

## MATH 30A NOTES 2009

These are lecture notes from the second part of the course starting in section 18 on rings, fields and applications to group theory.

### CONTENTS

18.	Rings and fields	2
18.1.	homomorphisms	4
18.2.	products	4
18.3.	integer multiplication	5
19.	Integral domains	7
20.	Fermat and Euler	9
20.1.	Fermat	9
20.2.	Euler	10
20.3.	Proof of Euler's formula	11
33.	Finite fields	14
33.1.	order of a field	14
33.2.	example: $GF(16)$	15
33.3.	units and polynomials	17
34.	Finite simple groups	20
34.1.	Matrices over finite fields	20
34.2.	orders of matrix groups	21
34.3.	centers of $GL$ and $SL$	22

## 18. RINGS AND FIELDS

**Definition 18.1.** A **ring**  $(R, +, \cdot)$  is a set  $R$  with two binary operations: addition  $+$  and multiplication  $\cdot$  so that

- (1)  $(R, +)$  is an additive group.
- (2) Multiplication is associative.
- (3) Multiplication distributes over addition on both sides, i.e.:

$$a(x + y) = ax + ay$$

$$(x + y)b = xb + yb$$

**Example 18.2.**  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  are rings with the usual operations of addition and multiplication. We will assume that multiplication is associative and distributive over addition without proof for these common rings. These rings are all commutative rings.

**Definition 18.3.** A **commutative ring** is ring  $R$  in which the multiplication is commutative:  $ab = ba$  for all  $a, b \in R$ . (Addition is always commutative.)

**Example 18.4.**  $M_n(\mathbb{R})$  is the ring of all  $n \times n$  matrices with coefficients in  $\mathbb{R}$ . This is a ring with matrix addition

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})_{ij}$$

and matrix multiplication:

$$(a_{ij})(b_{ij}) = \left( \sum_{j=1}^n a_{ij}b_{jk} \right)_{ik}$$

The notation is that  $(xxx)_{ij}$  is the matrix whose  $ij$  entry is the thing written in  $xxx$ . A more precise, rigorous definition is:  $AB = C$  where the entries of  $C$  in terms of the entries of  $A, B$  are:

$$c_{ij} = \sum_{k=1}^n a_{ik}b_{kj}$$

The ring  $M_n(\mathbb{R})$  is not commutative for  $n \geq 2$ . For example:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

**Proposition 18.5.** If  $R$  is any ring then  $M_n(R)$ , the set of  $n \times n$  matrices with coefficients in  $R$

But these rings all have unity.

**Definition 18.6.** A ring with **unity** is a ring containing an element  $1$  which is the multiplicative identity:

$$1x = x1 = x$$

for all  $x \in R$ . Unity is unique if it exists.

In the case of  $M_n(\mathbb{R})$  it is the  $n \times n$  identity matrix  $I_n$ . For an arbitrary ring  $R$ ,  $M_n(R)$  has unity if and only if  $R$  has unity.

**Definition 18.7.** If  $R$  is a ring with unity then a **unit** in  $R$  is defined to be an element  $u \in R$  which has a two-sided multiplicative inverse:  $u^{-1}$ :

$$u^{-1}u = 1 = uu^{-1}$$

The inverse is unique if it exists.

**Example 18.8.** In the ring  $(\mathbb{Z}_6, +_6, \cdot_6)$  the elements are:  $0, 1, 2, 3, 4, 5$ . Of these  $0$  is the zero (additive identity)  $1$  is unity,  $5$  is a unit since  $5 \cdot 5 = 1$  and the others are zero divisors since  $2 \cdot 3 = 0$  and  $3 \cdot 4 = 0$ .

**Definition 18.9.** If  $ab = 0$  in a ring then  $a, b$  are called **zero divisors**.  $a$  is a **left zero divisor** and  $b$  is a **right zero divisor**.

A **left annihilator** for the ring  $R$  is an element  $x \in R$  so that  $xy = 0$  for all  $y \in R$ . *right annihilators* are defined analogously. Usually annihilators are defined for subsets of  $R$ . For example,  $3$  is an annihilator for the subset  $\{0, 2, 4\}$  of  $\mathbb{Z}_6$  in the example above.

I also gave a very abstract example, the endomorphism ring of an additive group.

**Definition 18.10.** An **endomorphism** of an additive group  $A$  is defined to be a homomorphism  $\phi : A \rightarrow A$ . The **endomorphism ring**  $\text{End}(A)$  of  $A$  is the set of all endomorphisms of  $A$  with

- (1) Multiplication given by composition:  $\phi\psi := \phi \circ \psi$
- (2) Addition defined pointwise:  $(\phi + \psi)(a) = \phi(a) + \psi(a)$

**Theorem 18.11.** The endomorphism ring of  $A$  is a ring with unity.

### 18.1. homomorphisms.

**Definition 18.12.** A ring homomorphism is a mapping  $\phi : R \rightarrow S$  between two rings  $R$  and  $S$  so that

- (1)  $\phi$  is a homomorphism of additive group.

$$\phi(x + y) = \phi(x) + \phi(y) \quad \forall x, y \in R$$

- (2)  $\phi$  takes multiplication in  $R$  to multiplication in  $S$ :

$$\phi(xy) = \phi(x)\phi(y)$$

I will say  $\phi$  is multiplicative for short.

The kernel of  $\phi$  is defined to be

$$\ker \phi = \{x \in R \mid \phi(x) = 0\}$$

A ring homomorphism always takes 0 to 0. Why?

However, it might not take unity to unity. For example, take the mapping:

$$\phi : \mathbb{Z}_2 \rightarrow \mathbb{Z}_6$$

given by  $\phi(0) = 0$  and  $\phi(1) = 3$ . This is a homomorphism of additive groups since the order of 3 in  $\mathbb{Z}_6$  is 2. It is also multiplicative since  $3 \cdot 3 = 3$  in  $\mathbb{Z}_6$ . Thus 3 is **idempotent** in  $\mathbb{Z}_6$  (a solution of the equation  $x^2 = x$ ).

Show that, if  $R$  has unity and  $\phi : R \rightarrow S$  is a ring homomorphism, then  $\phi$  takes unity to an idempotent of  $S$ .

The kernel of  $\phi$  is an additive subgroup of  $R$ . Why?

**Definition 18.13.** An isomorphism of rings is a ring homomorphism  $\phi : R \rightarrow S$  which is also a bijection. Then  $R, S$  are said to be isomorphic as rings. Any property shared by isomorphic rings is called a structural property of the ring.

Which of the following are structural properties of rings?

- (1)  $R$  is commutative.
- (2)  $R$  is a ring with unity.
- (3)  $R$  has no zero divisors.
- (4)  $R$  is finite.

### 18.2. products.

**Definition 18.14.** The product of rings  $R_1, R_2, \dots, R_n$  is the Cartesian product of the underlying sets

$$\prod_{i=1}^n R_i = R_1 \times R_2 \times \cdots \times R_n$$

with addition and multiplication defined coordinate wise:

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$$

$$(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) = (a_1 b_1, a_2 b_2, \dots, a_n b_n)$$

The projection mapping  $p_j : \prod R_i \rightarrow R_j$  is a ring homomorphism for each  $j$ . Why is that?

**Example 18.15.**  $\mathbb{Z}_6$  is ring isomorphic to  $\mathbb{Z}_2 \times \mathbb{Z}_3$ . The isomorphism is given by  $\phi(n) = (n, n)$  where  $n$  is reduced modulo 2 in the first coordinate and reduced modulo 3 in the second coordinate.

When can you tell that a ring is a product?

One sign is that a product has many zero divisors since

$$(r, 0)(0, s) = (0, 0) \in R \times S$$

So, a ring without zero divisors cannot be a product of two smaller rings.

**18.3. integer multiplication.** If  $a$  is an element of a ring  $R$  and  $n$  is any integer then we can define

$$n \cdot a \in R$$

as follows. First  $0 \cdot a := 0$ . For  $n \geq 1$  the idea is:

$$n \cdot a = \underbrace{a + a + \dots + a}_{n \text{ times}}$$

However, the rigorous definition is:

$$(n + 1) \cdot a := n \cdot a + a$$

starting with  $n = 0$  which we already defined ( $0 \cdot a = 0$ ). For negative integers  $n = -k$ ,  $k > 0$  we define

$$(-k) \cdot a = -(k \cdot a)$$

This is the additive inverse of  $k \cdot a$ .

Problem: Show that, if  $\phi : R \rightarrow S$  is a ring homomorphism then

$$\phi(n \cdot a) = n \cdot \phi(a)$$

for all  $a \in R, n \in \mathbb{Z}$ .

**Definition 18.16.** The **characteristic** of a ring  $R$  is the smallest positive integer  $n$  so that  $n \cdot a = 0$  for all  $a \in R$ . If no such integer exists then the characteristic of  $R$  is defined to be 0.

For example,  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  all have characteristic zero and  $\mathbb{Z}_n$  has characteristic  $n$ . What is the characteristic of  $\mathbb{Z}_n \times \mathbb{Z}_m$ ?

**Lemma 18.17.**  $0a = 0$

*Proof.* Let  $x = 0a$ . We want to show that  $x = 0$ . We use distributivity:

$$x = 0a = (0 + 0)a = 0a + 0a = x + x$$

Subtract  $x$  from both sides to get  $x = 0$ . Why can we subtract  $x$ ?  $\square$

**Theorem 18.18.** *If  $R$  is a ring with unity then*

$$n \cdot a = (n \cdot 1)a$$

*Proof.* First take  $n \geq 0$ . We do induction.

$(n = 0)$   $0 \cdot a = 0$  is equal to  $(0 \cdot 1)a = 0a = 0$  (by the Lemma).

$(n + 1)$  Suppose we know that  $n \cdot a = (n \cdot 1)a$ . Then we want to know the same for  $n + 1$ :

$$(n + 1) \cdot a := n \cdot a + a = (n \cdot 1)a + a = (n \cdot 1 + 1)a = ((n + 1) \cdot 1)a$$

So the theorem holds for all  $n \geq 0$ .

Now suppose  $n$  is negative. So,  $n = -k$ ,  $k > 0$ . Then

$$(-k) \cdot a := -(k \cdot a) = -(k \cdot 1)a = (-k \cdot 1)a$$

by the second lemma which is below.  $\square$

**Lemma 18.19.**  $(-a)b = a(-b) = -ab$  for all  $a, b$  in any ring  $R$ .

*Proof.* By distributivity and the first lemma we have:

$$0 = 0b = (a + (-a))b = ab + (-a)b$$

So,  $(-a)b$  is the additive inverse of  $ab$ . The other identity  $a(-b) = -ab$  is similar.  $\square$

**Definition 18.20.** A **field** is a commutative ring with unity  $1 \neq 0$  in which every nonzero element is a unit. In particular,  $F$  has no zero divisors.

If  $F$  is a field then the nonzero elements form a multiplicative group  $F^\times$ . A nonexample is:  $\mathbb{Z}_{nm}$  is not a field for  $n, m \geq 2$  since  $n$  and  $m$  are zero divisors:  $(n)(m) = 0$  in  $\mathbb{Z}_{nm}$ .

**Theorem 18.21.** *The characteristic of a field  $F$  is either 0 or a prime number.*

**Lemma 18.22.** *If  $R$  is a ring with unity then the characteristic of  $R$  is the smallest positive integer  $n$  so that  $n \cdot 1 = 0$  (or  $\text{char } R = 0$  if no such  $n$  exists).*

*Proof of Theorem.* Suppose not. Then the characteristic of  $F$  is  $nm$  where  $n, m \geq 2$ . By the lemma,  $nm \cdot 1 = 0$  but  $a = n \cdot 1$  and  $b = m \cdot 1$  are nonzero. But,

$$ab = (n \cdot 1)b = n \cdot b = n \cdot (m \cdot 1)$$

$$= \underbrace{(1 + \cdots + 1)}_m + \cdots + \underbrace{(1 + \cdots + 1)}_m = nm \cdot 1 = 0$$

So,  $a, b$  are zero divisors. So,  $F$  is not a field.  $\square$

## 19. INTEGRAL DOMAINS

**Definition 19.1.** An **integral domain** (or **simply domain**) is defined to be a commutative ring with unity and no zero divisors.

For example,  $\mathbb{Z}$ ,  $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}, i = \sqrt{-1}\}$  are integral domains as is any subring of  $\mathbb{C}$ .

**Definition 19.2.** A **subring** of a ring  $R$  is a subset  $S \subseteq R$  so that

- (1)  $S$  is an additive subgroup of  $R$  (nonempty and closed under subtraction)
- (2)  $S$  is closed under multiplication in  $R$ .

Every field is an integral domain by definition and every subring of a field is an integral domain. For finite rings, the converse is true:

**Theorem 19.3.** Every finite integral domain is a field.

But first we need a lemma.

**Lemma 19.4.** Cancellation holds in a commutative ring iff it is an integral domain:

$$ax = ay, a \neq 0 \Rightarrow x = y$$

*Proof.* Suppose that  $R$  is a domain. Then  $ax = ay$  implies

$$0 = ax - ay = a(x - y) \Rightarrow a = 0 \text{ or } x - y = 0$$

Since  $a \neq 0$  we have  $x - y = 0$  or  $x = y$ . So, cancellation holds in a domain. Conversely suppose that cancellation does not hold. Then  $ax = ay$  for some  $a \neq 0$  and  $x \neq y$ . But then

$$a(x - y) = 0$$

shows that  $R$  is not an integral domain.  $\square$

*Proof of theorem.* Take any  $a \neq 0$  in a finite integral domain  $D$ . Then multiplication by  $a$  gives a mapping

$$f : D \rightarrow D, \quad f(x) = ax$$

which is 1-1 and therefore onto ( $D$  being finite). So,  $f(x) = ax = 1$  for some  $x \in D$  and  $x = a^{-1}$ .  $\square$

Here is chart with the definitions we have so far.

	commutative	noncommutative
no conditions	$2\mathbb{Z}$	
rings with unity	$\mathbb{Z}_{nm}, n, m \geq 2$	$M_n(\mathbb{R}), n \geq 2$
1 and no zero divisors	domains : $\mathbb{Z}, \mathbb{Z}[i]$	
1 and all nonzero are units	Fields : $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$	skew fields : $\mathbb{H}$

**Definition 19.5.** The ring of **quaternions**  $\mathbb{H}$  is defined to be  $\mathbb{R}^4$  with basis  $1, i, j, k$  and multiplication defined by:

$$\begin{array}{ll}
 i^2 = j^2 = k^2 = -1 & 1i = i1 = i, \text{ etc. (1 is unity)} \\
 ij = k & ji = -k \\
 jk = i & kj = -i \\
 ki = j & ik = -j
 \end{array}$$

Then extend linearly. For example:

$$(a + bi)(c + dj) = ac + bci + adj + bdk$$

**Theorem 19.6.**  $\mathbb{H}$  is a **skew-field** which means a noncommutative ring with unity in which every nonzero element is a unit.

*Proof.* The main point is that nonzero elements have inverses in the set:

$$(a + bi + cj + dk)^{-1} = \frac{1}{a^2 + b^2 + c^2 + d^2}(a - bi - cj - dk)$$

□

## 20. FERMAT AND EULER

Secure communication in the world today is based on Euler's formula and its generalizations. Euler's formula is in turn based on a formula of Fermat.

## 20.1. Fermat.

**Theorem 20.1** (Fermat's little theorem). *If  $p$  is prime and  $a$  is relatively prime to  $p$  ( $p$  does not divide  $a$ ) then*

$$a^{p-1} \equiv 1 \pmod{p}$$

The proof is based on Lagrange's Theorem which you need to know for the quiz. So, let's review that. Lagrange said that, if  $H$  is a subgroup of a finite group  $G$ , then the order of  $H$  divides the order of  $G$ . A corollary is that the order of any element of  $G$  divides the order of  $G$  since  $o(g) = |\langle g \rangle|$ . (The order of  $g$  is equal to the order of the subgroup of  $G$  generated by  $g$ .) This gave us the following formula which will be used to prove Fermat and Euler's formula.

**Lemma 20.2.** *If  $G$  is a group of order  $|G| = n$  then*

$$g^n = e$$

for all  $g \in G$ .

This is Corollary 10.7 in these notes. Do you remember the proof?

*Proof of Fermat's little theorem.* This congruence equation is the same as the actual equation

$$a^{p-1} = 1$$

for all  $a \neq 0$  in  $\mathbb{Z}_p$ . But  $\mathbb{Z}_p$  is a field. So,

$$\mathbb{Z}_p^\times = \{a \in \mathbb{Z}_p \mid a \neq 0\}$$

is a group of order  $p-1$ . So, the lemma above implies Fermat's formula.  $\square$

**Corollary 20.3.** *If  $p$  is prime then*

$$a^p \equiv a \pmod{p}$$

for all integers  $a$ .

*Proof.* If  $p$  divides  $a$  then both sides are congruent to 0 modulo  $p$ . If  $p$  doesn't divide  $a$  then this follows from Fermat.  $\square$

Application: We use this equation to test if a number is prime. There are very fast algorithms to compute  $a^n$  modulo  $p$  even if all three numbers have several hundred digits. The test is not foolproof but we do know that if

$$a^{n-1} \not\equiv 1 \pmod{n}$$

for some  $a$  then  $n$  is not prime.

**20.2. Euler.** Euler found a way to generalize Fermat's formula to all positive integers. He just needed the formula for the order of the group of units of  $\mathbb{Z}_n$ .

**Lemma 20.4.** *If  $R$  is any ring then the set of units of  $R$  is closed under multiplication and inverse and therefore forms a multiplicative group denoted  $U(R)$ .*

**Theorem 20.5.**  *$a$  is a unit in  $\mathbb{Z}_n$  if and only if  $a$  is relatively prime to  $n$ .*

*Proof.* This follows from the Euclidean Algorithm. (Do you remember that?) We used it to prove that the greatest common divisor  $d$  of two numbers  $a, b$  is an integer linear combination:

$$d = xa + yb$$

In this case,  $a$  and  $n$  are relatively prime so,  $d = 1$  and we get:

$$1 = xa + yn$$

But then  $xa \equiv 1 \pmod{n}$  or  $xa = 1 \in \mathbb{Z}_n$ . So,  $a$  is unit in  $\mathbb{Z}_n$ .

The converse is obvious. □

**Definition 20.6.** *The Euler  $\phi$  function is defined to be*

$$\phi(n) = |U(\mathbb{Z}_n)|$$

By the Lemma above which follows from Lagrange we have:

**Corollary 20.7.**

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

for all integers  $a$  which are relatively prime to  $n$ .

**Theorem 20.8.** *If  $n = \prod p_i^{k_i}$  then*

$$\phi(n) = \prod (p_i^{k_i} - p_i^{k_i-1}) = n \prod \frac{p_i - 1}{p_i}$$

For example, take  $n = 561 = 3 \cdot 11 \cdot 17$ . Then

$$\phi(561) = 2 \cdot 10 \cdot 16 = 240$$

Next: We need to prove the theorem and show that 561 is a *pseudo-prime*.

**20.3. Proof of Euler's formula.** I will prove Euler's formula 20.8 using groups and rings. As an application of the group theory behind the numerical formula we will see that 561 is a pseudoprime.

First, suppose that  $n$  is a power of a prime number  $p$ :

$$n = p^k$$

For example,  $n = 81 = 3^4$ . Then Theorem 20.5 says that the units of  $\mathbb{Z}_{p^k}$  are those numbers which are relatively prime to  $p^k$ . But this is the same as saying that they are not divisible by  $p$ . This is the complement of the subset

$$p\mathbb{Z}_{p^k} = \{0, p, 2p, 3p, \dots, p^k - p\}$$

In the example, this is

$$3\mathbb{Z}_{81} = \{0, 3, 6, 9, 12, \dots, 78\}$$

This is a subgroup of  $\mathbb{Z}_{p^k}$  of index  $p$ . So

$$|p\mathbb{Z}_{p^k}| = p^{k-1}$$

The elements left over are the units:

$$|U(\mathbb{Z}_{p^k})| = p^k - p^{k-1} = (p-1)p^{k-1} = \left(\frac{p-1}{p}\right) p^k$$

So, Euler's formula holds when  $n$  is a power of a prime.

Any positive integer  $n$  is a product of powers of distinct primes and we have two theorems.

**Theorem 20.9.** *If  $R, S$  are rings with unity 1 then  $(1, 1)$  is unity in  $R \times S$  and*

$$U(R \times S) = U(R) \times U(S)$$

*Note that  $R \times S$  is a product of rings and  $U(R) \times U(S)$  is a product of groups.*

This is an example of a theorem in which all of your knowledge and effort should be put into understanding what it says because the proof is completely trivial.

**Corollary 20.10.** *If  $R_1, \dots, R_n$  are rings with unity then*

$$U(R_1 \times R_2 \times \dots \times R_n) = U(R_1) \times U(R_2) \times \dots \times U(R_n)$$

The theorem says this is true for  $n = 2$ . For larger  $n$  it follows by induction in the standard way.

Next we need a theorem which we may have already proven:

**Theorem 20.11.** *If  $n, m$  are relatively prime then we have a ring isomorphism:*

$$\phi : \mathbb{Z}_{nm} \xrightarrow{\cong} \mathbb{Z}_n \times \mathbb{Z}_m$$

*Proof.* The ring homomorphism  $\phi$  is given by

$$\phi(x) = (x \pmod n, x \pmod m)$$

This is a ring homomorphism because  $n$  and  $m$  divide  $nm$ :

$$\phi(x +_{nm} y) = (x +_n y, x +_m y) = (x, x) + (y, y) = \phi(x) + \phi(y)$$

$$\phi(xy) = (xy, xy) = (x, x)(y, y) = \phi(x)\phi(y)$$

Let's look at just the first step:

$$x +_{nm} y \equiv x +_n y \pmod n$$

This is because both numbers are congruent to  $x + y$  modulo  $n$ .

To see that  $\phi$  is a bijection, use the Euclidean algorithm as I explained already twice.  $\square$

Instead of writing an arbitrary number, we will take

$$n = 360 = 8 \cdot 9 \cdot 5 = 2^3 \cdot 3^2 \cdot 5$$

Then we have an isomorphism of rings:

$$\mathbb{Z}_{360} = \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$

which gives an isomorphism of groups:

$$U(\mathbb{Z}_{360}) = U(\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5) = U(\mathbb{Z}_8) \times U(\mathbb{Z}_9) \times U(\mathbb{Z}_5)$$

Counting numbers of elements we get

$$\begin{aligned} \phi(2^3 \cdot 3^2 \cdot 5) = |U(\mathbb{Z}_{360})| &= |U(\mathbb{Z}_8)| \cdot |U(\mathbb{Z}_9)| \cdot |U(\mathbb{Z}_5)| = (8-4)(9-3)(5-1) \\ &= 360 \binom{2-1}{2} \binom{3-1}{3} \binom{5-1}{5} = 96 \end{aligned}$$

Although the group of units in  $\mathbb{Z}_{360}$  has order 96, we can conclude from the group formula that  $g^{12} = e$  for every  $g \in U(\mathbb{Z}_{360})$ . The reason is that

$$g = (a, b, c) \in U(\mathbb{Z}_8) \times U(\mathbb{Z}_9) \times U(\mathbb{Z}_5)$$

So,  $a^4 = e, b^6 = e, c^4 = e$ . (In fact  $a^2 = e$  since  $1^2 = 3^2 = 5^2 = 7^2 = 1$  in  $\mathbb{Z}_8$ .)

Do the same for  $n = 561 = 3 \cdot 11 \cdot 17$  and show that:

$$a^{560} \cong 1 \pmod{561}$$

for all integers  $a$  relatively prime to 561.

**Definition 20.12.** A positive integer  $n$  is called a pseudoprime or Carmichael number if it has the property that  $a^{n-1} \cong 1 \pmod n$  for all integers  $a$  relatively prime to  $n$ .

There are an infinite number of pseudoprimes and the smallest one is 561.

**What is next?**

After the quiz, we have three more topics which I want to cover to complete the circle of ideas.

- (1) Finite fields (also called *Galois fields*). The main results are:
  - (a) The number of elements in a finite field is a power of a prime:  $|GF| = p^k$ . And conversely, for any power of any prime, there is a unique Galois field with this number of elements. Usually we use  $GF(2^8)$ .
  - (b) The group of units is a cyclic group of order  $p^k - 1$ .  
We need polynomial rings (sections 22,23) to understand the structure of finite fields (section 33).
- (2) Finite simple groups of “Lie type” are constructed out of the finite fields. These account for most of the finite simple groups.
- (3) Extensions All finite groups are iterated extensions of simple groups. I will explain some of this very rich theory if I have time.

## 33. FINITE FIELDS

We will discuss the basic theoretical properties of finite fields, prove most of these properties and use them to deduce the precise structure of finite fields and to construct some of the classical finite simple groups.

The two basic properties of finite fields are the following. The first concerns the number of elements in a finite field.

- Theorem 33.1.** (1) *The number of elements of any finite field is a power of a prime number:  $|F| = p^k$ .*  
 (2) *Every power of every prime is the order of some finite field.*  
 (3) *Two finite fields with the same order are isomorphic.*

We will prove (1) using group theory.

This theorem tells us that there is a unique finite field for any power of any prime (up to isomorphism). This field is called the **Galois fields**  $GF(q)$  where  $q = p^k$ . Today, we will deduce the exact structure of  $GF(16)$  from the general theory.

The second main property of finite fields is Fermat's little theorem in the case of  $GF(p) = \mathbb{Z}_p$ .

- Theorem 33.2.** *The group of units of any finite field of order  $q$  is a cyclic group of order  $q - 1$ .*

We will prove this using polynomials with coefficients in the field  $F$ .

Problem: Using this theorem show that  $GF(9)$  is not a subfield of  $GF(27)$ .

**33.1. order of a field.** I will explain the proof and the consequences of Theorem 33.1

Recall that the *characteristic* of a field is either prime or 0. A finite field  $F$  cannot have characteristic 0 so it has prime characteristic  $p$ . This means that

$$p \cdot x = \underbrace{x + x + \cdots + x}_p = 0$$

for every  $x \in F$ . In other words, every element of the additive group  $(F, +)$  has order  $p$  (except for 0 which has order 1).

**Lemma 33.3.** *Suppose that  $G$  is a finite abelian group in which every nontrivial element has order  $p$  where  $p$  is a fixed prime. Then the order of  $G$  is a power of a prime.*

This is a simple induction on the order of  $G$  using the factor group

$$G/\langle g \rangle$$

for any nontrivial element  $g \in G$ .

*Proof.* The proof is by induction on  $n = |G|$ . Suppose that  $|G| = n = 1$ . Then  $1 = p^0$  is a power of  $p$  so the theorem holds.

Now suppose that  $n > 1$  and the theorem holds for all groups with fewer than  $n$  elements. Take  $g \neq e$  in  $G$ . Then by assumption we have  $o(g) = \langle g \rangle = p$ . Since  $G$  is abelian, every subgroup is normal. So, we have a factor group  $G/\langle g \rangle$  with order

$$|G/\langle g \rangle| = \frac{n}{p}$$

Claim Every nontrivial element of the factor group has order  $p$ .

Proof of Claim: Any element of the factor group has the form  $hN = h\langle g \rangle$ . So,

$$(h\langle g \rangle)^p = h^p \langle g \rangle = e \langle g \rangle = \langle g \rangle$$

which is the identity of  $G/\langle g \rangle$ . Since  $g^n = e$  implies that  $o(g)|n$ , the calculation above implies that  $o(h\langle g \rangle)$  is either  $p$  or 1. So, every nontrivial element of  $G/\langle g \rangle$  has order  $p$ .

Getting back to the proof of the lemma,

$$|G/\langle g \rangle| = \frac{n}{p} = p^k \Rightarrow n = p^{k+1}$$

So, the lemma holds for  $G$  and we are done.  $\square$

**33.2. example:  $GF(16)$ .** I will prove Theorem 33.2 next time. Today, I used it to construct  $F = GF(16)$ . Since  $16 = 2^4$ , we have  $p = 2$ . This implies that  $x + x = 0$  for all  $x \in F$ . In other words,  $x = -x$ .

The theorem says that  $GF(16)^\times = \langle x \rangle$  where  $x$  has multiplicative order 15:  $x^{15} = 1$ . Let  $\alpha = x^3$ . Then  $\alpha^5 = 1$ . Now, we represent elements of  $F$  as binary sequences with 4 binary digits. For example:

$$1010 = \alpha^3 + \alpha^2$$

This is *base*  $\alpha$ . If we have more than 4 digits, we can contract using the formula:

**Lemma 33.4.**

$$\boxed{\alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1}$$

*Proof.* We put everything on one side of the equation and multiply by  $\alpha - 1 = \alpha + 1$ :

$$(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1)(\alpha - 1) = \alpha^5 - 1 = 0$$

This is a product of two elements of the field  $F$ . But  $\alpha - 1 \neq 0$  since  $\alpha = x^3$  and  $x$  has order 15. Therefore, the other factor must be zero since  $F$  has no zero divisors:

$$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$$

This implies that

$$\alpha^3 + \alpha^2 + \alpha + 1 = -\alpha^4 = +\alpha^4$$

since  $+$  and  $-$  are the same thing in characteristic 2.  $\square$

Addition and multiplication of 4 digit sequences works like this:

$$\begin{array}{r} 1\ 0\ 1\ 0 \\ +\ 0\ 1\ 1\ 1 \\ \hline 1\ 1\ 0\ 1 \end{array}$$

The rule is: we add digits without carrying. These digits represent:

$$\begin{array}{r} \alpha^3 \qquad \qquad +\alpha \\ + \qquad \alpha^2 \quad +\alpha \quad +1 \\ = \alpha^3 \quad +\alpha^2 \qquad \quad +1 \end{array}$$

since  $\alpha + \alpha = 0$ .

Multiplication uses the boxed formula:

$$\begin{array}{r|l} & 1\ 0\ 1\ 0 \\ \times & 0\ 1\ 1\ 1 \\ \hline & 1\ 0\ 1\ 0 \\ 1 & 0\ 1\ 0 \\ 1\ 0 & 1\ 0 \\ \hline \alpha^4 & 1\ 1\ 1\ 1 \\ \alpha^5 & 0\ 0\ 0\ 1 \\ \hline & 1\ 0\ 0\ 0 \end{array}$$

Any digit beyond the first four can be shifted to the right since

$$1,0000 = \alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1 = 1111$$

$$10,0000 = \alpha^5 = 1 = 0001$$

$$100,0000 = \alpha^6 = \alpha = 0010$$

Problem: Show that  $1010^3 = 0010 = \alpha$  and  $1010$  has order 15.

**33.3. units and polynomials.** In both theory and practice it is important to use polynomials to work with finite fields. In the example of  $GF(16)$  each element is written as a sequence of 4 binary digits:

$$c_3c_2c_1c_0$$

where  $c_0, c_1, c_2, c_3$  are elements of  $GF(2) = \mathbb{Z}_2 = \{0, 1\}$ . But this notation represents the polynomial:

$$p(\alpha) = c_3\alpha^3 + c_2\alpha^2 + c_1\alpha + c_0$$

I will explain the bare minimum of the theory of polynomials with coefficients in an arbitrary field so that we can use this idea to handle arbitrary finite fields.

**Definition 33.5.** *Suppose that  $F$  is any field. Then a polynomial with coefficients in  $F$  is a formal expression:*

$$f(X) = c_nX^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$$

where each  $c_i$  is an element of  $F$  and  $c_n \neq 0$  ( $c_n$  is called the **leading coefficient** of  $f(X)$  and  $n$  is called the **degree** of the polynomial  $f(X)$ ). Addition and multiplication of polynomials is given in the usual way keeping in mind that the coefficients are elements of  $F$ . The set of all such polynomials is denoted  $F[X]$  and is called the **polynomial ring** in the variable  $X$  with coefficients in  $F$ .

It is very important that square brackets are used in the notation because  $F(X)$  means something else.

Here is an example to remind you how polynomials are added and multiplied. Take  $F = \mathbb{Z}_3$

$$(X^2 + 2X + 1) + (2X^2 + 2X) = (1 + 2)X^2 + (2 + 2)X + 1 = X + 1$$

$$(X - 1)^3 = (X + 2)^3 = X^3 + 6X^2 + 12X + 8 = X^3 + 2$$

Note that we can eliminate any minus signs since, e.g.,  $-1 = 2$  in  $\mathbb{Z}_3$ .

Problem: Show that  $F[X]$  is an integral domain (commutative with unity and no zero divisors). Hint: The leading coefficient of  $f(X)g(X)$  is the product of the leading coefficients of  $f(X)$  and of  $g(X)$ .

Problem: Show that  $F[X]$  has the same characteristic as  $F$ .

**Definition 33.6.** *A polynomial  $f(X)$  is called **monic** if its leading coefficient is 1.*

The reason that monic polynomials are important is because we can divide by them. Here is an example and a theorem which I feel is so obvious that it hardly requires proof.



If we insert any  $\beta_i$  for  $X$  we get:

$$f(\beta_i) = 0 = (\beta_i - \alpha)q(\beta_i)$$

Since  $\beta_i \neq \alpha$  we must have

$$q(\beta_i) = 0$$

But this makes  $q(X)$  into a polynomial of degree  $n - 1$  with  $n$  different roots which is not possible by the induction hypothesis. This proves the corollary.  $\square$

**Theorem 33.10.** *If  $F$  is a finite field of order  $q$  then  $F^\times$  is a cyclic group of order  $q - 1$ .*

In lieu of a proof, I will explain why this is true using two examples. Take  $q = 9$ . Then  $F^\times$  has 8 elements. So, every element has order a power of 2 (since  $o(g)$  divides  $|G|$  for any  $g \in G$ ). If  $F^\times$  is not cyclic then its elements all have order 2 or 4. This means that the polynomial

$$X^4 - 1$$

has 8 different roots which is impossible by the corollary we just proved.

Next, take  $q = 25$ . Then  $F^\times$  has  $24 = 3 \cdot 8$  elements. If the orders of the elements divide 12 then the polynomial  $X^{12} - 1$  has 24 roots which is impossible. So,  $F^\times$  has an element  $x$  of order 24 or an element  $\alpha$  of order 8 (these are the only two divisors of 24 which do not divide 12). But then  $\alpha = x^3$  has order 8. So, in both cases we get an element  $\alpha$  of order 8. Similarly,  $F^\times$  has an element  $\beta$  of order 3.

Claim: The product  $\alpha\beta$  has order 24 and therefore  $F^\times$  is cyclic.

To prove this suppose that  $o(\alpha\beta) = n$ . Then

$$(\alpha\beta)^n = \alpha^n\beta^n = 1$$

which implies that  $\beta^n = \alpha^{-n}$ . Cubing both gives  $\beta^{3n} = \alpha^{-3n} = 1$  which implies the order of  $\beta$  divides  $3n$ . So:

$$8|3n \Rightarrow 8|n$$

Also  $\alpha^{-8n} = \beta^{8n} = 1$  which implies the order of  $\alpha$  divides  $8n$ . So

$$3|8n \Rightarrow 3|n \Rightarrow 24|n$$

So,  $\alpha\beta$  has order 24.

Other cases are similar. But I won't go through the proof. It uses the following lemma which was illustrated in the second example we just did.

**Lemma 33.11.** *If  $G$  is an abelian group and  $\alpha, \beta \in G$  have order  $n, m$  which are relatively prime then  $\alpha\beta$  has order  $nm$ .*

## 34. FINITE SIMPLE GROUPS

Classification of finite simple groups: There are 18 infinite families of simple groups and 26 “sporadic” groups. Of all of these groups you know:

- (1) The cyclic groups  $\mathbb{Z}_p$  are simple when  $p$  is prime.
- (2) The alternating groups  $A_n$  are simple if  $n \geq 5$ .

The other 16 infinite families come from finite fields. The easiest to describe are the *projective unimodular groups*  $PSL(n, q)$ . Today, I will tell you what these groups are and what are their basic properties.

**34.1. Matrices over finite fields.** We take  $n \times n$  matrices with coefficients in the finite field  $GF(q)$ . They look like this:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a, b, c, d \in GF(q)$$

Question: How many  $2 \times 2$  matrices are there with coefficients in  $GF(q)$ ?

Matrices are added and multiplied in the usual way, keeping in mind that the entries lie in the field  $F = GF(q)$ . For example, if  $q = 3$  we get:

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}$$

The matrices on the left are called **elementary matrices** and they are denoted  $E_{12}(2)$  and  $E_{21}(2)$ . The notation is:  $E_{ij}(a)$  (with  $i \neq j$ ) is the identity matrix with  $(i, j)$  entry changed to  $a$ . For example:

$$E_{31}(a) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & 0 & 1 \end{pmatrix}$$

Recall from linear algebra: Left multiplication by  $E_{ij}(a)$  performs a row operation on a matrix and right multiplication by  $E_{ij}(a)$  performs a column operation. In the above example,  $XE_{21}(2)$  is the matrix  $X$  with twice the second column added to the first column.

Elementary matrices have determinant equal to 1. Therefore, any product of elementary matrices has determinant 1. For example:

$$\det \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix} = 2 - 4 = -2 = 1 \quad \in \mathbb{Z}_3 = GF(3)$$

**Definition 34.1.** If  $F$  is any field, let  $GL(n, F)$  denote the group of all  $n \times n$  invertible matrices with coefficients in the field  $F$ . This is the same as the set of all  $n \times n$  matrices (with coefficients in  $F$ ) whose

determinant is nonzero. Let  $SL(n, F)$  denote the subgroup of  $GL(n, F)$  consisting of matrices of determinant 1.

**Theorem 34.2.**  $SL(n, F)$  is a normal subgroup of  $GL(n, F)$ .

*Proof.*  $SL(n, F)$  is by definition the kernel of the homomorphism

$$\det : GL(n, F) \rightarrow F^\times$$

Therefore,  $SL(n, F) \trianglelefteq GL(n, F)$ . □

**Notation**  $GL(n, q) := GL(n, GF(q))$  and  $SL(n, q) := SL(n, GF(q))$ .

**34.2. orders of matrix groups.** Question: What is the order of the group  $GL(2, q)$ ?

**Theorem 34.3.**

$$|GL(2, q)| = (q^2 - 1)(q^2 - q)$$

*Proof.* There are a total of  $q^4$  matrices (of size  $2 \times 2$ )

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

since there are  $q$  possibilities for each of the entries  $a, b, c, d$ . We need to know how many of these satisfy the equation:

$$ad - bc \neq 0$$

The first obvious point is that  $a, c$  cannot both be zero. So, there are  $q^2 - 1$  possibilities for  $a, c$ .

Claim Once you choose  $a$  and  $c$  there are exactly  $q^2 - q$  choices for  $b$  and  $d$ . (In other words, there are exactly  $q$  choices which don't work.)

The ones that won't work are the multiples of  $\begin{pmatrix} a \\ c \end{pmatrix}$ :

$$\det \begin{pmatrix} a & ax \\ c & cx \end{pmatrix} = acx - cax = 0$$

Any other choice of  $b, d$  will give an invertible matrix. This is because, if the second column is not a multiple of the first then then we can do an elementary operation to make one of the entries in the second column zero. For example:

$$AE_{12}(-a^{-1}b) = \begin{pmatrix} a & 0 \\ c & d - ca^{-1}b \end{pmatrix}$$

has determinant

$$a(d - ca^{-1}b) \neq 0$$

□

**Corollary 34.4.**

$$|SL(2, q)| = (q^2 - 1)q = q^3 - q$$

*Proof.* This follows from the isomorphism theorem which says that for any homomorphism  $\phi : G \rightarrow H$ ,  $G/\ker \phi \cong im\phi$ . In this case the homomorphism is  $\det : GL(n, q) \rightarrow F^\times$  with kernel  $SL(n, q)$  which gives:

$$\frac{GL(n, q)}{SL(n, q)} \cong GF(q)^\times$$

So,

$$|SL(2, q)| = \frac{|GL(2, q)|}{|GF(q)^\times|} = \frac{(q^2 - 1)(q^2 - q)}{q - 1} = (q^2 - 1)q$$

□

**34.3. centers of  $GL$  and  $SL$ .** The center of  $GL(n, F)$  is the group of all diagonal matrices with the same entry repeated along the diagonal. For example:

$$Z = Z(GL(3, F)) = \left\{ \begin{pmatrix} x & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{pmatrix} : x \neq 0 \in F \right\}$$

If  $F = GF(q)$  then, no matter what  $n$  is we get

$$|Z| = q - 1$$

Question: What is the intersection:  $Z \cap SL(n, q)$ ?

We will discuss this next time.

**Definition 34.5.**

$$PSL(n, q) := \frac{SL(n, q)}{Z \cap SL(n, q)}$$

This is called the **projective unimodular group**

**Theorem 34.6.**  $PSL(n, q)$  is simple except in the two cases  $PSL(2, 2)$  and  $PSL(2, 3)$ .