Some Notes on Fields
Ma 362 Fall 2019

by Avinash Sathaye, Professor of Mathematics
October 16, 2019

Contents

1 Examples of Fields.

In mathematics, we work with numbers. The first numbers that we learn are the whole numbers or integers. Then we learn about fractions or rational numbers. A field is an abstraction of the important ideas associated with rational numbers.

Definition: Field.

Thus, a field is a set with built in operations of addition and multiplication. The operation of addition has an associated "subtraction" which is the inverse of addition. There is also a zero which acts as a neutral element for addition. The multiplication has its associated inverse called "division", but it is forbidden to divide by zero. There are natural distributive and commutative properties summarized in:

$$a(b+c) = ab + ac,\ a+b = b+a,\ ab = ba.$$

[1]

These are convenient properties for performing algebraic operations, so we like to study other fields.

The field of rational numbers is usually denoted by $\mathbb{Q}$. A much bigger field containing them is the field of real numbers, or the field of decimal numbers, which are permitted to possess infinite decimal expansions. This is denoted by $\Re$. There are many intermediate fields. One, for example may be thought of as $\mathbb{Q}\ (\sqrt{2})$ or the smallest field containing $\mathbb{Q}$ as well as $\sqrt{2}$. Its elements can be explicitely displayed as $a + b\sqrt{2}$ where a, b are rational numbers. It is easy to see how the addition and multiplication of these numbers can be carried out. It takes a little more imagination to work out that

$$\frac{1}{(a+b\sqrt{2})} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}.$$

These ideas can be extended to make $\mathbb{Q}\ (\alpha)$ into a field where α is the root of some polynomial equation over $\mathbb{Q}$. We shall work out examples in class discussions and homework.

Even bigger field is obtained by adjoining i the (non real) square root of -1 and denoted by $\mathbb{C}\ = \Re(i)$.

Another way of extending any field K is to adjoin indeterminates. Thus $K(X)$ is the field of rational functions of X with coefficients in K. It is easy to imagine adjoining many indeterminates in succession.

[1] We are giving a rather informal definition of a field. The reader should try to see if this is precise and consistent with the more formal and formidable definitions in books. It is also a worthy topic of discussion.

Yet another way of extending a field K is to form formal Laurent power series. A formal power series is like a polynomial but we allow the variable to take on infinitely many exponents, even some finitely many negative ones.

Thus, we allow expressions like

$$f(X) = a_{-m}X^{-m} + \cdots + a_0 + a_1X + \cdots + a_nX^n + \cdots .$$

The addition is termswise and multiplication is done just like polynomials, noting that at the time of collecting like terms, only finitely many products are involved at one time.

The calculation of the reciprocal of a power series does take some imagination and will be discussed in class meetings. Such ia field is denoted by $K((X))$.

Our first new example is, however, the field obtained by modular numbers or the so called finite field.

2 The finite Fields.

To create a finite field, we start with the set of integers denoted by $\mathbb{Z}$ and fix a prime p. We know that every integer n can be written as $n = qp + r$ where q s some integer and r is the remainder which is a number between 0 and $p - 1$.

Thus, there are p distinct remainders $0, 1, \cdots, p - 1$. These are called remainders modulo p and their set is denoted as $\mathbb{Z}_p$. We define operations on this set thus.

Define the sum of two remainders a, b to be the remainder of their sum $a + b$. Similarly, define the product of two remainders to be the remainder of their product. We shall say that two integers x, Y are equal as remainders if the remainder of $x - y$ is zero modulo p or p divides $x - y$ as an integer. This is written in notational form as $x - y \equiv 0 \pmod{p}$ or $x \equiv y \pmod{p}$.

Convention. In words, we may simply say that x equals y in $\mathbb{Z}_p$. Thus, we could say 17^2 equals 2 in $\mathbb{Z}_7$. One way of proving this is to first note that $17^2 = 289$ which has remainder 2 modulo 7. Let us note that a recommended procedure is to say that in $\mathbb{Z}_7$ we have 17 equal to 3, so its square is 9 whose remainder is 2. Thus, it is recommended that you simplify the work by taking remainders often!

The surprise is that now we can also find reciprocals of non zero remainders, even though such reciprocals don't exist in $\mathbb{Z}$, except for ± 1. Given a remainder $a \in \mathbb{Z}_p$ which is non zero, consider its multiples ax as x varies over $\mathbb{Z}_p$. I claim that $ax \neq ay$ in $\mathbb{Z}_p$ unless x equals y in $\mathbb{Z}_p$, or $x \equiv y \pmod{\ }$. This is seen thus:

Suppose if possible $ax \equiv ay \pmod{p}$. Then p must divide $a(x-y)$. But p is prime and by assumption, it does not divide a, so it must divide $(x-y)$, i.e. $x \equiv y \pmod{p}$.

■

Thus the remainders of ax as x varies over $\mathbb{Z}_p$ are p distinct numbers in $\mathbb{Z}_p$, so one of them, say some at must be 1. Then $at \equiv 1 \pmod{p}$ and thus t is the reciprocal of a in $\mathbb{Z}_p$.

For example, when $a = 2$ and $p = 7$ the set of elements of $\mathbb{Z}_7$ is $\{0, 1, 2, 3, 4, 5, 6\}$. The set $\{2x\}$ becomes $\{0, 2, 4, 6, 8, 10, 12\}$ and when we take the remainders, we get $\{0, 2, 4, 6, 1, 3, 5\}$. Thus the reciprocal of 2 is 4.

While the above was a clever proof and a useful technique (sometimes called the pigeon hole principle) it can be tedious, especially if the prime is large. A recommended method is to use the Euclidean division to get the answer. Thus, when a is not divisible by p, we get that the GCD of a, p is 1 (due to primeness of p). Then we have an expression

$$1 = ax - bp$$

and clearly the remainder of ax is 1 modulo p. So the inverse of a is x. For 2 modulo 7, we simply note that $1 = (2)(4) - (1)(7)$ and hence 4 is the answer!

2.1 Fermat's Little Theorem.

We next discuss one of the most important properties of $\mathbb{Z}_p$. First, recall the usual Binomial Theorem for p-th powers:

$$(X+Y)^p = X^p + \binom{p}{1} X^{p-1}Y + \cdots \binom{p}{i} X^{p-i}Y^i + \cdots Y^p.$$

We also know that the binomial coefficients

$$\binom{p}{i} = \frac{p \cdot (p-1) \cdots (p-i+1)}{i!}$$

are all integers divisible by p when $1 \leq i \leq p-1$. As a result all the terms between X^p and Y^p become zero in $\mathbb{Z}_p$. We thus have a wonderful formula

$$\text{in } \mathbb{Z}_p \text{ we have } (X+Y)^p = X^p + Y^p.$$

This is sometimes called the Freshman's Dream!

Now we have everything we need to prove the so-called

Theorem: Fermat's Little Theorem (FLT). For every integers x, we have $x^p \equiv x \pmod{p}$. Moreover, if $x \not\equiv 0 \pmod{p}$ then $x^{p-1} \equiv 1 \pmod{p}$.

Proof. By taking remainders mod p, it is enough to prove this for $x = 0, 1, \cdots, (p-1)$. It is obviously true for $x = 0, 1$. Also, since $(x+1)^p \equiv x^p + 1^p \pmod{p}$, we see that whenever $x^p \equiv x \pmod{p}$, we get that

$$(x+1)^p \equiv x^p + 1 \equiv x + 1 \pmod{p}.$$

Thus we are done by induction! The rest of the argument is obvious. ∎

Corollary Every element of a finite field $\mathbb{Z}_p$ is a root of the polynomial $X^p - X$. Moreover, since these are exactly p elements, we have a factorization:

$$X^p - X = \prod_0^{p-1} (X - i).$$

REMARK. Actually, we have proved something more general:

General FLT If we have any field F in which $p = 0$, then its elements a, b satisfy $(a+b)^p = a^p + b^p$.

Definition: Characteristic of a field. Such a "p" deserves a name. Thus, for any field F, we define its characteristic to be a positive integer p if the sum $1 + 1 + \cdots + 1$ of p terms evaluates to zero in F. The characteristic is said to be 0 if such a sum of 1's is never zero (as in $\mathbb{Q}$).

We leave it to the reader to prove that the characteristic is always a prime number, unless it is zero.[2]

Thus, in such a field F (of characteristic p), we have the following result:

Definition: Fröbenius Map Define a map $\sigma : F \to F$ by $\sigma(x) = x^p$. Then σ satisfies the properties:

$$\sigma(x+y) = \sigma(x) + \sigma(y) \text{ and } \sigma(xy) = \sigma(x)\sigma(y).$$

The first follows from the general FLT and the second is obvious. This map σ is said to be the **"Fröbenius"** map and is a very important tool in the study of finite fields.

Later on, when we deal with different fields, it would be convenient to denote σ by σ_p to indicate the characteristic being used.

We also note that given any field F of characteristic p, we can easily argue that the set $\{0, 1, \cdots, (p-1)\}$ contained in F is actually a field isomorphic to $\mathbb{Z}_p$ and every root of the polynomial $X^p - X$ is automatically contained in it! It is therefore called the **prime subfield** of F.

In case of characteristic zero, the prime subfield turns out to be $\mathbb{Q}$.

[2]Hint:

Write d for the sum of d 1's. Thus every natural number $1, 2, 3, \cdots$ has a well defined meaning as a sum of 1's.

Suppose $n = 0$ and $n = de$ for $1 < d, e < n$. Then $de = 0$ and we should get a contradiction.

In either case, the prime subfield is simply the smallest subfield which contains $0, 1$.

Later on we shall establish that if F is a finite field, then its number of elements $|F|$ is a power of p, its characteristic. Moreover, if $|F| = p^s$ then it consists of all the p^s roots of the polynomial $X^{p^s} - X$. Thus, each finite field is completely determined by its number of elements- a very remarkable fact!

2.2 Uses of the Fröbenius map.

Recall the skill needed to factor polynomial over $\mathbb{Q}$? We shall now show how the Fröbenius map σ_p gives a very effective technique for factorization over a finite field.

2.2.1 Quadratic extension of $\mathbb{Z}_p$.

Let $F = \mathbb{Z}_p$ where p is a prime number. Consider a quadratic equation

$$f(X) = X^2 + aX + b = 0.$$

The equation has potentially two roots, say α, β. It is possible that the two roots coincide. In principle, we could check the finitely many elements of F to see if any of them is a root. If it is, then $f(X)$ factors into linear factors and we we know both the roots. If not, then $f(X)$ is irreducible and the roots lie outside F.

Thus, for example, when $f(X) = X^2 + X + 2$ and $p = 5$, we see that that plugging in $X = 0, 1, 2, 3, 4$ gives non zero values, so $f(X)$ has no roots in $\mathbb{Z}_5$ and is irreducible. On the other hand, if $p = 7$, then $X = 3$ is a double root since $f(X) = (X - 3)^2$ over $\mathbb{Z}_7$. If we take $p = 11$, then we see that $X = 4, 6$ are two roots.

We now present an alternative to checking all the roots one by one. Note that

$$f(X)^p = X^{2p} + a^p X^p + b^p$$

in view of the general FLT. Note that by FLT, we get that $a^p = a$ and $b^p = b$. It follows that:

$$f(X)^p = (X^p)^2 + aX^p + b = f(X^p).$$

It follows that if α is any root of $f(X)$ so that $f(\alpha) = 0$ then we get $f(\alpha^p) = 0$ i.e. α^p is also a root. This is very fortunate, since usually, even when we know one root, it is not easy to find another so easily!

We illustrate how to use this for the above example of $f(X) = X^2 + X + 2$. Let x be an unknown root. Then we know that $x^2 = -x - 2$ since $f(x) = 0$. If $p = 5$, we try to compute $x^p = x^5$, by a sequence of steps.

$$x^3 = -x^2 - 2x = -(-x-2) - 2x = -x + 2.$$
$$x^4 = -x^2 + 2x = -(-x-2) + 2x = 3x + 2.$$
$$x^5 = 3x^2 + 2x = 3(-x-2) + 2x = -x - 6 = -x - 1.$$

Thus we see that $x^5 = x$ would lead to $x = -x - 1$ or $2x = -1$ or $x = 2$ in $\mathbb{Z}_5$. This is obviously not a root! This confirms that there are no roots in $\mathbb{Z}_5$.

If we analyze the same equation in $\mathbb{Z}_7$, then we see that when we divide X^7 by $X^2 + X + 2$ we get

$$X^7 = (X^5 - X^4 - X^3 + 3\,X^2 - X - 5)(X^2 + X + 2) + 7X + 10.$$

Thus if x is any root, then $x^7 = 10 = 3$ modulo 7. Hence $x = 3$ is a double root!

If we analyze it in $\mathbb{Z}_{11}$ then we get that

$$X^{11} = h(X)(X^2 + X + 2) + 23X - 22$$

where we have avoided writing out the quotient $h(X)$ of degree 9. Typically, we only compute remainders as illustrated for $p = 5$.

If x is a root modulo 11, then we see that

$$x^{11} = 23x - 22 = x \text{ modulo } 11.$$

Thus, we see that the roots are both in $\mathbb{Z}_{11}$, but we don't yet know what they are!

Thus, we have managed to argue that the equation factors in $\mathbb{Z}_{11}$ without finding the factors! There is no simple way to actually find the roots, except perhaps to invoke the usual quadratic formula valid here.

Remark. The usual quadratic formula works in all fields, **except when characteristic is 2.** What is usually unclear is how to decide if the discriminant has a square root, without actually checking all possible elements or using some theorems in number theory. Our method of using Fröbenius, gives an alternative.

Thus, to solve the equation

$$X^2 + AX + B = 0$$

we can still verify the formula:

$$X = \frac{-A \pm \sqrt{A^2 - 4B}}{2}$$

for the roots, provided $2 \neq 0$ in our field, i.e. $p \neq 2$. The question is if the $\sqrt{A^2 - 4B}$ exists in the field.

Let us denote $A^2 - 4B = D$ and note that we are simply trying to solve:

$$X^2 = D$$

in our field $\mathbb{Z}_p$. Let us apply the Fröbenius method. Write $p = 4q + r$ where $r = 1$ or $r = 3$.[3]

Set $m = \frac{p-1}{2}$ and we note that $m = 2q$ or $m = 2q + 1$ is an integer. Also we see that:

$$X^p = X^{2m+1} = (X^2)^m X = D^m X.$$

Thus $X^p = X$ iff $D^m = 1$ in our field $\mathbb{Z}_p$.

This gives us a simple test of when $\sqrt{D} \in \mathbb{Z}_p$: **Theorem Cauchy** Let $p \neq 2$ be a prime and $D \neq 0$ be an element of $\mathbb{Z}_p$.

Then $\sqrt{D} \in \mathbb{Z}_p$ iff $D^{\frac{p-1}{2}} = 1$ in $\mathbb{Z}_p$.

This is how we can use this for analyzing our equation.

For the equation $X^2 + X + 2 = 0$ our $D = (1)^-(4)(2) = -7$. For $p = 5$ we see that $m = \frac{p-1}{2} = \frac{4}{2} = 2$ and $(-7)^2 = 49 = -1 \bmod 5$. So, there are no roots in $\mathbb{Z}_5$ and it is irreducible.

For $p = 7$, $D = 0 \bmod 7$ and hence we get a double root.

For $p = 11$, we see that $D = -7 = 4 \bmod 11$. Since $4 = 2^2$, we need no test! The equation factors.

For $p = 13$, we get $D = -7 = 6$ and $m = 6$. Now we wish to calculate $6^6 \bmod 13$. Here are convenient steps for hand calculations.

$6^2 = 36 = -3 \bmod 13$. So $6^6 = (-3)^3 = -27 = -1 \bmod 13$. Thus, we have no roots in $\mathbb{Z}_{13}$.

For $p = 17$, we get that $D = -7 = 10 \bmod 17$ and $m = 8$. Now $D^2 = 100 = -2 \bmod 17$. So $D^8 = (D^2)^4 = (-2)^4 = 16 = -1$ so again there are no roots!

For $p = 23$, we get that $D = -7$ and $m = 11$. We wish to compute $(-7)^{11} \bmod 23$.

Here is an outline of how to do this even without a calculator!

Now $D^2 = 49 = 3 \bmod 23$. Then $D^4 = (3^2) = 9 \bmod 23$. Now $D^8 = 9^2 = 81 = 12 \bmod 23$. Also, $D^3 = D^2 \cdot D = (3)(-7) = -21 = 2 \bmod 23$.

Thus $D^{11} = D^8 D^3 = 12 \cdot 2 = 24 = 1 \bmod 23$. This says that it will factor! Of course, this does not yet help us find the factors.

If we had stopped and thought that $-7 = 16 \bmod 23$, then we would not have gone thru this test. We would have at once used the quadratic formula and declared the roots:

[3] In general r is one of $0, 1, 2, 3$ but the fact that $p \neq 2$ is a prime discards the other cases!

$$x = \frac{-1 \pm \sqrt{-7}}{2} = \frac{-1 \pm 4}{2} = \frac{3}{2}, -\frac{5}{2}.$$

What does it mean? If we note that $12 \cdot 2 = 24 = 1 \bmod 23$, we see that $\frac{1}{2} = 12 \bmod 23$ and hence the roots are $3 \cdot 12 = 36 = 13$ and $(-5) \cdot 12 = -60 = 9$.

3 Resultants

If we have two polynomials $f(X), g(X)$ over a field (or at least an integral domain) R, then we often need to know if they have a common root. If there is a common root, then it will be a root of the $GCD(f(X), g(X))$. So, it is enough to just find the GCD and check if it is 1 (or a degree zero polynomial). However, often, the polynomials $f(X)$ and $g(X)$ have variable coefficients and finding GCD is also messy.

We present a useful way to visualize and compute the GCD. Moreover, we can use it to analyze field extensions.

3.1 An example

Suppose that we are given two equations $f(X) - p = 0$ and $g(Y) - q = 0$. We wish to know all values of (p, q) for which these equations have a common root (value of X).

For example, let the equations be $X^3 - X = p, X^2 + X = q$. We can visualize this as a curve in the (p, q) plane parametrized by X. We construct a well defined polynomial in p, q denoted by $Resultant(f(X)-p, g(X)-q; X)$ and is equal to

$$\det \left[\begin{array}{ccccc} X^4 & X^3 & X^2 & X & 1 \\ \hline\hline 1 & 0 & -1 & -p & 0 \\ 0 & 1 & 0 & -1 & -p \\ 1 & 1 & -q & 0 & 0 \\ 0 & 1 & 1 & -q & 0 \\ 0 & 0 & 1 & 1 & -q \end{array} \right]$$

This can be evaluated by the definition of determinants by row or column expansions or better by row reductions. Note:

$$\det\begin{pmatrix} 1 & 0 & -1 & -p & 0 \\ 0 & 1 & 0 & -1 & -p \\ 1 & 1 & -q & 0 & 0 \\ 0 & 1 & 1 & -q & 0 \\ 0 & 0 & 1 & 1 & -q \end{pmatrix} \; R_3 - R_1 \to \; \det\begin{pmatrix} 1 & 0 & -1 & -p & 0 \\ 0 & 1 & 0 & -1 & -p \\ 0 & 1 & -q+1 & p & 0 \\ 0 & 1 & 1 & -q & 0 \\ 0 & 0 & 1 & 1 & -q \end{pmatrix}$$

We now expand by the first column to get a smaller determinant with the same value:

$$\det\begin{bmatrix} 1 & 0 & -1 & -p \\ 1 & 1-q & p & 0 \\ 0 & 1 & 1-q & p \\ 0 & 1 & 1 & -q \end{bmatrix}$$

One more operation $R_2 \to R_2 - R_1$ yields:

$$\det\begin{bmatrix} 1 & 0 & -1 & -p \\ 0 & 1-q & 1+p & p \\ 0 & 1 & 1-q & p \\ 0 & 1 & 1 & -q \end{bmatrix}$$

and now expansion by the first column yields a 3×3 determinant:

$$\det\begin{bmatrix} 2-q & 2+p & -q+p \\ 1 & 1-q & p \\ 1 & 1 & -q \end{bmatrix}.$$

This can be evaluated directly to yield: $-q^3+p^2+3\,qp+2\,q^2$ which is the equation of the p,q-curve with parametrization $X^3 - X = p, X^2 + X = q$.

To be continued ...