

# ALGEBRA - LECTURE I

## 1. INTRODUCTION

This semester we shall cover the following topics:

- Finite Fields, Group actions and Sylow Theorems,  $\mathbb{Z}$ -modules, Rings (Euclidean, PID), Modules, Projective Modules, Bilinear Forms, Tensor Products, Witt Group, Fields, Galois Theory,

Primary sources of material will be my web page.

## 2. FUNDAMENTAL THEOREM OF ARITHMETIC

Recall that dividing two positive integers  $a, b$  means finding a positive integer  $q$ , called a quotient, such that

$$a = qb + r$$

with  $0 \leq r < b$ . The number  $r$  is called a remainder. If  $r = 0$  then we say that  $b$  divides  $a$ , and write  $b|a$ . For example,

$$3 \mid 6 \text{ whereas } 4 \nmid 6.$$

Dividing two integers is probably the most difficult of the four standard binary operations. However, some of the most fundamental properties, such as the uniqueness of factorization, are based on the Euclidean Algorithm.

Recall that the *Greatest Common Divisor* of two integers  $m$  and  $n$  is the greatest integer  $d$  dividing both  $m$  and  $n$ . We write  $d = GCD(n, m)$ . For example, after factoring  $22 = 2 \cdot 11$  and  $60 = 3 \cdot 2^2 \cdot 5$ , one can easily see that

$$GCD(60, 22) = 2.$$

There are two issues here, however. First, we have secretly assumed the uniqueness of factorization. The second issue, also very important, is that factoring primes is a very difficult process, in general. A better way to find a *GCD* is based on the Euclidean Algorithm. More precisely, we will use the division algorithm to generate a sequence of numbers ( $b > r_1 > r_2 > \dots$ ) as follows. First, we divide  $a$  by  $b$ :

$$a = q_1b + r_1,$$

then divide  $b$  by  $r_1$ , and so on...

$$\begin{aligned} b &= q_2r_1 + r_2 \\ r_1 &= q_3r_2 + r_3 \\ &\vdots \\ &1 \end{aligned}$$

This process stops when the remainder is 0. Since  $b > r_1 > r_2 \dots$  it stops in less than  $b$  steps. We claim that the last non-zero remainder  $r_n$  is the gcd of  $a$  and  $b$ . Assume, for simplicity, that the last non-zero remainder is  $r_4$ . Then the last equation above is

$$r_3 = q_5 r_4 + 0.$$

We claim that  $r_4$  is precisely  $GCD(a, b)$ . Put  $d = GCD(a, b)$ . To show that  $d = r_4$  we need to check that

$$r_4 \mid a, b$$

which shows that  $r_4$  is a common divisor (thus  $r_4 \leq d$ ) and

$$d \mid r_4$$

which implies that  $d \leq r_4$ .

To check that  $r_4$  divides  $a$  and  $b$  we work up from the last equation  $r_3 = q_5 r_4$  which shows that  $r_4$  divides  $r_3$ . Then the next equation  $r_2 = q_4 r_3 + r_4$  shows that  $r_4$  divides  $r_2$  as well. Continuing in this fashion, we arrive to

$$r_4 \mid r_2, r_4 \mid r_1, r_4 \mid b, \text{ and } r_4 \mid a.$$

To check that  $d \mid r_4$  we work from the top to the bottom. The first equation  $a = qb + r_1$  shows that  $d$  divides  $r_1$ . The second equation  $b = q_2 r_1 + r_2$  shows that  $d$  divides  $r_2$ , and so on. We get

$$d \mid r_2, d \mid r_3, \text{ and } r_4,$$

which completes the proof.

**Theorem 1.** (*Fundamental Theorem of Arithmetic*) *If  $a, b$  are two positive integers, then there exist integers  $x, y$  such that  $ax + by = GCD(a, b)$*

*Proof.* We shall use the Euclidean Algorithm to construct a solution. Assume that  $r_3$  is the last non-zero remainder. (So  $GCD(a, b) = r_3$ .) Then

$$\begin{aligned} a &= q_1 b + r_2 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3. \end{aligned}$$

We can consider this as a system of three linear equations in five variables :  $a, b, r_1, r_2$  and  $r_3$ . We shall reduce this system to one equation in three variables  $a, b$  and  $r_3$  as follows. First, rewrite the system as

$$\begin{aligned} r_1 &= a - q_1 b \\ r_2 &= b - q_2 r_1 \\ r_3 &= r_1 - q_3 r_2. \end{aligned}$$

Next, eliminate  $r_2$  and  $r_1$  using the second and the first equation, respectively. More precisely, first substitute  $r_2 = b - q_2 r_1$  into the last equation, which then becomes

$$r_3 = -q_3 b + (1 + q_2 q_3) r_1.$$

Next, substitute  $r_1 = a - q_1 b$  to obtain

$$r_4 = (1 + q_2 q_3) a - (q_1 + q_1 q_2 q_3 + q_3) b.$$

Since  $d = r_4$ , we see that  $(x, y) = (1 + q_2 q_3, -q_1 - q_1 q_2 q_3 - q_3)$  is a solution of the equation.  $\square$

For example, if  $a = 123$  and  $b = 36$ , then the Euclidean Algorithm gives a sequence of equations

$$\begin{aligned} a &= 3 \cdot b + 15 \\ 36 &= 2 \cdot 15 + 6 \\ 15 &= 2 \cdot 6 + 3 \\ 6 &= 2 \cdot \boxed{3} + 0. \end{aligned}$$

In particular,  $GCD(123, 36) = 3$  We now rewrite as before ...

$$\begin{aligned} 15 &= a - 3 \cdot b \\ 6 &= b - 2 \cdot 15 \\ 3 &= 15 - 2 \cdot 6 \end{aligned}$$

After two substitutions the last equation becomes  $3 = 5a - 17b$  from which we identify a solution:

$$(x, y) = (5, -17).$$

### 3. THE FINITE FIELD $\mathbb{F}_p$

In modular arithmetic we identify two integers  $a$  and  $b$  if the difference  $a - b$  is divisible by  $n$ . This is classically denoted by

$$a \equiv b \pmod{n}.$$

and say that  $a$  is congruent to  $b$  modulo  $n$ . For example, if  $n = 5$ , then 6 is congruent to 1 modulo 5. If there is no fear of confusion, we will simply write  $6 = 1$ . Integers can be added and multiplied modulo  $n$ . For example,  $3 + 4 = 7$ , as integers, but  $7 \equiv 2 \pmod{5}$ , so

$$3 + 4 \equiv 2 \pmod{5}$$

or simply  $3 + 4 = 2$ . The modular arithmetic is associative, 0 is a neutral element, and inverse of  $a$  is  $-a$ , just as for integers. The set of integers modulo  $n$  is denoted by  $\mathbb{Z}/n\mathbb{Z}$ . Its elements are represented by the set

$$\{0, 1, \dots, n - 1\}.$$

Situation with modular multiplication is more delicate. It is also associative, and 1 is a neutral element, but what about the inverse? Integers, except  $-1$  and 1, do not have inverse with respect to multiplication. Consider, for example, the multiplication table modulo 5:

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Remarkably, every non-zero number modulo 5 has a multiplicative inverse. In particular,  $(\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\}$  is a group with respect to multiplication. This is not an accident, since we have the following general statement:

**Proposition 2.** *Let  $p$  be a prime. Then  $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, 3, \dots, p-1\}$  is a group for modular multiplication.*

*Proof.* Let  $1 \leq a \leq p-1$ . In order to show that  $a$  has an inverse, we must find an integer  $x$  such that  $ax \equiv 1 \pmod{p}$ . Since  $p$  is prime, and it does not divide  $a$ . Since  $p$  is a prime and  $a < p$  it follows that  $\text{GCD}(a, p) = 1$ . Thus, there exist two integers  $x$  and  $y$  such that

$$ax + py = 1$$

which, clearly, implies that  $ax \equiv 1 \pmod{p}$ , as desired.  $\square$

Summarizing, we have just shown that  $\mathbb{Z}/p\mathbb{Z}$  is a field for every prime  $p$ . This field is also denoted by  $\mathbb{F}_p$ .

#### 4. FIELD CHARACTERISTIC AND FROBENIUS

Let  $F$  be a field. It is a set with two operations  $+$  (addition) and  $\cdot$  (multiplication) which satisfy the set of axioms given in the previous lecture. In particular, the field  $F$  has at least two elements 0 and 1. Every integer  $n$  can be identified with an element  $\underline{n}$  of  $F$  as follows. If  $n$  is positive, we define

$$\underline{n} = \underbrace{1 + \dots + 1}_{n\text{-times}}.$$

Using the distributive property, it follows that the numbers  $\underline{n}$  and  $\underline{m}$  multiply by the formula

$$\underline{n} \cdot \underline{m} = \underbrace{(1 + \dots + 1)}_{n\text{-times}} \underbrace{(1 + \dots + 1)}_{m\text{-times}} = \underbrace{1 + \dots + 1}_{nm\text{-times}} = \underline{nm}.$$

In particular, it is safe to write  $n$  instead of  $\underline{n}$ , and we shall do so when it causes no confusion.

We have now two possibilities. Either  $\underline{n} \neq 0$  for every positive integer  $n$ , or there exists a positive integer  $n$  such that  $\underline{n} = 0$  in  $F$ . In the first case we say that the field  $F$  has *characteristic 0*. Examples of such fields are  $\mathbb{Q}$ ,  $\mathbb{R}$  and  $\mathbb{C}$ . In the second case we say that the field  $F$  has a positive characteristic or, more precisely, *characteristic  $p$*  where  $p$  is the smallest positive integer such that  $\underline{p} = 0$ . If  $p$  is a prime, then the finite field  $\mathbb{Z}/p\mathbb{Z}$  has the characteristic  $p$ . We have the following important observation:

*The field characteristic is either 0 or a positive prime number  $p$ .*

This is really easy. Indeed, if  $p = mn$  then

$$0 = \underline{p} = \underline{n} \cdot \underline{m}.$$

Since a field does not have zero divisors we must have either  $\underline{n} = 0$  or  $\underline{m} = 0$  in  $F$ . Since  $p$  is the smallest integer such that  $\underline{p} = 0$  in  $F$  we must have either  $n = p$  or  $m = p$ . This shows that  $p$  is prime as claimed.

Another important observation of this discussion is that if the characteristic of the field  $F$  is 0, then the ring of integers  $\mathbb{Z}$  can be viewed as a subring of  $F$ . If the characteristic of  $F$  is  $p$  then  $F$  contains  $\mathbb{Z}/p\mathbb{Z}$  as a sub-field.

**Proposition 3.** *(5-th grader's dream) Let  $F$  be a field of characteristic  $p$ . Then for any two elements  $a$  and  $b$  in  $F$  we have*

$$(a + b)^p = a^p + b^p.$$

*Proof.* The  $p$ -th power of  $a + b$  can be expressed in terms of binomial coefficients:

$$(a + b)^p = a^p + \binom{p}{1} a^{p-1}b + \binom{p}{2} a^{p-2}b^2 + \cdots + \binom{p}{p-1} ab^{p-1} + b^p.$$

The binomial coefficients are computed using the Pascal triangle. In the characteristic  $p$ , the coefficients are computed modulo  $p$ . For example, if  $p = 7$ , then the first eight rows of the Pascal triangle calculated modulo 7 are.

$$\begin{array}{cccccccc}
 & & & & & & & 1 \\
 & & & & & & 1 & 1 \\
 & & & & 1 & 2 & 1 & \\
 & & 1 & 3 & 3 & 1 & & \\
 & 1 & 4 & 6 & 4 & 1 & & \\
 1 & 1 & 5 & 3 & 3 & 5 & 1 & \\
 & 1 & 6 & 1 & 6 & 1 & 6 & 1 \\
 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1
 \end{array}$$

Here the first 5 rows coincide with the usual Pascal triangle. The first difference appears in the sixth row, where instead of 10 (twice) we have  $3 \equiv 10 \pmod{7}$ . The vanishing of coefficients modulo 7 in the 8-th row or, more generally, vanishing of coefficients modulo  $p$  in the  $p + 1$ -st row can be easily explained. Recall that the binomial coefficients are *integers* and given by the following formula:

$$\binom{p}{k} = \frac{p!}{n!(p-n)!}.$$

Since  $p$  is prime, both factors in the denominator do not contain  $p$  as a factor, as they are products of numbers less than  $p$ . On the other hand, the numerator is divisible by  $p$ . Thus, the quotient of the numerator and the denominator is still divisible by  $p$ . It follows that the binomial coefficients are 0, when considered as elements of the field  $F$ . This completes the proof.  $\square$

The above proposition shows that the map  $\text{Fr}(x) = x^p$ , also called the Frobenius, is a rather interesting mapping, since

$$\text{Fr}(ab) = \text{Fr}(a) \cdot \text{Fr}(b)$$

and

$$\text{Fr}(x + y) = \text{Fr}(x) + \text{Fr}(y)$$

which implies that  $\text{Fr}$  is a homomorphism for both group structures at the same time. In this sense it is similar to the complex conjugation. But that is not all. We also have the following:

**Proposition 4.** *Let  $F$  be a field of characteristic  $p$ . Let  $x$  be an element in  $F$ . Then  $\text{Fr}(x) = x$  if and only if  $x$  is in the subfield  $\mathbb{Z}/p\mathbb{Z}$  of  $F$ .*

*Proof.* The equation  $\text{Fr}(x) = x$  can be written as

$$x^p - x = 0.$$

Thus, an element of the field  $F$  satisfies  $\text{Fr}(x) = x$  if and only if it is a root of the polynomial  $x^p - x$ . By the Little Fermat Theorem, all elements of  $\mathbb{F}_p$  are roots of this polynomial. In this way we have already accounted for  $p$  roots of  $x^p - x$ . Since, over any field, a polynomial of degree  $p$  cannot have more than  $p$  roots, the elements of  $\mathbb{F}_p$  are precisely all roots of  $x^p - x$ .  $\square$

We shall now construct some additional examples of finite fields. Complex numbers  $z = x + iy$  such that  $x$  and  $y$  are integers are called Gauss's integers. Here, of course,  $i^2 = -1$ . Gauss's integers also admit modular arithmetic. If  $n$  is a positive integer, two Gauss's integers are said to be congruent modulo  $n$

$$a + bi \equiv c + di \pmod{n}$$

if  $a \equiv c \pmod{n}$  and  $b \equiv d \pmod{n}$ . Addition and multiplication are performed just as with the complex numbers, except the coefficients  $x$  and  $y$  are always considered modulo  $n$ . For example, if  $n = 11$  then

$$(2 + 5i)(5 + 4i) = -10 + 33i \equiv 1 + 0i = 1 \pmod{11}.$$

If  $p$  is an odd prime such that  $-1$  is not a square (for example  $p = 3$ ) then the set of Gauss's integers modulo  $p$  is a finite field of characteristic  $p$ . The reason for this is simple. In order to compute the inverse of  $a + ib \neq 0$ , we need to find  $x + iy$  such that  $(a + bi)(x + iy) = 1$ . This leads us to a  $2 \times 2$ -system of equations (in unknowns  $x$  and  $y$ )

$$\begin{aligned} ax - by &= 1 \\ bx + ay &= 0 \end{aligned}$$

with determinant  $a^2 + b^2$ . We can solve this system as long as  $a^2 + b^2 \not\equiv 0 \pmod{p}$ . If  $a^2 + b^2 \equiv 0 \pmod{p}$  then

$$\left(\frac{a}{b}\right)^2 \equiv -1 \pmod{p},$$

a contradiction if  $-1$  is not a square modulo  $p$ . This argument works if  $b \neq 0$ . A similar argument works if  $a \neq 0$ . Since  $a + ib \neq 0$  one of the two must hold. In any case, assuming that  $-1$  is not a square modulo  $p$ , we have shown that the set of Gauss's integers modulo  $p$  is a field. This field is usually denoted by  $\mathbb{F}_{p^2}$ . Since  $x$  and  $y$  are integers modulo  $p$ , there are  $p$  choices for both,  $x$  and  $y$ . In all, we have  $p^2$  elements in  $\mathbb{F}_{p^2}$ .

But when is  $-1$  a square modulo an odd prime  $p$ ? This is answered by the first part of Gauss's quadratic reciprocity:  $-1$  is a square modulo  $p$  if and only  $p \equiv 1 \pmod{4}$ . One direction of this statement is easy: If  $-1$  is a square, then there is an element of order 4 in the group  $(\mathbb{Z}/p\mathbb{Z})^\times$ . It follows that 4 divides  $p - 1$  (or  $p \equiv 1 \pmod{4}$ ) by the theorem of Lagrange. In order to prove the converse statement we need to use the Frobenius map. If  $a + bi$  is a Gauss's integer then, modulo  $p$ , we have

$$(a + bi)^p \equiv a^p + b^p i^p \pmod{p}.$$

By Fermat's Little Theorem  $a^p \equiv a \pmod{p}$  and  $b^p \equiv b \pmod{p}$ . If  $p \equiv 1 \pmod{4}$ , we can write  $p = 4k + 1$ . Thus,

$$i^p = i^{4k+1} = i^{4k} \cdot i = i$$

since  $i^4 = 1$ . Putting things together,

$$(a + bi)^p \equiv a + bi \pmod{p}.$$

In words, every Gauss's integer modulo  $p$  is a root of the polynomial  $x^p - x$ . Thus we have a situation where there are  $p^2$  solutions of a polynomial of degree  $p$ . It follows that set of Gauss's integers modulo  $p \equiv 1 \pmod{4}$  is not a field, implying that  $-1$  must be a square.

It is interesting to see how the Frobenius map acts if  $p \equiv 3 \pmod{4}$ , when the set of Gauss's integers modulo  $p$  is a field. To this end, write  $p = 4k + 3$ . Then

$$i^p = i^{4k+3} = i^{4k} \cdot i^3 = -i$$

since  $i^3 = -i$ . It follows that

$$(a + bi)^p \equiv a - bi = \overline{a + bi} \pmod{p}$$

making the analogy with complex conjugation rather convincing.

## 5. QUADRATIC RECIPROCITY

The Legendre Symbol is a function

$$\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \{\pm 1\}$$

defined as follows. If  $n$  is an element in  $(\mathbb{Z}/p\mathbb{Z})^\times$  or, simply, an integer relatively prime to  $p$  then

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \text{ is a square modulo } p \text{ and} \\ -1 & \text{if } n \text{ is not a square modulo } p. \end{cases}$$

Since the map  $x \mapsto x^2$  is two to one, the subgroup of squares has index 2 in the group  $(\mathbb{Z}/p\mathbb{Z})^\times$ . It follows that the symbol is a homomorphism:

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right) \left(\frac{n}{p}\right).$$

**Proposition 5.** *Let  $p$  be an odd prime. Then*

- (1)  $-1$  is a square modulo  $p$  if and only if  $p \equiv 1 \pmod{4}$ .
- (2)  $2$  is a square modulo  $p$  if and only if  $p \equiv 1, 7 \pmod{8}$ .
- (3) Let  $q$  be an odd prime. Then

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right).$$