\underline{w}, \underline{v}) > 0$.
   Hint: Convert he assertions to words.
   (*c) (Triangle inequality) Show that for any $\underline{w}, \underline{v}, \underline{u} \in X$, $d_{\mathrm{H}}(\underline{w}, \underline{u}) \le d_{\mathrm{H}}(\underline{w}, \underline{v}) + d_{\mathrm{H}}(\underline{v}, \underline{u})$.
   Hint: In what co-ordinates can $\underline{w}, \underline{u}$ differ?

Coding Theory: Repetition Coding

(Repetition coding) Alice and Bob can communicate through a channel which allows Alice to send one symbol at a time (in other words, Alice chooses a symbol from Σ, gives it to the channel, and Bob gets a symbol from the channel at the other end). Unfortunately, the channel is not perfect and sometimes Bob gets back a different symbol from the one transmitted by Alice. We assume however that the channel never loses symbols or creates new ones, so that Bob gets exactly one symbol for each symbol Alice transmits. In order to guard against errors, Alice and Bob agree that Alice send every letter of her message $2n+1$ times rather than just once.

3. Let's say Σ is the English alphabet and Alice will repeat every letter 5 times. Bob got HHHTH-EEUVE-LLLLL-LLRBL-OOOOK-WAWWW-YWWWW-OOOOO-RARRR-LALLL-DDDDD. Can you guess what message Alice wanted to send?

Of course, we'd like a computer to be able to make this "guess". Let's see how this is done.

4. Inside $X = \Sigma^{2n+1}$ let C be the set of "constant words": the set of words of the form $\sigma\sigma\sigma\ldots\sigma$ where $\sigma \in \Sigma$ (in problem 3, these would be: AAAAA to ZZZZZ).
   (a) Let $\underline{u}, \underline{v} \in C$ be distinct. What is $d_{\mathrm{H}}(\underline{u}, \underline{v})$?
   (b) Let $\underline{w} \in X$, and let $\underline{u}, \underline{v} \in C$ be both at distance at most n from $\underline{w}$. Use the triangle inequality to show $d_{\mathrm{H}}(\underline{u}, \underline{v}) \le 2n$. Then use part (a) of this problem to show that $\underline{u} = \underline{v}$.

*5. Assume that the channel can corrupt at most n symbols out of any $2n+1$ it transmits. Show that Bob can unambiguously recover any message sent by Alice.

Rings and maps

6. (Injectivity and kernels: exercise in reading definitions) Let R,S be rings, and $f\colon R \to S$ a ring homomorphism. (The precise meaning is Definition 69 in the notes).
   (a) Assume that f is injective (also called $1-1$), that is that if $r,r' \in R$ are distinct then $f(r), f(r')$ are distinct elements of S. Show that if $r \in R$ satisfies $r \neq 0_R$ then $f(r) \neq 0_S$. *Hint*: What is $f(0_R)$?
   (b) Assume that f has the property that $f(r) = 0_S$ only if $r = 0_R$. Show that f is injective. *Hint:* Use $f(r) - f(r') = f(r - r')$.

7. (Scalar matrices) Let R be a ring, and let $S = M_n(R)$ be the ring of $n \times n$ matrices with entries in R. Let $\iota\colon R \to S$ be the map where $\iota(r)$ is the diagonal matrix with r along the diagonal and zeroes elsewhere) (if $n = 2$ then $\iota(r) = \begin{pmatrix} r & 0_R \\ 0_R & r \end{pmatrix}$).
   (a) Show that ι is a homomorphism of rings.
   (b) Show that ι is *injective*.
   (c) Let $T \subset S$ be the set of scalar matrices. Show that $\iota\colon R \to T$ is an isomorphism.

8. Let R be a ring. Call $a \in R$ *invertible* if there is $b \in R$ such that $ab = 1_R$, a *zero-divisor* if there is $b \in R$, $b \neq 0_R$, such that $ab = 0_R$. Let S be the ring R^X for some non-empty set X.
   (a) Let $f\colon \{0,1,2\} \to \mathbb{Z}/11\mathbb{Z}$ be the function $f(i) = [i]_{11}$. Is f a zero-divisor? If so find a non-zero $g \in (\mathbb{Z}/11\mathbb{Z})^{\{0,1,2\}}$ such that $fg = 0$.
   (b) Show that $f \in R^X$ is invertible in the ring R^X exactly when $f(x)$ is invertible in R for all x. What is the inverse?

Supplementary Problems

A. (The boolean ring) Let X be a set, $\mathcal{P}(X)$ the *powerset* of X, that is the set of subsets of X.

(a) For $A, B \in \mathcal{P}(X)$ (that is, for two subsets of X) show that
$$(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$$
and that this is the set of elements of X that belong to *exactly one* of A, B. Call the set the *symmetric difference* and denote it $A \Delta B$.

(b) Show that the symmetric difference is an associative and commutative operation on $\mathcal{P}(X)$. Show that the empty set is an netural element for this operation, and find an inverse to every set (for every A find B so that $A \Delta B = \emptyset$).

(c) Show that the intersection opreation ($A, B \mapsto A \cap B$) is an associative and commutative operation on $\mathcal{P}(X)$. Show that the set X is a neutral element for this operation.

(d) (de Morgan's law) Show the distributive law $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$.

(e) Conclude that $\mathcal{A} = (\mathcal{P}(X), \emptyset, X, \Delta, \cap)$ is a commutative ring.

B. (Characteristic functions) Consider the map $\chi \colon \mathcal{P}(X) \to (\mathbb{Z}/2\mathbb{Z})^X$ which associates to every $A \subset X$ the function $\chi_A \colon X \to \mathbb{Z}/2\mathbb{Z}$ where:
$$\chi_A(x) = \begin{cases} [1]_2 & x \in A \\ [0]_2 & x \notin A \end{cases}.$$
Show that χ is an isomorphism of the boolean ring $\mathcal{A}$ and the ring of functions from X to $\mathbb{Z}/2\mathbb{Z}$ with pointwise addition and multiplication.

C. Let $C(\mathbb{R})$ denote the ring of continuous real-valued functions defined on the entire real line. Let $\varphi \colon C(\mathbb{R}) \to \mathbb{R}$ be the *evaluation map* $\varphi(f) \overset{\text{def}}{=} f(0)$. In other words, φ is the rule that associates to each function $f \in C(\mathbb{R})$, the real number $f(0)$.

(a) Show that φ is a ring homomorphism.

(b) Did your proof use the continuity of f?

(c) Let X be a set, R a ring. Choose a point $x \in X$, and consider the evaluation map $e_x \colon R^X \to R$ given by $e_x(f) \overset{\text{def}}{=} f(x)$ (recall that R^X is the ring of functions from X to R). Show that e_x is a ring homomorphism.

4.2. Fields (25/10/11)

Maps of rings which repsect multiplication don't have to map the identity element of the identity element – check out the map $f\colon M_2(R) \to M_3(R)$ given by the upper right corner:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Thus the condition $f(1) = 1$ for homomorphisms is essential. That said, if $f\colon R \to S$ is a homomorphism of rings, we do that $f(1) \cdot f(a) = f(a)$ for all $a \in R$. Sometimes this would force $f(1) = 1$.

DEFINITION 73. Let R be a ring, and let $r \in R$.

(1) Say that r is *invertible* (or that it is a *unit*) if these exists $\bar{r} \in R$ such that $r \cdot \bar{r} = \bar{r} \cdot r = 1_R$.
(2) Say that r is a *zero-divisor* if these exists a non-zero $s \in R$ such that $rs = 0$ or $sr = 0$.

LEMMA 74. *Let r be invertible. Then it has a unique multiplicative inverse, to be denoted r^{-1} from now on.*

PROOF. Assume that $\bar{r}$ and s are two multiplicative inverses of $r \in R$. Then $s = 1_R \cdot s = (\bar{r}r)s = \bar{r}(rs) = \bar{r} \cdot 1_R = \bar{r}$. □

ASSUMPTION 75. *From now on assume that $1_R \neq 0_R$ for any ring R.*

DEFINITION 76. We say that a commutative ring R is an *integral domain* if its only zero-divisor is 0_R, a *field* if its only non-unit is 0_R.

EXAMPLE 77. $\mathbb{Z}$ is an integral domain; $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields.

PROPOSITION 78. *$\mathbb{Z}/m\mathbb{Z}$ is a field iff m is prime.*

PROOF. This is 50(4). □

4.3. Vector spaces

Fix a field F, to be knows as the "field of scalars".

DEFINITION 79. A *vector space over F* is a quadruplet $(V, \underline{0}, +, \cdot)$ where V is a set, $\underline{0} \in V$ is a distinguished element, $+\colon V \times V \to V$ is a binary operation ("addition"), and $\cdot\colon F \times V \to V$ is another operation ("multiplication by scalars") such that:

(1) $+$ is an associative and commutative operation.
(2) $\underline{0}$ is neutral element for addition, and every $\underline{v} \in V$ has an additive inverse.
(3) For all $\underline{v} \in V$, we have $1_F \cdot \underline{v} = \underline{v}$.
(4) For all $\alpha, \beta \in F$ and $\underline{v} \in V$, $\alpha \cdot (\beta \cdot \underline{v}) = (\alpha\beta) \cdot \underline{v}$ (note that on the left both operations are multiplication of a vector by a scalar, but on the right one is a multiplication in F and the other combines a vector with the scalar $\alpha\beta$).
(5) For all $\alpha, \beta \in F$ and $\underline{u}, \underline{v} \in V$, $(\alpha + \beta)(\underline{u} + \underline{v}) = \alpha \cdot \underline{u} + \beta \cdot \underline{u} + \alpha \cdot \underline{v} + \beta \cdot \underline{v}$ (note that the RHS is meaningful since addition is associative and commutative).

EXAMPLE 80. Let X be a set. Then $\left(F^X, , +, \cdot\right)$ has the structure of a vector space over F where addition is the usual addition of functions and scalar multiplication takes the form $(\alpha f)(x) = \alpha \cdot f(x)$.

PROOF. When discussing the ring structure on F^X we checked the axioms regarding addition. It is also clear that $1 \cdot f = f$ for all f. Next, note that $\alpha \cdot f = (\alpha \cdot \mathbb{1}) \cdot f$ where the second operation is multiplication of functions. To check that scalar multiplication is associative and distributive we then use the associative and distributive laws in the ring of functions – we only need to check that $(\alpha \cdot \mathbb{1}) \cdot (\beta \cdot \mathbb{1}) = ((\alpha\beta) \cdot \mathbb{1})$ and $(\alpha \cdot \mathbb{1}) + (\beta \cdot \mathbb{1}) = ((\alpha + \beta) \cdot \mathbb{1})$ which are clear. □

EXAMPLE 81. If X is the finite set $[n] = \{0, 1, \ldots, n-1\}$ of size n we obtain the vector space F^n of column vectors of length n.

LEMMA 82. *Let V be a vector space over F. Then for every $\underline{v} \in V$ we have $0_F \cdot \underline{v} = \underline{0}$.*

PROOF. Let $\underline{w} = 0_F \cdot \underline{v}$. Then $\underline{w} + \underline{w} = 0_F \cdot \underline{v} + 0_F \cdot \underline{v} = (0_F + 0_F) \cdot \underline{v} = 0_F \cdot \underline{v} = \underline{w}$, where the second equality uses the distributive law, the third the properties of addition in F. Adding $-\underline{w}$ to both sides, we conclude that

$$\underline{w} = \underline{w} + \underline{0} = \underline{w} + (\underline{w} + (-\underline{w})) = (\underline{w} + \underline{w}) + (-\underline{w}) = \underline{w} + (-\underline{w}) = \underline{0}$$

as claimed, where the third equality follows from the associative law for addition, the others from properties of zero and additive inverses. □

DEFINITION 83. Let V be a vector space over F, and let $S \subset V$. Say that S is *linearly dependent* if there exists finite sequences $\{\underline{v}_i\}_{i=1}^r \subset S$, $\{\alpha_i\}_{i=1}^r \subset F$ not all zero such that $\underline{v}_i \neq \underline{v}_j$ for $i \neq j$ and so that

$$\sum_{i=1}^r \alpha_i \underline{v}_i = \underline{0}.$$

We define the empty sum (the case $r = 0$) to be equal to $\underline{0}$. Call S *linearly independent* if it is not dependent. Finally, say that $\underline{v} \in V$ *depends* on S if $\underline{v}$ is a linear combination of vectors from S (in particular, $\underline{0}$ depends on every set).

EXAMPLE 84. Fixing a field F and an integer n, let $\underline{e}^i \in F$ denote the standard basis vector. Then $\{\underline{e}^i \mid 1 \leq i \leq n\}$ is independent.

EXAMPLE 85. For each $n \geq 0$ let $f \in C(\mathbb{R})$ denote the function $f_n(x) = x^n$. Then $\{f_n \mid n \geq 0\} \subset C(\mathbb{R})$ is linearly independent.

PROOF. Let f be a non-empty finite linear combination of these functions. Without loss of generality it is of the form $\sum_{i=0}^n \alpha_i f_i =$ with $\alpha_n \neq 0$. If $\alpha_n > 0$ then $\lim_{x\to\infty} f(x) = \infty$, while if $\alpha_n < 0$ then $\lim_{x\to\infty} f(x) = -\infty$. In either case, it is clear that $f \neq$. □

PROPOSITION 86. *(Linear dependence and independence)*

(1) *$S \subset V$ is dependent iff there exists $\underline{v} \in S$ such that $\underline{v}$ depends on $S \setminus \{\underline{v}\}$.*
(2) *If S is independent and $\underline{v}$ is independent of S, then $S \cup \{\underline{v}\}$ is independent.*

PROOF. In the first part, assume that $\sum_i \alpha_i \underline{v}_i = \underline{0}$ with $\alpha_{i_0} \neq 0$. Then α_{i_0} is invertible since F is a field, and we have

$$\underline{v}_{i_0} = \sum_{i \neq i_0} \left(-\alpha_{i_0}^{-1} \alpha_i\right) \underline{v}_i .$$

Conversely, if $\underline{v} = \sum_i \alpha_i \underline{v}_i$ with $\{\underline{v}_i\}_{i=1}^r \subset S \setminus \{\underline{v}\}$ a sequence of distinct vectors we extend the sequence by setting $\underline{v}_{r+1} = \underline{v}$. Then the sequence $\{\underline{v}_i\}_{i=1}^{r+1} \subset S$ still consists of distinct vectors, and with $\alpha_{r+1} = -1_F$ we have $\sum_{i=1}^{r+1} \alpha_i \underline{v}_i = \sum_{i=1}^r \alpha_i \underline{v}_i + \alpha_{r+1} \underline{v}_{r+1} = \underline{v} - \underline{v} = \underline{0}$. Moreover, not all coefficients are zero since $\alpha_{r+1} \neq 0$.

The second part has a similar proof: Assume that

$$\alpha\underline{v}+\sum_{i=1}^{r}\alpha_i\underline{v}_i=\underline{0}$$

with $\underline{v}_i \in S$ distinct. If $\alpha \neq 0$ then it would be invertible, allowing us to write $\underline{v}=\sum_{i=1}^{r}\left(-\alpha^{-1}\alpha_i\right)\underline{v}_i$ which would make $\underline{v}$ depend on S. Thus $\alpha = 0$ so that $\sum_{i=1}^{r}\alpha_i\underline{v}_i=\underline{0}$. Now we must have $\alpha_i = 0$ for all i since S is independent. It follows that $S\cup\{\underline{v}\}$ is independent. □

DEFINITION 87. A subset $W \subset V$ is call a *subspace* if it contains zero and is closed under addition and scalar multiplication (if $\underline{w},\underline{v} \in W$ and $\alpha \in F$ then $\alpha\underline{w}+\underline{v} \in W$).

LEMMA 88. *A subspace is a vector space.*

DEFINITION 89. Let $S \subset V$. The *span* $\mathrm{Span}_F S$ is the set of all (finite) linear combinations of elements of S. We say that S *spans* V if $\mathrm{Span}_F S = V$.

LEMMA 90. $\mathrm{Span}_F S$ *is a subspace of* V*, in fact the smallest one containing* S*.*

PROOF. We first prove that the span is a subspace. $\underline{0} \in \mathrm{Span}_F S$ as the empty linear combination. Adding two linear combinations of vectors from S gives a linear combination of vectors from S, similarly for multiplying a linear combination by a scalar. Next, if W is any subspace of V containing S then W is closed under the linear operations, hence contains all linear combinations of vectors from S – in other words if $S \subset W$ then $\mathrm{Span}_F S \subset W$ which is what we needed to prove. □

DEFINITION 91. A *basis* of V is a spanning independent set.

LEMMA 92. *Every vector space has a basis.*

PROOF. Let $B \subset V$ be a maximal independent set. Assume that $\underline{v} \in V$ is not in the $\mathrm{Span}_F B$. Then $\underline{v}$ is independent of B and hence $B\cup\{\underline{v}\}$ would be independent as well, a contradiction to the maximality of B. □

FACT 93. *(Linear Algebra) Let* V *be a vector space over* F*. Then any two bases of* V *have the same cardinality. The cardinality of any basis is called the* dimension *of* V *and denoted* $\dim_F V$.

Math 342 Problem set 8 (due 3/11/11)

Rings and vector spaces

1. Let R be a ring. We define a map $f\colon \mathbb{N} \to R$ inductively by $f(0) = 0_R$ and $f(n+1) = f(n) + 1_R$.
   (a) Show that $f(1) = 1_R$. Show that $f(n+m) = f(n) + f(m)$ for all $n,m \in \mathbb{N}$.
   Hint: Induction on m.
   (b) Show that f respects multiplication, that is for all $n,m \in \mathbb{N}$, $f(nm) = f(n) \cdot f(m)$.
   Hint: Induction again. The case $m = 0$ uses a result from class.
   SUPP Extend f to a function $g\colon \mathbb{Z} \to R$ by setting $g(n) = f(n)$ if $n \in \mathbb{Z}_{\geq 0}$, and $g(n) = -f(-n)$ if $n \in \mathbb{Z}_{\leq 0}$. Show that g is a ring homomorphism.
   Hint: Divide into cases.

*2. Let E be a field, and let $F \subset E$ be a *subfield* (F contains $0_E, 1_E$, and is closed under addition, multiplication, negatives and inverses). Consider the set E with the following two operations: addition in E and multiplying elements of E by elements of F. Show that this makes E into a vector space over F.
Hint: You need to go over the axioms in Definition 79 and deduce them from what you know about E due to Definition 58.

Linear algebra

3. In each case, check whether the vector is linearly dependent on the other vectors. If it is, exhibit it as a linear combination. If not, prove that this cannot be done.
   (a) $(1,2,3)$ on $\{(2,4,0),(0,0,1),(0,0,0)\}$ in $\mathbb{R}^3$?
   (b) $(5,7,-2)$ on $\{(3,2,1),(1,0,0)\}$ in $\mathbb{R}^3$.
   (c) $([5]_{11},[7]_{11},[-2]_{11})$ on $\{([3]_{11},[2]_{11},[1]_{11}),([1]_{11},[0]_{11},[0]_{11})\}$ in $\mathbb{F}_{11}^3$ (for a prime p, $\mathbb{F}_p$ is another notation for the field $\mathbb{Z}/p\mathbb{Z}$).
   (d) The polynomial $[5]_7x + [1]_7$ on $\left\{[2]_7x^2 + [1]_7x, x^2 + [5]_7x + [3]_7\right\}$ in the space of polynomials over $\mathbb{F}_7$.

*4. Let F be a field, V a vector space over F, and let $B = \{\underline{v}_i\}_{i=1}^n \subset V$ be a linearly independent subset of V which spans V. Consider the map $f\colon F^n \to V$ given by $f(x_1,\ldots,x_n) = \sum_{i=1}^n x_i\underline{v}_i$.
   (a) Show that f is a linear map.
   (b) Show that f is *onto*, that is that the image f is the whole of V.
   Hint: What is the definition of "span"?
   (c) Show that f is *injective*, that is that if $\underline{x} \neq \underline{y}$ in F^n then $f(\underline{x}) \neq f(\underline{y})$ in V.
   Hint: Assume $f(\underline{x}) = f(\underline{y})$, subtract $f(\underline{y})$ from both sides, and use the definition of independence to show $\underline{x} = \underline{y}$.
   (d) Conclude that every n-dimensional vector space over F is isomorphic to F^n.

REMARK 94. This is why the case of F^n is the one most studied.

The Hamming Code (variant)

5. Let $H \in M_{3\times 7}(\mathbb{F}_2)$ be the matrix whose columns are all non-zero vectors in $\mathbb{F}_2^3$, that is

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

(a) Let $a,b,c,d \in \mathbb{F}_2$be a 4-bit "message" we want to transmit. Show that there exist unique $x,y,z \in \mathbb{F}_2$ so that $H \cdot (x,y,z,a,b,c,d)^T = \underline{0}$. We will trasmit the redundant 7-bit vector instead.

Hint: Need to show both that x,y,z exist and that they are unique. Express the problem as a system of linear equations over $\mathbb{F}_2$.

(b) For each $1 \le i \le 7$, let $\underline{e}^i$ be the standard basis vector of $\mathbb{F}_2^7$ with 1 at the ith co-ordinate. Calculate the seven vectors $H\underline{e}^i$.

(c) Let $\underline{v}, \underline{v}' \in \mathbb{F}_2^7$ be at Hamming distance 1. Show that there exists i so that $\underline{v}' = \underline{v} + \underline{e}^i$.

(d) Now let's say Alice transmits the 7-bit vector $\underline{v} = (x,y,z,a,b,c,d)^T$ from part (a), through a channel that can change at most one bit in every seven. Denote by $\underline{v}'$ the 7 bits Bob receives, and show that if $\underline{v}' \neq \underline{v}$ then $H\underline{v}' \neq \underline{0}$. Conclude that Bob can detect if a 1-bit error occured.

Hint: Use the fact that $H\underline{v} = \underline{0}$ and your answers to parts (c) and (b).

(e) In fact, if at most one bit error can occur then Bob can *correct* the error. Using the fact that the vectors $H\underline{e}^i$ are all different (see your answer to part (b)), show that knowing only $\underline{v}'$ and that at most one error occured, he can calculate the difference $\underline{e} = \underline{v}' - \underline{v}$ and hence the original vector $\underline{v}$.

Hint: What are the possibilities for $\underline{e}$? For $H\underline{e}$? how do they match up? Don't forget that it's possible that $\underline{v}' = \underline{v}$.

Supplementary problems

A (Prime fields and finite fields)

(a) Let g be the map from 1(c). Show that $\mathrm{Ker}(g)$ is an ideal of $\mathbb{Z}$.

(b) Let E be a field, and let $g\colon \mathbb{Z} \to E$ be the map from problem 1. Show that $\mathrm{Ker}(g) = (p)$ where $p = 0$ or p is prime.

Hint: If $m = ab$ apply g to both sides.

(c) Conclude that every finite field contains a copy of $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$ for a prime p.

(d) Show that every finite field has p^n elements for some n.

REMARK. It is also true that for every $q = p^n$ there exists a field $\mathbb{F}_q$ of size q, unique up to isomorphism.

4.4. Linear transformations and subspaces

Let F be a field.

DEFINITION 95. Let V,W be vectors spaces over F. A map $f\colon V \to W$ is called a *linear transformation* (or a *linear map* or a *homomorphism*) if for all $\alpha \in F$ and $\underline{u},\underline{v} \in V$, we have

$$f(\underline{u}+\underline{v}) = f(\underline{u}) + f(\underline{v}).$$
$$f(\alpha \cdot \underline{u}) = \alpha \cdot f(\underline{u}).$$

LEMMA 96. *If f is a linear transformation then $f(\underline{0}_V) = f(\underline{0}_W)$.*

PROOF. $f(\underline{0}_V) = f(0_F \cdot \underline{0}_V) = 0_F \cdot f(\underline{0}_V) = \underline{0}_W$. □

LEMMA 97. *TFAE*

(1) *$f\colon V \to W$ is a linear transformation.*
(2) *For all $\gamma,\delta \in F$ and $\underline{u}',\underline{v}' \in V$, $f(\gamma\underline{u}' + \delta\underline{v}') = \gamma f(\underline{u}') + \delta f(\underline{v}')$*

PROOF. Let f be a linear transformation, and let $\gamma,\delta,\underline{u}',\underline{v}'$ be as in (2). Then

$$\begin{aligned} f\left(\gamma\underline{u}' + \delta\underline{v}'\right) &= f\left(\gamma\underline{u}'\right) + f\left(\delta\underline{v}'\right) \\ &= \gamma f\left(\underline{u}'\right) + \delta f\left(\underline{v}'\right). \end{aligned}$$

Conversely, taking $\gamma = 1$, $\delta = 1$ and $\gamma = \alpha$, $\delta = 0$ in (2) gives the two defining properties of a linear transformation. □

EXAMPLE 98. (Rethinking some calculus) The map $\frac{d}{dx}\colon C^1(\mathbb{R}) \to C(\mathbb{R})$ is linear. The map $\int_a^b\colon C([0,1]) \to \mathbb{R}$ is linear. The map $f(\underline{v}) = \underline{v} + \underline{w}$ is not linear unless $\underline{w} = \underline{0}$ (why?)

DEFINITION 99. Let $f\colon V \to W$ be a linear transformation. The *kernel* of f it the set $\operatorname{Ker}(f) = \{\underline{v} \in V \mid f(\underline{v}) = \underline{0}_W\} \subset V$. Its image is the set $\operatorname{Im}(f) = \{\underline{w} \in W \mid \exists \underline{v} \in V : f(\underline{v}) = \underline{w}\}$.

LEMMA 100. *Both the kernel and the image of a linear map are subspaces.*

PROOF. Since $f(\underline{0}_V) = \underline{0}_W$, we have $\underline{0}_V \in \operatorname{Ker}(f)$ and $\underline{0}_W \in \operatorname{Im}(f)$. Next, let $\underline{u},\underline{v} \in \operatorname{Ker}(f)$ and let $\alpha \in F$. Then $f(\alpha\underline{u} + \underline{v}) = \alpha f(\underline{u}) + f(\underline{v}) = \alpha \cdot \underline{0} + \underline{0} = \underline{0}$. Thus $\operatorname{Ker}(f)$ is closed under addition and scalar multiplication. Similarly, let $\underline{x},\underline{y} \in \operatorname{Im}(f)$. Choose $\underline{u},\underline{v} \in V$ so that $f(\underline{u}) = \underline{x}$, $f(\underline{v}) = y$. Then $f(\alpha\underline{u} + \underline{v}) = \alpha f(\underline{u}) + f(\underline{v}) = \alpha\underline{x} + \underline{y}$, that is that $\alpha\underline{x} + \underline{y} \in \operatorname{Im}(f)$. □

CHAPTER 5

Error-correcting codes: Block codes (1-3/11/2011)

Problem: two parties (Alice and Bob) would like to communicate across a noisy channel.

Model: There is a "channel alphabet" Σ. The channel recieves symbols from Alice one at a time, and gives Bob symbols one at a time. Symbols are never lost or created, but occasionally Bob may receive a different symbol from the one Alice sent.

Example: $\Sigma = \{0,1\}$. Alice sends 000110 Bob gets 001111.

Goal: transmit accurate information despite potential errors.

Idea: Alice will create *redundancy* in the symbols she sends; thus few errors will not destroy any information.

5.1. Block codes (abstract picture)

Let M be a set (the "message alphabet"). Fix an integer n (the *block size*) and a subset $C \subset \Sigma^n$ (the *code*) with the same size as M. Let $d = \min\{d_{\mathrm{H}}(\underline{u},\underline{v}) \mid \underline{u} \neq \underline{v} \in C\}$ be the *separation* or *minimal distance*.

Fix a bijection $E\colon M \to C$ ("encoding").

Block Encoding: For each $m \in M$ that Alice wishes to send, she will trasmit the sequence $\underline{s} = E(m)$.

Block Decoding: After he recieves $\underline{r} \in \Sigma^n$, Bob will take $D(\underline{r})$ to be that element of M such that $E(m)$ is closest to $\underline{r}$.

PROPOSITION 101. *(Hamming) Assume that the channel can introduce at most e errors per block. Then:*

(1) *If $e < d$ then Bob will always know that errors have occured.*
(2) *If $e < \frac{d}{2}$ then Bob will recover the message Alice sent. ("C can correct e errors")*

PROOF. Say Alice sends $\underline{s}$, Bob recieves $\underline{r}$. In case (1), the only possibility for $\underline{r} \in C$ is if $\underline{r} = \underline{s}$, since other elements are at least d away. In case (2), $d_{\mathrm{H}}(\underline{r},\underline{s}) < \frac{d}{2}$ implies that for any other codeword $\underline{c} \in C$, $d_{\mathrm{H}}(\underline{r},\underline{c}) \geq d_{\mathrm{H}}(\underline{c},\underline{s}) - d_{\mathrm{H}}(\underline{r},\underline{s}) > d - \frac{d}{2} = \frac{d}{2} > d_{\mathrm{H}}(\underline{r},\underline{s})$. It follows that $\underline{s}$ is the unique member of C closest to $\underline{r}$. □

REMARK 102. When d is even, Bob can recover the message if $e < \frac{d}{2}$ and tell if there was an error when $e = \frac{d}{2}$ (the two cases are incompatible). Thus his algorithm will preform *reliably* as long as there are at most $\frac{d}{2}$ errors.

EXAMPLE 103. (PS7) Repetition codes.

DEFINITION 104. The *rate* of the code is $\frac{\log_{\#\Sigma} C}{n}$.

EXAMPLE 105. (PS8) Code with rate $\frac{4}{7}$.

REMARK 106. In class we compared channels with adversarial error (channel can freely choose which bits to corrupt) to channels with probabilistic error (corrupted bits are chosen at random).

DEFINITION 107. Call two codes $C,D \subset \Sigma^n$ *equivalent* if one can be obtained from the other by permuting the co-ordinates.

5.2. Linear codes

5.2.1. Setup. Take $\Sigma = F$ for a finite field F (usually $F = \mathbb{F}_2$). The "blocks" we will transmit will then be vectors in F^n. A subspace $C \subset F^n$ will be called a *linear code*.

Assume that $\dim_F C = k$. Then C *i*s isomorphic to F^k for some k, and the encoding map will be a linear isomorphism $G\colon F^k \to C$ called the "generating matrix".

REMARK 108. (Linear Algebra) We identify G with its matrix (an element of $M_{n\times k}(F)$). Then C is the *column space* of G, that is the span of its columns. In other words, choose k linearly independent vectors $\underline{v}^1,\ldots,\underline{v}^k \in C$ which span it. Then the matrix $G \in M_{n\times k}(F)$ with these vectors as columns, $G = \left(\underline{v}^1 \cdots \underline{v}^k\right)$, defines a linear map $G\colon M_{n\times k}(F) \to F^n$ with image exactly C.

- *Goal*: Find C of large dimension (high rate) and large separation (good error-correction).

NOTATION 109. (Hamming) Call C and $[n,k]$-code if C is a k-dimensional subspace of F^n. Call C an $[n,k,d]$-code if it is an $[n,k]$-code with minimal distance d.

Our definition of equivalence from above translates to the following: two linear codes $C,D \subset F^n$ are equivalent iff there exists an $n \times n$ permutation matrix Π such that $\Pi(C) = C'$.

5.2.2. Encoding, the standard form and the parity check matrix.

PROPOSITION 110. *(Column reduction) Up to permuting the co-ordinates of F^n (that is, up to replacing C with an equivalent code), we may assume that the generating matrix G is of the* "standard form" $\begin{pmatrix} I_k \\ P \end{pmatrix}$ *with I_k the $k\times k$ identity matrix and $P \in M_{(n-k)\times k}(F)$.*

PROOF. The usual column reduction procedure does not change the column span of the matrix G while converting it to one with k of its rows matching those of the identity matrix. To obtain the desired form we now permute the rows, which amounts to passing to an equivalent code. The procedure does not terminate early because G has rank k – its columns must all be linearly independent since they span the k-dimensional space C. □

NOTATION 111. When the encoding function is given by a matrix G in standard form, we say that the first k entries of $\underline{v} \in C$ are *data bits*, the other $n-k$ entries are *check bits*.

LEMMA 112. *Given $G \in M_{n\times k}$ of the form $\begin{pmatrix} I_k \\ P \end{pmatrix}$, let $H \in M_{(n-k)\times n}$ be the matrix $\begin{pmatrix} P & -I_{n-k} \end{pmatrix}$. Then the column space $C = \mathrm{Im}(G) = G(F^k)$ equals the nullspace $\mathrm{Ker}(H) = \{\underline{v} \in F^n \mid H\underline{v} = \underline{0}\}$.*

PROOF. Let C' denote the kernel of H. For $\underline{m} \in F^k$, let $\underline{v} = G\underline{m}$ be its encoding. Then $\underline{v} = \begin{pmatrix} \underline{m} \\ P\underline{m} \end{pmatrix}$. Then $\begin{pmatrix} P & -I_{n-k} \end{pmatrix} = P\underline{m} - I_{n-k}(P\underline{m}) = P\underline{m} - P\underline{m} = \underline{0}$. In other words, every $\underline{v} \in C$ belongs to the nullspace C'. For the converse, Say $H\underline{v} = \underline{0}$ for some $\underline{v} \in F^n$ and let $\underline{m} \in F^k$ be the first k entries of $\underline{v}$, $\underline{r} \in F^{n-k}$ the remaining entries. Then $\begin{pmatrix} P & -I_{n-k} \end{pmatrix}\underline{v} = \underline{0}$ reads: $P\underline{m} - I_{n-k}\underline{r} = \underline{0}$, or $\underline{r} = P\underline{m}$, but this exactly means $\underline{v} = G\underline{m}$ and $\underline{v} \in C$. □

We have thus found three roughly equivalent ways to describe an $[n,k]$-code:

- As a k-dimensional subspace $C \subset F^n$.
- As the column space (image) of an encoding matrix $G\colon F^k \to F^n$, preferably of standard form.
- As the nullspace (kernel) of a parity-check matrix $H\colon F^n \to F^{n-k}$, preferably of standard form.

5.2.3. Linear decoding and weights. Say Alice wants to send the message $\underline{m} \in F^k$. She encodes it as $\underline{s} = G\underline{m} \in C$ which she sends to Bob. Bob recieves some vector $\underline{r} \in F^n$, perhaps different from $\underline{s}$. Let $\underline{e} = \underline{r} - \underline{s}$ be the "error", which is not known to Bob. Then $H\underline{e} = H\underline{r}$ since $H\underline{s} = \underline{0}$. Thus decoding amounts to solving the inhomogenous linear equation $H\underline{x} = (H\underline{r})$ – one of its solutions is the desired error $\underline{e}$. The Block-decoding method of least distance amount to choosing among all solutions the one with *minimal weight* and guessing it to be the error vector:

DEFINITION 113. Let $\underline{v} \in F^n$. The *weight* of $\underline{v}$ is the number of non-zero entries in $\underline{v}$. We write it as $w(\underline{v}) = d_{\mathrm{H}}(\underline{v}, \underline{0})$.

LEMMA 114. *For a linear code, the* separation d *(see Section 5.1) and the* minimal weight $w(C) = \min\{w(\underline{v}) \mid \underline{v} \in C, \underline{v} \neq \underline{0}\}$ *coincide.*

PROOF. We have $d = \min\left\{d_{\mathrm{H}}(\underline{x},\underline{y}) \mid \underline{x},\underline{y} \in C\right\}$. Since $\underline{0} \in C$ (it's a subspace), the distance of a non-zero codeword to $\underline{0}$ is at least the minimal distance of any two codewords, so $w(C) \geq d$. Conversely, for any $\underline{x},\underline{y} \in C$ we have $d_{\mathrm{H}}(\underline{x},\underline{y}) = w(\underline{x}-\underline{y})$ and $\underline{x}-\underline{y} \in C$ since C is a subspace. This means that the set of distances of codewords is exactly the set of weights of codewords. In particular, the minimal distance is also a weight and $w(C) \leq d$. □

We can now rephrase our abstract block-decoding algorithm from above. Having received $\underline{r}$, Bob guesses that the errror $\underline{e} = \underline{r} - \underline{s}$ is such to make $\underline{r}$ as close to $\underline{s} \in C$ as possible, that is such that $\underline{e}$ has minimal weight among all possible $\underline{e}$. We thus have:

Block Decoding for Linear Codes: After he recieves $\underline{r} \in \Sigma^n$, Bob will take $\underline{e}$ to be that solution $\underline{x}$ of $H\underline{x} = H\underline{r}$ with minimal weight. He then guesses $\underline{s} = \underline{r} - \underline{e}$.

Math 342 Problem set 9 (due 8/11/11)

The Parity Code

Let $p\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be the *parity map* $p(v_1,\ldots,v_n) = \sum_{i=1}^n v_i$ where the addition is in $\mathbb{F}_2$.

1. Calculate the parity of the following bit vectors: 00110101, 01101011, 11011111, 00000000.

– We saw in class that p is a linear transformation. By Lemma 100 of the notes, $P = \left\{\underline{v} \in \mathbb{F}_2^n \mid p(\underline{v}) = 0\right\}$ is a subspace. Call it the *parity code*.

3. The *weight* of a vector is its number of non-zero entries, equivalently its Hamming distance from the zero vector. The *weight* of a linear code is the smallest weight of a non-zero vector. What are the possible weights of elements of P? Show that the code P has weight 2.

4. Say $n = 8$. Take the following 7-bit vectors and extend them to vectors in P: 0011010, 0110101, 1101111, 0000000.

5. Show that for any 7-bit vector there is a unique 8-bit extension with even parity. Let the extension map be $G\colon \mathbb{F}_2^7 \to \mathbb{F}_2^8$. Write down the matrix for this map – the *generator matrix* of the code P.

6. It is often said that parity can detect one error, but cannot correct any. Give an example of a bit vector $\underline{v}' \in \mathbb{F}_2^8$ and *two* distinct vectors $\underline{u}, \underline{v} \in P$ both at distance 1 from $\underline{v}'$. Explain why your example validates the saying.

A non-linear code

Let $m \geq 1$, and let $n = 2^m$. Construct a subset $C_m \subset \mathbb{F}_2^{2^m}$ of size $2(m+1)$ as follows: for every k, $0 \leq k \leq m$, divide the 2^m co-ordinates into 2^{m-k} consecutive blocks of length 2^k (so if $k = m$ you get only one block, if $k = m-1$ you get two blocks each with half the co-ordinates, with $k = 0$ every block has size 1). Now fill the first block with all zeros, the second block with all ones and keep alternating. Put the resulting vector in C_m, as well as the one obtained by the reverse procedure (i.e. by starting with 1). Here's the example with $m = 3$, $n = 8$:

$k = 3$: 00000000, 11111111; $k = 2$: 00001111, 00001111; $k = 1$: 00110011, 11001100, $k = 0$: 01010101, 10101010.

7. For any distinct $\underline{x}, \underline{y} \in C_m$, should that $d_{\mathrm{H}}\left(\underline{x}, \underline{y}\right) \geq \frac{n}{2}$.
Hint: First work out the case $m = 3$ from the example, but you need to address the case of general m.

8. How many errors can this code correct? How many errors can it detect?

9. For the case $m = 3$, find the nearest codeword to the received words 00010101, 11010000, 10101010 (prove that you found the right codeword!).

10. For $m \geq 2$, show that $C_m \subset \mathbb{F}_2^n$ is *not* a subspace of $\mathbb{F}_2^n$. Thus this code is not linear.

CHAPTER 6

Abstract Algebra II: Rings of Polynomials (16-20/3)

6.1. Polynomials

DEFINITION 115. Let F be a field. By a *polynomial over F in the variable x* we mean a finite expression

$$f(x) = \sum_{i=0}^{d} a_i x^i$$

with $a_0, a_1, \ldots, a_d \in F$, with the proviso that the *leading coefficient a_d* is non-zero unless $d = 0$. We call d the *degree* of f, a_i the *coefficients*. Call f *monic* if $a_d = 1$. We let $F[x]$ denote the set of all polynomials.

EXAMPLE 116. $0x^0$, $1x^0$, $0x^0 + 0x + x^2$, $1x^0 + x + 0x^2 + \pi x^3$ are all elements of $\mathbb{R}[x]$, of degress $0, 0, 2, 3$.

REMARK 117. From now on we supress monomials with coefficient zero, supress the expression x^0 and identify polynomials which differ only in having or omitting zero monomials. We can thus write the same polynomials as: 0, 1, x^2, $1 + x + \pi x^3 + 0x^4$. The degrees are still $0, 0, 2, 3$.

DEFINITION 118. Let $f, g \in F[x]$ have the forms $f = \sum_{i=0}^{d} a_i x^i$, $g = \sum_{j=0}^{e} b_j x^j$, $\alpha \in F$. We make the following definitions:

$$\begin{aligned}
f + g &\overset{\text{def}}{=} \sum_{i=0}^{\max d,e} (a_i + b_i) x^i ; \\
f \cdot g &\overset{\text{def}}{=} \sum_{k=0}^{d+e} \left(\sum_{i+j=k} a_i b_j \right) x^k ; \\
\alpha \cdot f &\overset{\text{def}}{=} \sum_{i=0}^{d} (\alpha a_i) x^i .
\end{aligned}$$

PROPOSITION 119. *These definitions give $F[x]$ the structure of both a vector space over F and a commutative ring.*

PROOF. Let $F[x]^{\leq d}$ denote the set of polynomials of degree less than $d \geq 1$. Note that it is closed under both the addition and scalar multiplication operations defined above; we start by showing that it is a vector space. For this let $M\colon F^{d+1} \to F[x]^{\leq d}$ be the map

$$M \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{d-1} \\ a_d \end{pmatrix} = \sum_{i=0}^{d} a_i x^i .$$

Then M is a bijection which respects addition and scalar multiplication. That the vector space axioms hold in $F[x]^{\leq d}$ then follows immediately from the fact that F^{d+1} is a vector space. In particular, the zero polynomial (the only with all coefficients zero) serves as the zero vector, and if $f = \sum_{i=0}^{d} a_i x^i$ is a polynomial then its additive inverse is $-f = \sum_{i=0}^{d}(-a_i)x^i$.

To check the vector space axioms in $F[x]$ note that in any particular instance it's enough to calculate in $F[x]^{\leq d}$ for d large enough. For example, to see if $(f+g)+h = (f+g)+h$ for any three polynomials one notes that if d is larger than the degrees of all three then all sums to be considered lie in $F[x]^{\leq d}$, which is a vector space.

Next, we check that $F[x]$ is also a ring. First, it is clear that $1 = 1x^0$ is a multiplicative identity: $\left(\sum_{i=0}^{d} a_i x^i\right) \cdot \left(1x^0\right) = \sum_{i=0}^{d} (a_i \cdot 1)\, x^{i+0} = \sum_{i=0}^{d} a_i x^i$. We also checked the addition axioms, so it remains to see that multiplication is associative and commutative and that the distributive law holds. The definition is symmetric in the a's and b's (multiplication in F is commutative), so multiplication is commutative. For associativity, we calculate:

$$\begin{aligned}
\left(\sum_{i=0}^{d} a_i x^i \cdot \sum_{j=0}^{e} b_j x^j\right) \cdot \sum_{k=0}^{f} c_k x^k &= \left(\sum_{l=0}^{d+e} \left\{\sum_{i+j=l} a_i b_j\right\} x^l\right) \cdot \left(\sum_{k=0}^{f} c_k x^k\right) \\
&= \sum_{m=0}^{d+e+f} \left[\sum_{n+k=m} \left\{\sum_{i+j=n} a_i b_j\right\} c_k\right] x^m \\
&= \sum_{m=0}^{d+e+f} \left[\sum_{i+j+k=m} (a_i b_j)\, c_k\right] x^m .
\end{aligned}$$

A similar calculatio shows:

$$\sum_{i=0}^{d} a_i x^i \cdot \left(\sum_{j=0}^{e} b_j x^j \cdot \sum_{k=0}^{f} c_k x^k\right) = \sum_{m=0}^{d+e+f} \left[\sum_{i+j+k=m} a_i \left(b_j c_k\right)\right] x^m .$$

We may now apply the associative law of F. For the distributive law, we have:

$$\begin{aligned}
\left(\sum_{i=0}^{d} a_i x^i + \sum_{j=0}^{e} b_j x^j\right) \cdot \sum_{k=0}^{f} c_k x^k &= \left(\sum_{i=0}^{\max\{d,e\}} (a_i + b_i) x^i\right) \cdot \left(\sum_{k=0}^{f} c_k x^k\right) \\
&= \sum_{m=0}^{\max\{d,e\}+f} \left[\sum_{i+k=m} (a_i + b_i) c_k\right] x^m \\
&= \sum_{m=0}^{\max\{d,e\}+f} \left[\sum_{i+k=m} a_i c_k + b_i c_k\right] x^m \\
&= \left\{\sum_{m=0}^{\max\{d,e\}+f} \left[\sum_{i+k=m} a_i c_k\right] x^k\right\} + \left\{\sum_{m=0}^{\max\{d,e\}+f} \left[\sum_{i+k=m} b_i c_k\right] x^k\right\} \\
&= \left(\sum_{i=0}^{d} a_i x^i \cdot \sum_{k=0}^{f} c_k x^k\right) + \left(\sum_{j=0}^{e} b_j x^j \cdot \sum_{k=0}^{f} c_k x^k\right) .
\end{aligned}$$

□

REMARK 120. All this makes sense for any ring R (perhaps non-commutative), giving us the ring $R[x]$ of polynomials over R. For example, note that $M_n(R)[x] \simeq M_n(R[x])$.

REMARK 121. We will later use the k-dimensional space $\mathbb{F}_p[x]^{<k}$ as our *message space* for the *Reed-Solomon code*.

6.2. $F[x]$ is like $\mathbb{Z}$ – compare with Chapter 2

Fix a field F.

LEMMA 122. *(Degree valuation) Let $f, g \in F[x]$. Then* $\deg(fg) = \deg(f) + \deg(g)$ *and* $\deg(f + g) \leq \max\{\deg f, \deg g\}$*, with equality if* $\deg f \neq \deg g$.

LEMMA 123. *Let $f, g \in F[x]$. Then*

(1) *(zero-divisors) $fg = 0$ only if one of f, g is zero.*
(2) *(units) $fg = 1$ only if $\deg f = \deg g = 0$ and $fg = 1$ in F.*

PROOF. Consider the coefficients of highest degree. □

REMARK 124. ("Well-ordering principle in $F[x]$") Let $S \subset F[x]$ be non-empty. Then S contains an element of smallest degree.

PROOF. Look at the image of S under the map $\deg\colon F[x] \to \mathbb{N}$. □

6.2.1. Division with remainder.

THEOREM 125. *(Division with remainder) Let $f, g \in F[x]$ with $f \neq 0$. Then there exists unique $q, r \in F[x]$ with* $\deg r < \deg f$ *so that*

$$g = qf + r.$$

PROOF. Say $f = \sum_{i=0}^{d} a_i x^i$ with $x_d \neq 0$. Let $S = \{g - qf \mid q \in F[x]\}$, and let $r \in S$ be an element of minimal degree, say $r = \sum_{j=0}^{e} b_j x^j$ with $b_e \neq 0$. We show first that $e < d$. Otherwise, consider the polynomial $r - \left(\frac{b_e}{a_e} x^{e-d}\right) \cdot f \in S$. This is a polynomial of degree at most e, but its leading coefficient is $b_e - \frac{b_e}{a_e} a_e = 0$, hence of degree at most $\deg r - 1$, a contradiction. Secondly, we show that r is unique. For this assume that $g = q'f + r'$ also. Then $r' - r = (g - q'f) - (g - qf) = (q - q')f$. If $q \neq q'$ then the degree of the RHS is at least $\deg f$ while the degree of the LHS is strictly smaller than that, a contradiction. □

Division with remainder in practice. Consider the following algorithm:

ALGORITHM 126. *(Division with remainder) Input: Polynomials f, g. Output: q, r:*

(1) *Inititalize $q = 0$, $r = g$.*
(2) *If* $\deg r < \deg f$ *then stop and return q, r.*
(3) *Let f have degree d with leading coefficient a_d; let r have degree e and leading coefficient b_d. Then replace:*
    (a) $q \mapsto q + \left(\frac{b_e}{a_e} x^{e-d}\right)$
    (b) $r \mapsto r - \left(\frac{b_e}{a_e} x^{e-d}\right) \cdot f$
(4) *Return to step 2.*

The proof of Theorem 125 amounts to showing that the algorithm terminates in finitely many steps and calciulates the quotient and the remainder. Note the *loop invariant*: at all times (except in the middle of step 3) we have $g = qf + r$. The algorithm keeps reducing the degree of r while keeping this invariant condition true until the degree cannot be reduced anymore, at which point it must be the case that $\deg r < \deg f$.

6.2.2. Divisors, GCD, LCM and unique factorization.

DEFINITION 127. $f,g,h \in F[x]$.

- Say that f *divides* g, or that g is a *multiple* of f is there exists h such that $fh = g$.
- Say that f is *irreducible* if whenver $f = gh$ one of g,h is a unit, reducible if $f = gh$ for some g,h both of degree at least 1.
- Say that f is *prime* if whenver $f|gh$ we have either $f|g$ or $f|h$ (or both).
- If $f,g \in F[x]$ and $f = \alpha g$ for $\alpha \in F^\times$ we say that f,g are *associate*. This is an equivalence relation, and every equivalence class has a unique monic member.

DEFINITION 128. Let $f,g \in F[x]$. A *greatest common divisor* of f,g is the monic polynomial h of maximal degree which divides both of them.

THEOREM 129. *Let f,g be polynomials. Then the Euclidean algorithm will compute a GCD, which can be written in the form $hf + kg$ for some $h,k \in F[x]$.*

PROOF. Consider the set $I = \{hf + kg \mid h,k \in F[x]\}$. It is non-empty and closed under addition and under multiplication by arbitrary polynomials. If $I = \{0\}$ then $f = g = 0$ and there is nothing to prove. Otherwise let $r \in I$ be a non-zero element of minimal degree. Division with remainder then shows that $I = (r) = \{ur \mid u \in F[x]\}$, and hence that r is a common divisor of $f,g \in I$. Since every common divisor of f,g divides every element of I, every common divisor of f,g divides r so r is a common divisor of maximal degree.

That Euclid's algorithm works follows by induction on the degrees: the algorithm starts with a pair (f,g) both non-zero. Without loss of generality $\deg g \geq \deg f$ and we then replace g by its remainder when dividing by f. This reduces the degree of g, hence the total degree $\deg f + \deg g$. This cannot continue forever so after finitely many steps we must have $f = 0$ or $g = 0$, at which point we have found the GCD. □

EXAMPLE 130. $\left(5x^4+2x^3+x+5, x^2+x+2\right)$ over $\mathbb{Q}$. Then:

$$\begin{aligned}
\left(5x^4+2x^3+x+5, x^2+x+2\right) &= \left(\left(5x^4+2x^3+x+5\right)-5x^2\left(x^2+x+2\right), x^2+x+2\right) = \\
\left(-3x^3-10x^2+x+5, x^2+x+2\right) &= \left(\left(-3x^3-10x^2+x+5\right)+3x\left(x^2+x+2\right), x^2+x+2\right) = \\
\left(-7x^2+7x+5, x^2+x+2\right) &= \left(\left(-7x^2+7x+5\right)+7\left(x^2+x+2\right), x^2+x+2\right) = \\
\left(14x+19, x^2+x+2\right) &= \left(\left(x^2+x+2\right)-x\left(x+\frac{19}{14}\right), x+\frac{19}{14}\right) = \\
\left(-\frac{5}{14}x+2, x+\frac{19}{14}\right) &= \left(x-\frac{28}{5}, x+\frac{19}{4}\right) = \\
&= (1).
\end{aligned}$$

EXAMPLE 131. $(x^n-1, x^m-1) = x^{(n,m)}-1$.

PROPOSITION 132. *Every polynomial can be written as a product of irreducibles. A polynomial is irreducible iff it is prime. Every polynomial has a unique factorization into primes (up to associates).*

PROOF. Let S be the set of polynomials which cannot be written as a product of irreducibles, and let $f \in S$ be an element of minimal degree. Then f is reducible; say $f = gh$. Then $\deg g, \deg h < \deg f$. Then $g, h \notin S$ and hence they can be written as products of irreducibles – but $f = gh$, a contradiction.

Next, let f be irreducible and assume that $f|gh$. Consider $GCD(f,g)$. If it has positive degree then it is associate f since f is irreducible, and hence $f|g$. Otherwise it is equal to 1. By Bezout's Theorem there exist $k, l \in F[x]$ so that $kf + lg = 1$. Multiplying by h we find:

$$h = kfh + lgh\,.$$

Then f divides both fkh and $gh|ghl$ so that f divides h.

Finally, we show that any two representations as product of primes are the same up to associates. Say

$$\prod_{i=1}^{r} p_i = \prod_{j=1}^{s} q_j$$

where p_i, q_j are all prime. We can write $p_i = \alpha_i p_i'$, $q_j = \beta_j q_j'$ with p_i', q_j' monic. Then

$$\alpha \prod_i p_i' = \beta \prod_j q_j'$$

with $\alpha = \prod \alpha_i$, $\beta = \prod \beta_j$. Examining the leading coefficients shows $\alpha = \beta$. □

6.3. Cyclic Redundancy Check

Encode bit sequences as polynomials over $\mathbb{F}_2$: to the message $\underline{m} = 100101_2 \in \mathbb{F}_2^6$ we associate the *message polynomial* polynomial $m(x) = x^5 + x^2 + 1$ for example (in practice, take the input bit stream and divide it into blocks of size k). Fix a polynomial $F_\ell(x)$ of degree ℓ. Let $R(x) \in \mathbb{F}_2[x]^{<\ell}$ be the remainder of dividing $m(x)$ by $F_\ell(x)$. Then $R(x)$ is of degree less than ℓ, that is can be represented by ℓ bits. We then tramsit the $n = k + \ell$ bit vector (m, R).

EXAMPLE 133. (Good choices)

(1) $F_2(x) = x + 1$ ("parity") – one-bit redundancy
(2) $F_4(x) = x^4 + x + 1$
(3) $F_{16} = x^{16} + x^{12} + x^5 + 1$ (used by Bluetooth, CDMA cellular telephony) – 16-bit redundancy
(4) $F_{32} = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$ (used in MPEG & PNG) – 32-bit redundancy.

EXAMPLE 134. (Bad choice) Show that the remainder of dividing $m(x)$ by x^ℓ is simply the sum of the monomials of degree less than ℓ. Conclude that taking $F_\ell = x^\ell$ amounts to resending the lowest-order ℓ bits twice, getting no redundancy about the high-order bits.

- **CRC Encoding:** Given the polynomial $m(x)$ send (m, R) where $m(x) = Q(x) \cdot F_\ell(x) + R(x)$.
- **CRC Check:** Given the pair (m', R') check if $m' = Q'(x) \cdot F_\ell(x) + R'(x)$. If not, ask for retransmit.

LEMMA 135. *Let $m(x) \in \mathbb{F}_2[x]$. Then $m(1)$ is the parity of its coefficient bit vector, and $m(x) = Q(x) \cdot (x+1) + m(1)$ for some polynomial $Q(x)$.*

PROOF. Since $1^i = 1$ for all i (even $i = 0!$), $m(1) = \sum_{i=0}^{k-1} m_i$. Doing the addition in $\mathbb{Z}$ would give the number of 1s, and projecting mod 2 gives the parity. Next, by the division theorem, can write $m(x) = Q(x)(x+1) + R(x)$ for a polynomial R of degree< 1, that is a constant. Plugging in 1 and using $1+1 = 0$ shows:

$$m(1) = Q(1) \cdot (1+1) + R = R.$$

□

PROPOSITION 136. *Let k be of arbitrarily large size compared to ℓ. Assume $F_\ell(0) = 1$. Then CRC with F_ℓ can detect any "burst error" of length $\leq \ell$ in the message, that is any change which is confined to a sequence of bits of length at most ℓ.*

PROOF. We show that if $m - m' = \sum_{i=0}^{l-1} a_i x^{t+i}$ for some t then $m \not\equiv m' \,(F_l)$. Indeed, we can write $m - m' = x^t \cdot g$ where $\deg(g) \leq l-1$. Now $(F_l, x) = 0$ since $F_l(0) = 1$, so if F_l divided $m - m'$ it would also divide g which is impossible. □

EXAMPLE 137. With CRC-4, say the message is $m(x) = x^{10} + x^7 + x^2 + x$. Then $m(x) - x^6 F_4(x) = x^6 + x^2 + x$, so $m(x) - (x^6 + x^2)F_4(x) = x^3 + x$, so $m(x) = (x^6 + x^2 + 1)F_4(x) + (x^3 + x)$ and $R(x) = x^3 + x$. We transmit

$$(10010000110, 1010)$$

. Let's say that we have a 2-bit error in the message, and the recipient gets

$$(10001000110, 1010)$$

instead (changed coefficients of x^6, x^7 instead). Then the difference of the two is $x^7 + x^6$ (check), which we can also write as $x^6(x+1)$. This is not zero modulu F_4 since F_4 is relatively prime to x, and $(x+1)$ has smaller degree than F_4, so the remainders cannot match.

PROOF. Let $\underline{m} \in \mathbb{F}_2^k$ be the message bit sequence, $m(x)$ be the associated polynomial, and say $m(x) = Q(x)F_\ell(x) + R(x)$ so we transmit (m, R). Say $\underline{m'}$ is obtained from $\underline{m}$ by changing the bits in positions between $i, i+1, \ldots, i+\ell-1$. To ensure that the check will work, we have to see that m' has a different remainder than m when divided by F_ℓ.

For this we use the usual paradigm of taking the *difference.* Consider the error polynomial $e(x) = m'(x) - m(x)$ – it has the form

$$a_i x^i + a_{i+1} x^{i+1} + \cdots + a_{i+\ell-1} x^{i+\ell-1}.$$

Taking out a common factor this means $e(x) = x^i \cdot f(x)$ with $f(x)$ of degree at most $\ell - 1$. Now assume by contradiction that $m'(x) = Q'(x)F_\ell(x) + R(x)$ with the *same* remainder. Then we'd have $m'(x) - m(x) = (Q'(x) - Q(x))F_\ell(x)$, that is $F_\ell(x) | e(x)$. But $F_\ell(0) = 1$ means that F_ℓ is relatively prime to x, hence to x^i, so if F_ℓ divides $x^i f(x)$ it must divide $f(x)$. But $f(x)$ is of smaller degree, so this is impossible. □

REMARK 138. CRC is very effective at *detecting* errors (especially burst errors) but not as effective in *correcting* them. It does not have good separation.

6.4. Reed-Solomon Codes

6.4.1. Polynomials and roots. Fix a field F. To every $f \in F[x]$ we can associate a function $x \mapsto f(x)$ from F to F given by evaluating the polynomial. We denote the function by the same letter. This gives a map $F[x] \to F^F$ which is both a ring homomorphism and a linear map of F-vector spaces.

DEFINITION 139. Call $a \in F$ a *root* of $f \in F[x]$ if $f(a) = 0$.

LEMMA 140. *a is a root of f iff $(x-a)|f$.*

PROOF. If $f(x) = (x-a)\cdot g(x)$ then $f(a) = (x-a)g(a) = 0$. If $f(a) = 0$ then $f(x) = f(x) - f(a)$. Now $x^n - a^n$ is divisible by $(x-a)$ for all n, and $f(x) - f(a)$ is a linear combination of such. □

LEMMA 141. *For any $a \in F$, the polynomial $x - a \in F[x]$ is prime, and any two such are relatively prime.*

PROOF. If $x - a \mid fg$ then $f(a)g(a) = 0$. It follows that either $f(a) = 0$ or $g(a) = 0$ (or both). Also, by Euclid's Algorithm $(x-a, x-b) = (b-a, x-b) = (1, x-b) = 1$ as long as $b - a \neq 0$. □

COROLLARY 142. *Let $\{a_i\}_{i=1}^k \subset F$ be roots of f. Then $\prod_{i=1}^k (x-a_i)|f$.*

PROOF. They are all relatively prime and divide f separately. □

COROLLARY 143. *A non-zero polynomial with k distinct roots has degree at least k.*

PROPOSITION 144. *Let F be a finite field with q elements, $f, g \in F[x]$ polynomials of degree at most $q-1$. Then $f(a) = g(a)$ for all $a \in F$ if and only if $f = g$ as polynomials.*

PROOF. The polynomial $f - g$ has degree at most $q-1$. If it vanishes at every $a \in F$ then it has at least q distinct roots. Hence $f - g$ is the zero polynomial. □

REMARK 145. Fermat's Little Theorem is the statement that x^p and x give the same function on $\mathbb{F}_p$, so this is optimal.

6.4.2. Reed-Solomon Codes. Let $\mathbb{F}_q$ be a finite field and let $k \leq q$. Let $M = \mathbb{F}_q[x]^{<k}$ (the "message space") be the k-dimensional vector space of all polynomials of degree less than k. Let $\{e_i\}_{i=1}^n \subset \mathbb{F}_q$ be distinct points. We then have the following linear map ("Reed-Solomon encoding")

$$\begin{array}{rcl} E_{\mathrm{RS}} \colon M & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(e_i))_{i=1}^n \,. \end{array}$$

EXAMPLE 146. $q = 7$, $n = 6$, $k = 2$. The points will be $1,2,3,4,5,6$ modulu 7. To encode the message $([1],[3]) \in \mathbb{F}_7^2$ we think of it as the polynomial $f = 1 + 3x$, and tramsmit the six values

$$\begin{array}{rcl} f(1) & = & [4]_7 \\ f(2) & = & [7]_7 = [0]_7 \\ f(3) & = & [3]_7 \\ f(4) & = & [6]_7 \\ f(5) & = & [2]_7 \\ f(6) & = & [5]_7 \end{array}$$

that is we send $([4]_7,[0]_7,[3]_7,[6]_7,[2]_7,[5]_7)$.

PROPOSITION 147. *Let $C_{RS} \subset \mathbb{F}_q^n$ be the code, that is the image of the encoding map. Then C_{RS} is an $[n,k,n-k+1]$-code.*

PROOF. C_{RS} is the image of a linear map, hence a linear subspace. Let $\underline{v} \in C$ have weight at most $n-k$, and say $\underline{v}$ encodes the polynomial f. Then the polynomial f (of degree$< k$) vanishes in at least $n-(n-k)$ points. It follows that $f=0$ and hence that $\underline{v}=\underline{0}$. □

EXAMPLE 148. In the case above with $q=7$, $n=6$, $k=2$ we have $d=5$. In other words, we should be able to correct 2 errors. Say we recieve $\underline{v}' = ([4]_7,[1]_7,[3]_7,[2]_7,[2]_7,[5]_7)$ – how do we tell what was sent? We look for the line that passes through as many points as possible: for every pair i,j we look at the unique line through the points (i,v'_i) and $\left(j.v'_j\right)$ and try to see how many points its passes through. For example, the line through $(1,4)$ and $(2,1)$ (mod 7) is $[4]_7x+[0]_7$. This line also passes through $(4,2)$, so through a total of 3 points. The line through $(1,4)$ and $(3,3)$ is $[3]_7x+[1]_7$. It passes through $(5,3)$ and $(6,5)$ so through 4 points total – so this line is consistent with at most 2 errors. Since at most one line can do that, this line is best.

Math 342 Problem set 10 (due 22/11/11)

Working with polynomials

1. For each pair of polynomials f,g below, find $q,r \in \mathbb{Q}[x]$ such that $g = qf + r$ and $\deg r < \deg f$.
   (a) $g = 2x+4$, $f = 2$.
   (b) $g = 2x+4$, $f = x+1$.
   (c) $g = 2x+4$, $f = x^2-2$
   (d) $g = x^6+5x^4+3x^3+x+1$, $f = x^2+2$.

2. Same as problem 1, but reduce all coefficients modulu 5. Thus think of f,g as elements of $\mathbb{F}_5[x]$ and find q,r in $\mathbb{F}_5[x]$.

3. Simplify the products $(x+1)\cdot(x+1) \in \mathbb{F}_2[x]$, $(x+1)(x+1)(x+1) \in \mathbb{F}_3[x]$. Explain why x^2+1 is not irreducible in $\mathbb{F}_2[x]$ (even though it is irreducible in $\mathbb{Z}[x]$!)

4. The following transmissions were made using CRC-4. Decide whether the recieved message should be accepted. Write an identity of polynomials justifying your conclusion.
   (a) $(00000000, 0000)$
   (b) $(00000100, 0000)$
   (c) $(00101100, 0000)$
   (d) $(10110111, 1011)$

5. Over the field $\mathbb{F}_5$ we would like to encode the following three-digit messages by Reed-Solomon coding, evaluating at the 4 non-zero points $\{1,2,3,4\}$ modulu 5. For each message write the associated polynomial and encoded 4-digit transmission.
   (a) $\underline{m} = (1,2,3) \mod 5$ (here $m(x) = 1+2x+3x^2 \mod 5$).
   (b) $\underline{m} = (0,0,0) \mod 5$.
   (c) $\underline{m} = (1,4,2) \mod 5$.
   (d) $\underline{m} = (2,0,2) \mod 5$.

6. Working over the field $\mathbb{F}_5$, the sender has enocded two-digit messages by evaluating the associated linear polynomial at the 4 non-zero points in the same order as above. You receive the transmissions below, which may contained corrupted bits. For each 4-tuple find the linear polynomial which passes through as many points as possible.
   (a) $\underline{v}' = (1,2,3,3)$.
   (b) $\underline{v}' = (4,1,3,0)$.
   (c) $\underline{v}' = (2,4,3,1)$.

The general linear group

7. Let F be a field. Define $\mathrm{GL}_n(F) = \{g \in M_n(F) \mid \det(g) \neq 0\}$. Using the formulas $\det(gh) = \det(g)\det(h)$, $\det(I_n) = 1$ and the fact that if $\det(g) \neq 0$ then g is invertible, show that $\mathrm{GL}_n(F)$ contains the identity matrix and is closed under multiplication and under taking of inverses.

(continued on the reverse)

8. Consider the vector space $V = \mathbb{F}_p^2$ over $\mathbb{F}_p$.
   (a) How many elements are there in V? In a 1-dimensional subspace of V?
   (b) How many elements in V are non-zero? If W is a given 1-dimensional subspace, how many elements are there in the complement $V \setminus W$?
   (c) Let $\underline{w} \in V$ be a non-zero column vector. How many $\underline{v} \in V$ exist so that the 2×2 matrix $(\underline{w}\,\underline{v})$ is invertible?
   (d) By multiplying the number of choices for $\underline{w}$ by the number of choices for $\underline{v}$, show that $\mathrm{GL}_2(\mathbb{F}_p)$ has $(p+1)p(p-1)^2$ elements.

Supplementary Problems

A. (The field of rational functions) Let F be a field.
   (a) Let Q be the set of all formal expressions $\frac{f}{g}$ with $f, g \in F[x]$, $g \neq 0$. Define a relation $\sim$ on Q by $\frac{f}{g} \sim \frac{f'}{g'}$ iff $fg' = gf'$. Show that $\sim$ is an equivalence relation.
   (b) Let $F(x)$ denote the set $Q/\sim$ of equivalence classes in Q under $\sim$. Show that $F(x)$ has the structure of a field.
   Hint: Define operations by choice of representatives and show that the result is independent of your choices up to equivalence.
   (c) Show that the map $F[x] \to F(x)$ mapping $f \in F[x]$ to the equivalence class of $\frac{f}{1}$ is an injective ring homomorphism. Obtain in particular a ring homomorphism $\iota \colon F \to F(x)$.

B. (Universal properties of $F[x]$, $F(x)$) Let E be another field, and let $\varphi \colon F \to E$ be a homomorphism of rings.
   (a) Show that φ is injective.
   Hint: Assume $x \neq 0$ but $\varphi(x) = 0$ and show that $\varphi(1) = 0$.
   (b) Now let $\alpha \in E$. Show that there exists a ring homomorphism $\bar{\varphi} \colon F[x] \to E$ such that (i) $\bar{\varphi} \circ \iota = \varphi$ and (ii) $\bar{\varphi}(x) = \alpha$.
   (c) Show that there is at most one $\bar{\varphi}$ satisfying (i),(ii).
   Hint: By induction on the degree of the polynomial.
   (d) Assume that α is *transcendental* over F, that is that it is not a zero of any polynomial in $F[x]$. Show that $\bar{\varphi}$ extends uniquely to a field homomorphism $\tilde{\varphi} \colon F(x) \to E$.

C. (Degree valuation) For non-zero $f \in F[x]$ set $v_\infty(f) = -\deg f$. Also set $v_\infty(0) = \infty$.
   (a) For $\frac{f}{g} \in Q$ set $v_\infty\left(\frac{f}{g}\right) = v_\infty(f) - v_\infty(g)$. Show that v_∞ is constant on equivalence classes, thus descends to a map $v_\infty \colon F(x) \to \mathbb{Z} \cup \{\infty\}$.
   (b) For $r, s \in F(x)$ show that $v_\infty(rs) = v_\infty(r) + v_\infty(s)$ and $v_\infty(r+s) \geq \min\{v_\infty(r), v_\infty(s)\}$ with equality if the two valuations are different (cf. Problem A, Problem Set 4).
   (c) Fix $q > 1$ and set $|r|_\infty = q^{-v_\infty(r)}$ for any $r \in F(x)$ ($|0|_\infty = 0$). Show that $|rs|_\infty = |r|_\infty |s|_\infty$, $|r+s|_\infty \leq |r|_\infty + |s|_\infty$.

REMARK. When F is a finite field, it is natural to take q equal to the size of F. Then $\mathbb{F}_p(x)$ with the absolute value $|\cdot|_\infty$ behaves a lot like $\mathbb{Q}$ with the p-adic absolute value $|\cdot|_p$.

D. ($F[x]$ is a Principle Ideal Domain) Let $I \subset F[x]$ be an ideal. Show that there exists $f \in F[x]$ such that $I = (f)$, that is $I = \{f \cdot g \mid g \in F[x]\}$.

CHAPTER 7

Symmetry and Groups (23/3-2/4)

7.1. Symmetries

Rings and Fields are abstractions coming from practice of *arithmetic*. Vector spaces come from the phenomenon of *linearity*. Groups come from the phenomenon of *symmetry*.

- Symmetries of a rectange are given by the *four-group* $V = \{1,a,b,c\}$ with multiplication table $a^2 = b^2 = c^2 = 1$ and $ab = ba = c$, $bc = cb = a$, $ca = ac = b$.
- Symmetires of a square are given by the *dihedral group* $D_8 = C_2 \ltimes C_4$. This contains the *orientation-preserving* symmetries C_4.
- Isometries of the plane: rotations; affine isometries.
- Permuting the co-ordinates is a symmetry of the parity code.
- Symmetries of a vector spaces given by $\mathrm{GL}(V)$.
- Complex conjugation.

Symmetries in general.

- Universe X.
- "structure" on X: functions $f_k\colon X^k \to Y$.
- Symmetry: bijection $\sigma\colon X \to X$ such that $f_k(x_1,\dots,x_k) = f_k(\sigma x_1,\dots,\sigma x_k)$ for all $\underline{x} \in X^k$.
- Identity map is always a symmetry.
- If σ,τ are symmetries then so are σ^{-1} and $\sigma\circ\tau$.

EXAMPLE 149. The *symmetric group* on X is the set S_X of all bijections $X \to X$.

- Every symmetry group is a subset of S_X closed under inverse and composition.

LEMMA 150. *Let $R \xrightarrow{\rho} S \xrightarrow{\sigma} T \xrightarrow{\tau} U$, Then $\tau\circ(\sigma\circ\rho) = (\tau\circ\sigma)\circ\rho$. Indeed at every $r \in R$ both sides evaluate to $\tau(\sigma(\rho(r)))$.*

COROLLARY 151. *Composition is an associative operation in S_X.*

DEFINITION 152. A *group* is a triplet $(G,e,\cdot)$ where $e \in G$ and $\cdot\colon G\times G \to G$ is a binary operation such that

(1) (associative law) $\forall a,b,c \in G : (ab)c = a(bc)$.
(2) (identity) $\forall a \in G : ae = ea = a$.
(3) (inverse) $\forall a \in G : \exists \bar{a} \in G : a\bar{a} = \bar{a}a = e$.

LEMMA 153. *The symmetric group, with the identity function and composition operation is a group.*

NOTATION 154. Let $X = \{1,\dots,n\}$. We then write S_n for S_X ("the symmetric group on n letters"). We denote elements the following way:

$$\begin{pmatrix} 1 & 2 & \cdots & i & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(i) & \cdots & \sigma(n) \end{pmatrix}.$$

LEMMA 155. *The identity element and the inverse are unique.*

PROOF. Let e' be an identity as well. Then $e = ee' = e'$ since both are identities. Similarly assume that a' is also an inverse to a. Then

$$a' = a'e = a'\left(a\bar{a}\right) = \left(a'a\right)\bar{a} = e\bar{a} = \bar{a}\,.$$

□

NOTATION 156. Denote the unique inverse to a by a^{-1}.

LEMMA 157. *The inverse to ab is $b^{-1}a^{-1}$.*

PROOF. $(ab)\left(b^{-1}a^{-1}\right) = a\left(b\left(b^{-1}a^{-1}\right)\right) = a\left((bb^{-1})a^{-1}\right) = a\left(ea^{-1}\right) = aa^{-1} = e$. Similarly $\left(b^{-1}a^{-1}\right)(ab) = \left(\left(b^{-1}a^{-1}\right)a\right)b = \left(b^{-1}\left(a^{-1}a\right)\right)b = \left(b^{-1}e\right)b = b^{-1}b = e$. □

EXAMPLE 158. Not every group starts its life as a symmetry group.

- (Cyclic groups) The group $(\mathbb{Z}/n\mathbb{Z}, [0]_n, +)$ is called the *cyclic group of order n* and denoted C_n.
- (Unit groups) Let R be a ring. Then the set $(R^{\times}, 1_R, \cdot_R)$ is a group called the *group of units of* $\mathbb{R}$.

Math 342 Problem set 11 (due 29/11/11)

Reed-Solomon decoding

1. Working over the field $\mathbb{F}_5$, the sender has enocded two-digit messages by evaluating the associated linear polynomial at the 4 non-zero points of $\mathbb{F}_5$ in order. You receive the transmissions below, which may contained corrupted bits. For each 4-tuple find the linear polynomial which passes through as many points as possible.
   (a) $\underline{v}' = (1,2,3,3)$.
   (b) $\underline{v}' = (4,1,3,0)$.
   (c) $\underline{v}' = (2,4,3,1)$.

The symmetric group

2. Multiply (compose) the following permutations in S_4. Explain why the answers to (b) and (d) are the same.
   (a) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$
   (b) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$
   (c) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$
   (d) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

3. Let S_3 be the symmetric group on three letters, C_6 the group $(\mathbb{Z}/6\mathbb{Z}, [0]_6, +)$.
   (a) Show that both C_6 and S_3 have six elements.
   (b) Find two elements a,b of S_3 which do not commute (that is, such that $ab \neq ba$.
   (c) Using (b) explain why the groups S_3 and C_6 cannot be "the same group".
   (d) For the a,b you found calculate $c = (ab)(ba)^{-1} = aba^{-1}b^{-1}$. This is called the "commutator" of a,b.
   (e) Let $f\colon S_3 \to C_6$ be a group homomorphism (that is: $f(\mathrm{id}) = [0]_6$, $f(\sigma\tau) = f(\sigma) + f(\tau)$, $f(\sigma^{-1}) = -f(\sigma)$ for all $\sigma, \tau \in S_3$). Show that $f(c) = [0]_6$.
   Hint: Calculate $f(c)$ in terms of the (unknown) $f(a), f(b)$ and simplify your answer using properties of modular addition.
   (f) Conclude that any group homomorphism $f\colon S_3 \to C_6$ is not injective, in particular not an isomorphism.

Orders

4. (General cancellation property) Let G be a group and let $x,y,z \in G$. Show that if $xz = yz$ then $x = y$ and that if $zx = zy$ then also $x = y$.

5. For each $\sigma \in S_3$ find the smallest k such that $\sigma^k = \mathrm{id}$. This is called the *order* of σ.

Supplementary problems

A. Direct products and sums.

  (a) Let G,H be groups. On $G\times H$ define a binary operation by $(g_1,h_1)\cdot(g_2,h_2)\overset{\text{def}}{=}(g_1g_2,h_1h_2)$. Together with the identity element (e_G,e_H) show that this makes $G\times H$ into a group called the *direct product* of G,H.

  (b) More generally, let $\{G_i\}_{i\in I}$ be a family of groups. Let $\prod_{i\in I}G_i$ be the set of all functions f with domain I such that $f(i)\in G_i$ for all i. Give $\prod_{i\in I}G_i$ the structure of a group. This is the *direct product* of the family. When the G_i are all isomorphic to a fixed group G this is usually denoted G^I.

  (c) Let $\Sigma_{i\in I}G_i\subset\prod_i G_i$ be the set of *finitely supported* functions, that is those functions f such that $f(i)=e_{G_i}$ for all but finitely many i. Show that $\sum_{i\in I}G_i$ is a group, called the *direct sum* of the groups G_i. When the G_i are all isomorphic to a fixed group G this is sometimes denoted $G^{\oplus I}$.

B. Distinguishing direct products and sums.

  (a) Show that $C_2^{\oplus\mathbb{N}}$ is not isomorphic to $C_2^{\mathbb{N}}$, and that $\mathbb{Z}^{\oplus\mathbb{N}}$ is not isomorphic to $\mathbb{Z}^{\mathbb{N}}$.
  Hint: In both cases show that the direct sum is countable and that the direct product has the cardinality of the continuum.

  (b) Show that every element of $\sum_{n=1}^{\infty}C_n$ has finite order.

  (c) Show that $\prod_{n=1}^{\infty}C_n$ has elements of infinite order.

7.2. Subgroups and homomorphisms

DEFINITION 159. Let G be a group. A subset $H \subset G$ is a *subgroup* if $e \in H$ and if it is closed under the group operations, that is: $\forall g,h \in H : gh \in H$ and $\forall h \in H : h^{-1} \in H$. In that case we write $H < G$.

EXAMPLE 160. Every group of symmetries is a subgroup of a symmetric group.

DEFINITION 161. Let G,K be groups. A map $f\colon G \to K$ is a *homomorphism of groups* if $\forall g,h \in G\colon f(gh) = f(g)f(h)$.

LEMMA 162. *Let $f \in \mathrm{Hom}(G,K)$. Then $f(e_G) = e_K$ and $f(g^{-1}) = f(g)^{-1}$.*

PROOF. For the first claim, we have $f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G)$. Now multiply by $f(e_G)^{-1}$ on both sides. For the second note that $f(g) \cdot f(g^{-1}) = f(g^{-1})f(g) = f(e) = e$. By the uniqueness of the inverse it follows that $f(g^{-1}) = f(g)^{-1}$. □

EXAMPLE 163. $\det\colon \mathrm{GL}_n(F) \to F^{\times}$ is a group homomorhpism. $\mathrm{SL}_n(F) = \{g \in \mathrm{GL}_n(F) \mid \det(g) = 1_F\}$ is a subgroup.

EXAMPLE 164. Let V be an n-dimentional vector space over F. Then the group $\mathrm{GL}(V)$ of invertible linear transformations of V is isomorphic to $\mathrm{GL}_n(F)$ – every choice of basis gives an isomorphism where one represents each linear transformation by a matrix.

EXAMPLE 165. $\exp\colon (\mathbb{R},0,+) \to (\mathbb{R}_{>0},1,\cdot)$ is an isomorphism of groups. Its inverse is the logarithm. These statements rephrase the well-known laws:

$$e^{a+b} = e^a e^b$$

and

$$\log(xy) = \log x + \log y\,.$$

FACT 166. *(Cayley) For every group G there is an injective homomorphism $r_G\colon G \to S_G$.*

7.3. Interlude: Cyclic groups

Summary: examples of groups. We have seen already:

- The trivial group $\{1\}$.
- The symmetric groups S_n.
- Additive groups of rings and vector spaces: $(\mathbb{Z},0,+) < (\mathbb{R},0,+)$, $(\mathbb{R}^n,\underline{0},+)$.
- Unit groups of rings and fields: $\mathbb{Z}/m\mathbb{Z}^{\times}$, $\mathrm{GL}_n(F) = M_n(F)^{\times}$, $\mathbb{R}^{\times}$.
- The 4-group V (symmetry group of the rectangle).

The additive group of $\mathbb{Z}/n\mathbb{Z}$ looks like a "circle" with n spokes: adding 1 corresponds to rotating the circle by $\frac{1}{n}$, so that n rotations bring us back to the starting point. We can also think of it as a group of symmetries of the regular n-gon, "generated" by the permutation $c_n \in S_n$ defined by:

$$c_n(i) = \begin{cases} i+1 & 1 \le i \le n-1 \\ 1 & i = n \end{cases}$$

(that is, $c_n(i) = i+1 \mod n$). Then $\mathrm{id}, c_n, c_n^2, \cdots, c_n^k, \cdots, c_n^{n-1}$ are all different while $c_n^n = \mathrm{id}$ again and the cycle repeats. Since $c_n^k c_n^l = c_n^r$ if $k+l \equiv r(n)$, $C_n = \left\{c_n^k\right\}_{k=0}^{n-1} \subset S_n$ is a subgroup and it is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. A group isomorphic to C_n is called a *finite cyclic group*. Problems 5-6 of PS11 show that every element in a group "generates" a cyclic subgroup.

FACT 167. *Let F be a finite field. Then $F^\times$ is cyclic, that is isomorphic to a cyclic group.*

Say $F = \mathbb{F}_q$. Then $\mathbb{F}_q^\times$ has $q-1$ elements. Since it is cyclic,

7.4. Orders of groups and elements

DEFINITION 168. The *order* of a group is the number of its elements. The *order* of an element of a group is the order of the smallest subgroup containing it. If $x \in G$ is of finite order then the order is equal to the smallest positive integer k such that $x^k = e$. If $x \in G$ is of infinte order then $x^k \neq e$ for all $e \in \mathbb{Z} \setminus \{0\}$.

PROPOSITION 169. $\#S_n = n!$.

PROOF. The empty set has only the empty permutation, so $\#S_0 = 1$. We continue by inductionon on n. For every permutation $\sigma \in S_{n+1}$ let $\sigma(n+1) = i$. If $i = n+1$ set $\sigma' = \sigma$. Otherwise, let $j = \sigma^{-1}(n+1)$ and let σ' be the permutation:

$$\sigma'(t) = \begin{cases} i & t = j \\ n+1 & t = n+1 \\ \sigma(t) & t \neq j, n+1 \end{cases} .$$

Then σ' is injective hence a permutation. Let $f(\sigma) = \sigma \restriction_{\{1,\dots,n\}}$. Then $f(\sigma) \in S_n$. Now let $T_i = \{\sigma \mid \sigma(n+1) = i\}$. Then $f \restriction_{T_i}$ is a bijection of T_i with S_n. It follows that $\#S_{n+1} = \sum_i \#T_i = (n+1) \cdot n! = (n+1)!$. □

DEFINITION 170. For $x, y \in G$ say that x, y *belong to the same left H-coset* write $x \equiv_L y\,(H)$ if $xh = y$ for some $h \in H$ (equivalently, if $y^{-1}x \in H$).

LEMMA 171. *The relation $\equiv_L$ is an equivalence relation.*

PROOF. $x \cdot e = x$ and $e \in H$ so $x \equiv_L x\,(H)$ for all x. Next, if $xh = y$ then $x = yh^{-1}$ so $x \equiv_L y\,(H)$ iff $y \equiv_L x\,(H)$. Finally, if $x \equiv_L y \equiv_L z\,(H)$ then $y^{-1}x \in H$ and $z^{-1}y \in H$. Since H is closed under multiplcation, we also have $z^{-1}x = (z^{-1}y)(y^{-1}x) \in H$ that is $x \equiv_L z\,(H)$. □

DEFINITION 172. Equivalence classes of this relation are called (left) *cosets* of G *modulu* H. They behave very much like residue classes, except that they are not a necessarily a group. The set of equivalence classes is denoted G/H. Call $\#G/H$ the *index* of H in G and write $[G:H] \stackrel{\text{def}}{=} \#(G/H)$.

Since $\mathbb{R}^\times_{>0}$ is of index 2 in $\mathbb{R}^\times$we think of it as $\frac{1}{2}$ of the group.

EXAMPLE 173. If $G = \mathbb{Z}$, $H = m\mathbb{Z}$ then the cosets are precisely the residue classes mod m and G/H is $Z/m\mathbb{Z}$. If $G = \mathbb{R}^\times$ and $H = \mathbb{R}^\times_{>0}$ then $y^{-1}x \in H$ iff x, y have the same sign, so $G/H = \{\mathbb{R}_{>0}, \mathbb{R}_{<0}\}$. H is the coset of the identity element.

LEMMA 174. *For any $g \in G$ the set $gH = \{gh \mid h \in H\}$ is the coset (equivalence class) containing g. In particular, if A is a coset then $A = aH$ for any $a \in A$.*

PROOF. Since $(h^{-1}g)(gh') = h^{-1}h' \in H$ we have $gh' \equiv gh\,(H)$ for any $h, h' \in H$. Conversely, if $x \in G$ satisfies $x \equiv_L g\,(H)$ then $g^{-1}x \in H$ so $x = g(g^{-1}x) \in gH$. □

LEMMA 175. *The map $aH \to bH$ given by $x \mapsto ba^{-1}x$ is a bijection. Thus all cosets have the same size.*

PROOF. Indeed if $x = ah$ then $(ba^{-1})x = (ba^{-1})(ah) = bh \in bH$, and we have an inverse: the map $y \mapsto ab^{-1}y$. □

THEOREM 176. *(Lagrange) Let G be a finite group, $H < G$ a subgroup. Then $\#G = [G:H] \cdot \#H$ and in particular $\#H$ divides $\#G$.*

PROOF. G is the disjoint union of $[G:H]$ cosets. Each coset has $\#H$ elements. □

COROLLARY 177. *Let $g \in G$. Then the order of g divides the order of G.*

PROOF. If g has order k then $\left\{1, g, \dots, g^{k-1}\right\}$ is a subgroup of order k, so k divides the order of G. □

COROLLARY 178. *(Euler) Let $a \in \mathbb{Z}$ be relatively prime to m. Then $a^{\varphi(m)} \equiv 1\,(m)$.*

PROOF. Say that $[a]_m$ has order k. By Lagrange's Theorem, $k|\varphi(m)$. It follows that $[a]_m^{\varphi(m)} = \left([a]_m^k\right)^{\varphi(m)/k} = [1]_m^{\varphi(m)/k} = [1]_m$. □

DEFINITION 179. Let G be a group, H a subgroup. Call a set $X \in A$ a *system of coset representatives* for G/H if $G/H = \{xH \mid x \in X\}$. In other words, X intersects every coset at exactly one element.

EXAMPLE 180. Let F be a field, $G = \mathrm{GL}_2(F)$, $B = \left\{\begin{pmatrix} a & b \\ & d \end{pmatrix} \in \mathrm{GL}_2(F)\right\}$, $\bar{N} = \left\{\begin{pmatrix} 1 & \\ c & 1 \end{pmatrix} \in \mathrm{GL}_2(F)\right\}$. Then $\bar{N} \cup \left\{\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}\right\}$ is a system of coset representatives for G/B.

PROOF. For any $n, n' \in \bar{N}$, $n^{-1}n' \in \bar{N}$ since $\bar{N}$ is a subgroup. Since $\bar{N} \cap B = \{I_2\}$, $n \equiv n'\,(B)$ iff $n = n'$ so they are all distinct. Similarly can check that $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix} = w \not\equiv n\,(B)$ for any $n \in \bar{N}$. Next, let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ and $\begin{pmatrix} \alpha & \beta \\ & \delta \end{pmatrix} \in B$. Then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ & \delta \end{pmatrix} = \begin{pmatrix} \alpha a & \beta a + \delta b \\ \alpha c & \beta c + \delta d \end{pmatrix}.$$

If $a \neq 0$ then choosing $\alpha = \frac{1}{a}$, $\beta = -\frac{b}{a}$, $\delta = 1$, we see

$$g \equiv g' = \begin{pmatrix} 1 & 0 \\ c' & d' \end{pmatrix}.$$

Now multiplying on the right by $\begin{pmatrix} 1 & \\ & 1/d' \end{pmatrix}$ show that $g \equiv_L g''\,(B)$ with $g'' = \begin{pmatrix} 1 & 0 \\ c'' & 1 \end{pmatrix} \in \bar{N}$.

If $a = 0$ then $c \neq 0$ (since g is invertible), so we choose $\alpha = \frac{1}{c}$, $\delta = 1$ and $\beta = -\frac{d}{c}$ to show

$$g \equiv g' = \begin{pmatrix} 0 & b' \\ 1 & 0 \end{pmatrix}.$$

Now multiplying on the right by $\begin{pmatrix} 1 & \\ & 1/b' \end{pmatrix}$ shows that $g \equiv_L w\,(B)$. □

LEMMA 181. *Every system of coset representatives has exactly $[G:H]$ elements.*

Math 342 Problem set 12 (not for submission)

The subgroup generated by an element

1. Let G be a group, $g \in G$. Define a function $f \colon \mathbb{N} \to G$ by setting $f(0) = e$, $f(n+1) = f(n) \cdot g$. Extend f to a function $f \colon \mathbb{Z} \to G$ by setting $f(-n) = f(n)^{-1}$.
   (a) What is $f(1)$?
   (b) Show that for all $m, n \in \mathbb{N}$, $f(m+n) = f(m) \cdot f(n)$.
   (c) Let $n, m \in \mathbb{N}$ with $n > m$. Show that $f((-m)+n) = f(-m) \cdot f(n)$.
   Hint: Show that $f(m) \cdot f((-m)+n) = f(m) \cdot (f(-m) \cdot f(n))$ [for the LHS use part (b), for the second associativity] then use problem 3.
   (d) Show that $f(n+m) = f(n) \cdot f(m)$ for all $n, m \in \mathbb{Z}$.
   We have shown: for any group G and element $g \in G$ there exists a group homomorphism $f \colon (\mathbb{Z}, 0, +) \to G$ such that $f(1) = g$.
   OPTIONAL Show that such f is *unique.*
   Because of this we usually write $f(n)$ as g^n.

2. (Continuation)
   (a) Let $I = \{n \in \mathbb{Z} \mid f(n) = e\}$. Show that $0 \in I$ and that I is closed under addition.
   (b) Show that I is closed under multiplication by elements of $\mathbb{Z}$.
   Hint: Multiplication is repeated addition.
   OPTIONAL Show that f descends to an injection $g \colon \mathbb{Z}/I \hookrightarrow G$.

Subgroups and Lagrange's Theorem

Let $G = \mathrm{GL}_2(\mathbb{F}_p)$, and let $B = \left\{ \begin{pmatrix} a & b \\ & d \end{pmatrix} \in G \right\}, N = \left\{ \begin{pmatrix} 1 & b \\ & 1 \end{pmatrix} \in G \right\}, T = \left\{ \begin{pmatrix} a & \\ & d \end{pmatrix} \in G \right\}$.

In Problem Set 11 we saw that the order of G (the number of its elements) is $(p+1)p(p-1)^2$.

3. (orders of the groups)
   (a) Find the order of N.
   (b) Find the order of T.
   (c) Find the order of B.
   (d) Check that $\#B = \#N \cdot \#T$.

4. (Lagrange's Theorem) Among the groups G, B, N, T find all pairs such that one is a subgroup of the other. In each case verify that the order of the subgroup divides the order of the larger group. (For example: N is a subgroup of G so its order must divide the order of G).

5. (B/T; see Example 180 in the notes)
   (a) Let $n_1, n_2 \in N$ be distinct. Show that $n_1 \not\equiv_L n_2 \, (T)$. Conclude that all elements of N belong to different costs modulu T.
   Hint: what is $n_2^{-1} n_1$? When would it belong to T?
   (b) Use Lagrange's Theorem and your answer to 1(d) to show that N is a complete system of representatives for B/T.
   Hint: Can the number of cosets be larger than $\#N$?

(c) Let $g = \begin{pmatrix} a & b \\ & d \end{pmatrix} \in B$ and let $t = \begin{pmatrix} \alpha & \\ & \delta \end{pmatrix} \in T$. Calculate the product $gt \in B$.

(d) Given g, find t so that $gt \in N$. Conclude that every element of B belongs to the coset of an element of N and again show that N is a complete system of representatives.

OPTIONAL Following the same steps, show that T is a system of coset representatives for G/N.

A group isomorphism

6. Let F be a field, $G = \mathrm{GL}_n(F)$, $V = F^n$, $X = V \setminus \{\underline{0}\}$ the set of non-zero vectors.

(a) Show that for any $g \in G$, $x \in X$, we also have $gx \in X$.

(b) Show that for any $g \in G$, the map $\sigma_g \colon X \to X$ given by $\sigma_g(x) = gx$ is a bijection of X to itself.
Hint: find an inverse to the map.

(c) Show that the map $g \mapsto \sigma_g$ is a group homomorphism $G \to S_X$.

(d) Assume that σ_g is the identity permutation. Show that g is the identity matrix. Conclude that the map from part (c) is injective.

(e) Now assume $F = \mathbb{F}_2$, $n = 2$. What are the sizes of G? Of V? of X? Show that in this case the map from part (c) is surjective, hence an isomorphism.

Optional Problems

A. Let R be a commutative ring, $I \subset R$ an ideal (a non-empty subset closed under addition and under multiplication by elemenets of R). Consider the relation $f \equiv g\,(I) \iff f - g \in I$ defined for $f, g \in R$.

(a) Show that $f \equiv g\,(R)$ is an equivalence relation.

(b) Show that the set R/I of equivalence classes has a natural ring structure so that the map $Q\colon R \to R/I$ given by $Q(f) = [f]_I$ is a surjective ring homomorphism.

(c) Let J be an ideal of R/I. Show that $F^{-1}(J)$ is an ideal of R.

(d) Assume that every ideal of R is principal. Show that every ideal of R/I is principal.

B. Let F be a field, $R = F[x]$, $I = (x^n - 1) = \{f(x^n - 1) \mid f \in R\}$, $\bar{R} = R/I$. Show that the restriction of the quotient map $Q\colon R \to \bar{R}$ to the subset $F[x]^{<n}$ is bijective. It is an isomorphism of vector spaces over F.

C. The cyclic group C_n acts on F^n by cyclically permuting the co-ordinates. Show that under the usual identifications of F^n with $F[x]^{<n}$ and $F[x]^{<n}$ with $F[x]/(x^n - 1)$, the action of the generator of C_n in F^n corresponds to multiplication by x in $\bar{R}$.

D. Let $C \subset F^n$ be a *cyclic code*, that is a code for which if $\underline{v} = (v_1, \ldots, v_n)$ is a code word then $(v_2, v_3, v_{4,}, \ldots, v_n, v_1)$ is also a codeword. Show that under the correspondence above a cyclic code C is the same as an ideal in $\bar{R}$.

Hint: Let $J \subset F[x]$ be a linear subspace closed under multiplication by x. Show by induction on the degree of $f \in F[x]$ that J is closed under multiplication by f.

E. Let C be a cyclic code, $J \subset \bar{R}$ the corresponding ideal. Let $g \in R$ be a polynomial of minimal degree such that $Q(g)$ generates J (this exists by problem A(d)). Show that $GCD(g, x^n - 1)$ also generates J. Conclude that $g | x^n - 1$.

CHAPTER 8

Applied algebra: Elliptic-curve cryptography (6-8/4)

8.1. Discrete logarithm

Discssed using cyclic groups in cryptography:

- The DLP.
- Diffie-Hellman key exchange.

Discussed the computational inequivalence of isomorphic groups. Discrete log is easy to calculate in $\mathbb{Z}/p\mathbb{Z}$, believed hard in $(\mathbb{Z}/p\mathbb{Z})^{\times}$.

8.2. Elliptic curves

Discussed adding points at infinity as limiting directions; and hinted at projective geometry.

Pointed out that a line intersects a cubic at three points and used this to define the addition law on a plane cubic. Asserted that this gives a group. Plotted pictures over $\mathbb{R}$, explained that one works over $\mathbb{F}_p$.