Finite fields 2017

A winter course at the Nesin Matematik Köyü

David Pierce

January 16–22, 2017
Edited January 5, 2018

Matematik Bölümü
Mimar Sinan Güzel Sanatlar Üniversitesi
mat.msgsu.edu.tr/~dpierce/

Preface

The present typeset document is based on a course of lectures at the Nesin Mathematics Village in Şirince, Selçuk, İzmir, January 16–22 (Monday–Sunday), 2017.

My course was one of three on the general theme of linear algebra. The students were university undergraduates, though not necessarily from mathematics departments, along with a few high-school students. The other teachers were Ali Nesin and Salih Durhan. I usually taught 9:00–11:00 (strictly, 9:00–50 and 10:00–50) in the Nişanyan Kütüphanesi, and the other courses were 11:00–13:00 and 17:00–19:00, with meals following each of these lecture.*

I started typesetting this document on Thursday morning, after three lectures had been completed. The sources are (1) my handwritten notes, prepared before the lectures, (2) the typeset notes from a similar course last year, (3) my memory of what happened in the lectures, and sometimes (4) my wishes for enlargements or improvements. Thus the notes are not a precise record of what actually happened, though they should be close.

I lectured mostly in Turkish, though writing on the board in English. Students' questions were mostly in Turkish, though sometimes, face to face during the break or after the second hour, in English.

1 Monday, January 16

We shall study *vector spaces over finite fields.* A **field** is a commutative ring in which $1 \neq 0$ and every nonzero element has a multiplicative inverse. Examples of fields include $\mathbb{C}$, $\mathbb{R}$, and $\mathbb{Q}$. A **vector space** is a module over a field. Every field is a vector space over every field that it *includes* as a subfield: thus $\mathbb{C}$ is a vector space over $\mathbb{R}$ and $\mathbb{Q}$, and $\mathbb{R}$ is a vector space

*On Monday I taught at 9:00, and Salih taught at 11:00 about modules in general. I was told Monday evening that Ali would teach at 9:00 the next day; I, 11:00. An SMS sent to Ali around 8:40 on Tuesday going unanswered, I went to the library anyway. Ali not being there at 9, I taught. He had been planning to come, but came late. Meanwhile, it transpired that the library was needed for another event at 11:00, involving children; lunch for our group was rescheduled for 12:00, but I did not get the message. (I did get lunch though, just before the children invaded the Bol Kepçe at 13:00.)

over $\mathbb{Q}$. We shall prove the following theorems.

1. The size of every finite field is the power of a prime number (Theorem 14, page 14).
2. For every prime power q, there is a field $\mathbb{F}_q$ of size q, and all such fields are isomorphic (Theorem 21, page 18).
3. If p is prime, and k and m are positive integers,

$$\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^m} \iff k \mid m$$

(Theorem 22, page 22).
4. The multiplicative group ${\mathbb{F}_q}^\times$ of *units* of $\mathbb{F}_q$ is isomorphic to $\mathbb{Z}_{q-1}$ (Theorem 25, page 23).

In order to be able to prove these theorems, we shall prove the following results from number theory.

1 Euclid's Lemma. *For all primes p,*

$$p \mid ab \ \& \ p \nmid a \implies p \mid b.$$

2 Bézout's Lemma. *For all integers a and b, not both 0, if d is the greatest common divisor of a and b, then the equation*

$$ax + by = d$$

is soluble.

Properly formulated,

- Euclid's Lemma will be true for every commutative ring for which Bézout's Lemma is true;
- Bézout's Lemma will be true for every commutative ring in which greatest common divisors can be found by the **Euclidean Algorithm.**

However, the converses fail; there are commutative rings in which Euclid's Lemma is true, but not Bézout's Lemma; and in which Bézout's Lemma is true, but the Euclidean Algorithm is not available.

The ring $\mathbb{Z}_5$ is $\{0, 1, 2, 3, 4\}$; one can check that this is a field, since, *modulo* 5,

$$2 \cdot 3 \equiv 1, \qquad\qquad 4 \cdot 4 \equiv 1,$$

and so all nonzero elements of $\mathbb{Z}_5$ have inverses. However, the ring $\mathbb{Z}_6$, namely $\{0, 1, 2, 3, 4, 5\}$, is not a field, since $2 \cdot 3 \equiv 0 \pmod 6$, so 2 can have no inverse.

We let $\mathbb{N}$ be the set $\{1, 2, 3, \dots\}$ or $\{x \in \mathbb{Z} \colon x > 0\}$ of positive integers, that is, counting numbers. If $n \in \mathbb{N}$, then

$$\mathbb{Z}_n = \{x \in \mathbb{Z} \colon 0 \leqslant x < n\}. \tag{1}$$

This is a ring with addition $\oplus$ and multiplication $\otimes$, where

$$\begin{aligned} a \oplus b = c &\iff a + b \equiv c \pmod n, \\ a \otimes b = c &\iff ab \equiv c \pmod n. \end{aligned}$$

(We shall work this out precisely tomorrow.)*

3 Theorem. *For all n in $\mathbb{N}$, if the ring $\mathbb{Z}_n$ is a field, then n must be prime.*

Proof. We show the contrapositive. If n is not prime, then it is either 1 or a composite ab, where $1 < a < n$. Since $\mathbb{Z}_1 = \{0\}$, this is not a field, since $1 \neq 0$ in a field. In the other case, $a \not\equiv 1$, but $ab \equiv 0 \pmod n$, so a has no inverse. □

*I did not use the notation $\oplus$ and $\otimes$ in class.

We shall show the converse, that for all primes p, $\mathbb{Z}_p$ is a field.* We have this already when p is 5. It is obviously true when p is 2.

On the four-element set $\{0, 1, \alpha, \beta\}$, we define addition and multiplication as in the following tables.

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\times$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

These are derived from the rules

$$1 + 1 = 0, \qquad \alpha^2 = \alpha + 1 = \beta, \tag{2}$$

assuming also that the resulting structure will be a field, so that, in particular,

$$x + x = 1x + 1x = (1 + 1)x = 0.$$

One can check that the structure *is* a field, which we may call $\mathbb{F}_4$; but this checking may be tedious, unless we develop some general principles.†

*I say that we shall use the Euclidean Algorithm for this; but here I shall turn out not to be correct. A student says he can prove the theorem without the Algorithm; but what he turns out to mean is that he can prove that every finite integral domain is a field.

†With students who ask questions after class, I observe that our $\mathbb{F}_4$ is $\mathbb{F}_2[\alpha]$, and this is ${\mathbb{F}_2}^2$ with multiplication of vectors by scalars extended to allow multiplication by all vectors. In the same way, $\mathbb{C}$ is $\mathbb{R}[\mathrm{i}]$, where $\mathrm{i}^2 + 1 = 0$; so $\mathbb{C}$ is $\mathbb{R}^2$ with multiplication similarly extended.

2 Tuesday, January 17

We want to show that, whenever p is prime, then $\mathbb{Z}_p$ is a field. What *is* $\mathbb{Z}_p$ anyway? More generally, when $n \in \mathbb{N}$, why is $\mathbb{Z}_n$ a ring? The relation R given by

$$x \mathrel{R} y \iff x \equiv y \pmod{n}$$

is an equivalence relation on $\mathbb{Z}$, meaning

$$\begin{gathered} x \mathrel{R} x, \\ x \mathrel{R} y \implies y \mathrel{R} x, \\ x \mathrel{R} y \ \&\ y \mathrel{R} z \implies x \mathrel{R} z. \end{gathered}$$

If $a \in \mathbb{Z}$, we define

$$[a] = \{x \in \mathbb{Z} \colon a \mathrel{R} x\},$$

the equivalence class of a with respect to R. Now we can define

$$\mathbb{Z}_n = \{[x] \colon x \in \mathbb{Z}\}.$$

The next two theorems allow us to use the definition in (1). We shall use the notation

$$\omega = \{0, 1, 2, \dots\} = \{0\} \cup \mathbb{N} = \{x \in \mathbb{Z} \colon x \geqslant 0\}.$$

4 **Division Theorem.** *For all n in $\mathbb{N}$ and a in $\mathbb{Z}$, the system*

$$a = nx + y \ \&\ 0 \leqslant y < n$$

has a unique solution.

Proof. We shall use that ω is *well-ordered*: every nonempty subset has a least element. The set

$$\{a - nx \colon x \in \mathbb{Z}\} \cap \omega$$

is nonempty (why?); so it has a least element, r, and then for some q,

$$a = nq + r.$$

If $r \geqslant n$, then $a = n(q+1) + (r - n)$, so $r - n \in \{a - nx \colon x \in \mathbb{Z}\} \cap \omega$, but is less than the least element, which is absurd. So $0 \leqslant r < n$. Uniqueness is an exercise. $\square$

5 Theorem. *For all n in $\mathbb{N}$,*
1) $\mathbb{Z}_n = \{[x] \colon 0 \leqslant x < n\}$;
2) $|\mathbb{Z}_n| = n$.

Proof. The first part follows from the previous theorem. For the second part, if $0 \leqslant a < b < n$, then $0 < b - a < n$, so $n \nmid b - a$, and so $a \not\equiv b \pmod{n}$. $\square$

We now establish that $\mathbb{Z}_n$ is a ring.

6 Theorem. *For all n in $\mathbb{N}$, for all a, b, c, and d in $\mathbb{Z}$, if*

$$a \equiv c \;\;\&\;\; b \equiv d \pmod{n},$$

then

$$a + b \equiv c + d \;\;\&\;\; ab \equiv cd \pmod{n}.$$

This means the following definitions are valid on $\mathbb{Z}_n$:

$$[x] + [y] = [x + y], \qquad [x] \cdot [y] = [xy].$$

Then $\mathbb{Z}_n$ must satisfy all identities, like $x \cdot (y + z) = xy + xz$, that involve addition and multiplication* and are true in $\mathbb{Z}$.

*In class I wrote only the example $xy = yx$.

Since commutative rings are defined as satisfying some such identities, $\mathbb{Z}_n$ must be a commutative ring, like $\mathbb{Z}$.

However, not all properties of $\mathbb{Z}$ are inherited by $\mathbb{Z}_n$. For example, $\mathbb{Z}$ is infinite, but $\mathbb{Z}_n$ is not. Moreover, $\mathbb{Z}$ satisfies

$$0 \neq 1 \ \& \ \forall x\, \forall y\, (xy = 0 \ \& \ x \neq 0 \implies y = 0);$$

this means it is an **integral domain.** All fields are integral domains, but $\mathbb{Z}$ is an integral domain that is not a field. The example $\mathbb{Z}_6$ is not even an integral domain.

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

Proof. Let R be a finite integral domain and $a \in R \smallsetminus \{0\}$. The function $x \mapsto ax$ having domain $R \smallsetminus \{0\}$ has range included in $R \smallsetminus \{0\}$, since if $b \neq 0$ in R, then $ab \neq 0$. Similarly, the function is injective:

$$ab = ac \implies a(b - c) = 0 \implies b - c = 0 \implies b = c.$$

By the Pigeonhole Principle, the function must be surjective. This means the equation $ax = 1$ has a solution. $\square$

Euclid's Lemma is that, for all primes p,

$$ab \equiv 0 \ \& \ a \not\equiv 0 \implies b \equiv 0 \pmod{p},$$

that is, in $\mathbb{Z}_p$,

$$ab = 0 \ \& \ a \neq 0 \implies b = 0.$$

Since $p > 1$ in $\mathbb{Z}_p$, we have $0 \neq 1$ there. Thus we can restate Euclid's Lemma (Theorem 1) as follows.

8 Euclid's Lemma (second form)**.** *For all primes p, $\mathbb{Z}_p$ is an integral domain.*

Again, we shall prove this by means of Bézout's Lemma, which we shall prove as we proved the Division Theorem (Theorem 4).

Proof of Bézout's Lemma. Let d be the least element of the set
$$\{ax+by\colon (x,y)\in\mathbb{Z}\times\mathbb{Z}\}\cap\mathbb{N}.$$
By the Division Theorem, for some q and r in $\mathbb{Z}$, we have
$$a=dq+r \;\;\&\;\; 0\leqslant r<d.$$
Then for some x and y we have
$$r=a-dq=a-(ax+by)q=a(1-qx)+b(-qy),$$
so r belongs to $\{ax+by\colon (x,y)\in\mathbb{Z}\times\mathbb{Z}\}$. By the minimality of d as a positive element of this set, r must be 0. Thus $d\mid a$. Likewise $d\mid b$. Since d is of the form $ax+by$, every common divisor of a and b must divide d. □

We denote the greatest common divisor of a and b by
$$\gcd(a,b).$$

3 Wednesday, January 18

Proof of Euclid's Lemma. Suppose $p\mid ab$, but $p\nmid a$. Then
$$\gcd(a,p)=1,$$
so for some x and y,
$$\begin{aligned}ax+py&=1,\\ abx+pby&=b.\end{aligned}$$
Since $p\mid abx+pby$ for all x and y, we conclude $p\mid b$. □

9 Theorem. *For all primes p, $\mathbb{Z}_p$ is a field.*

Proof. By Euclid's Lemma, $\mathbb{Z}_p$ is an integral domain; then by Theorem 7, it is a field. $\square$

To emphasize that it is a field, we shall write $\mathbb{Z}_p$ as $\boxed{\mathbb{F}_p.}$ What other finite fields can there be? On Monday we saw the example $\{0, 1, \alpha, \beta\}$, with the conditions (2). We can write the field as $\mathbb{F}_2[\alpha]$, where $\alpha^2 + \alpha + 1 = 0$. In general, if R is a commutative ring, and α belongs to some larger commutative ring, then

$$R[\alpha] = \{0\} \cup \bigcup_{n \in \omega} \{x_0\alpha^n + x_1\alpha^{n-1} + \cdots + x_{n-1}\alpha + x_n \colon (x_0, \dots, x_{n-1}) \in R^n \ \& \ x_0 \neq 0\},$$

which is the smallest ring that includes R and contains α. Note that, for this definition to make sense, α should already belong to some commutative ring that includes R. If X is a "variable" or *indeterminate,* we define $R[X]$ formally, just as we do $R[\alpha]$; but the elements of $R[X]$ are the **polynomials** in X with coefficients from R. Then we have

$$R[\alpha] = \{f(\alpha) \colon f \in R[X]\}.$$

We are going to show how $R[\alpha]$ may be determined by some desired property, falling short of membership in a known ring. For example, $\mathbb{C} = \mathbb{R}[\mathrm{i}]$, where $\mathrm{i}^2 + 1 = 0$. We shall be able to define $\mathbb{F}_8$ as $\mathbb{F}_2[\alpha]$, where now $\alpha^3 = \alpha + 1$, so that, as a set,

$$\mathbb{F}_8 = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}.$$

For example, $\alpha \cdot (\alpha^2 + \alpha) = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$. But if we separately require $\beta^3 = \beta^2 + \beta + 1$, then

$$\mathbb{F}_2[\beta] = \{0, 1, \beta, \beta + 1, \beta^2, \beta^2 + 1, \beta^2 + \beta, \beta^2 + \beta + 1\}.$$

This is a commutative ring, but not an integral domain, since

$$0 = \beta^3 + \beta^2 + \beta + 1 = (\beta^2 + 1)(\beta + 1),$$

but neither factor is 0.

In any commutative ring R, the invertible elements are called **units,** and they compose the multiplicative group denoted by

$$R^\times.$$

For example, $\mathbb{Z}^\times = \{\pm 1\}$, while $K^\times = K \smallsetminus \{0\}$ for any field K. An element π of R is called **irreducible** if it has the properties of prime numbers: $\pi \neq 0$ and $\pi \notin R^\times$, but

$$\pi = ab \ \& \ a \notin R^\times \implies b \in R^\times.$$

We shall use irreducibles in $K[X]$ to obtain fields, just as we used primes in $\mathbb{N}$ to obtain the fields $\mathbb{F}_p$.

For any element a of R, we define

$$(a) = \{ax \colon x \in R\}.$$

This determines an equivalence relation R given by

$$x \mathrel{S} y \iff x - y \in (a).$$

Now for any b in R we define

$$[b] = \{x \in R \colon x \mathrel{S} a\} = \{x \in R \colon a \mid x - y\}.$$

Finally,

$$R/(a) = \{[x] \colon x \in R\}.$$

Thus, in particular,

$$\mathbb{Z}_n = \mathbb{Z}/(n).$$

Just as we showed, for all p in $\mathbb{N}$,

$$\mathbb{Z}/(p) \text{ is a field} \iff p \text{ is prime},$$

so we shall show, for all f in $K[X]$,

$$K[X]/(f) \text{ is a field} \iff f \text{ is irreducible}.$$

4 Thursday, January 19

As an example, X^3+X+1 is irreducible in $\mathbb{F}_2[X]$, because if it is not, then we have

$$X^3+X+1=(X+a)(X^2+bX+c)$$

for some a, b, and c in $\mathbb{F}_2$; but in this case

$$X^3+X+1=X^3+(a+b)X^2+(ab+c)X+ac,$$

so $a=c=1$ (since $1=ac$), and then $b=a=1$ (since $0=a+b$), so $1=ab+c=0$, which is absurd.

The polynomial X^2+1 is irreducible over $\mathbb{R}$, but not over $\mathbb{C}$, since

$$X^2+1=(X+\mathrm{i}\,)(X-\mathrm{i}\,).$$

An element π of an integral domain R is called **prime** if $\pi\neq 0$ and $\pi\notin R^{\times}$, but

$$\pi\mid ab\ \ \&\ \ p\nmid a\implies p\mid b.$$

Thus we have:

10 Euclid's Lemma (third form)**.** *All irreducibles in* $\mathbb{Z}$ *are prime.*

We proved this using Bézout's Lemma. We can do the same for $K[X]$, using an analogue of Theorem 4. Every nonzero element f of $K[X]$ is, for some d in ω,

$$a_0+a_1X+\dots+a_dX^d,$$

where the a_i are in K, and $a_d\neq 0$; and then

$$d=\deg(f),$$

the **degree** of f. For completeness, we may define

$$\deg(0) = -\infty.$$

11 Division Theorem (for polynomials). *For all fields K, for all f in $K[X]$ and g in $K[X] \smallsetminus \{0\}$, there are some q and r in $K[X]$ such that*

$$f = gq + r \ \ \& \ \ \deg(r) < \deg(g).$$

Moreover, $\deg(r)$ *is uniquely determined by f and g.*

Proof. Exercise. (Let r be an element of $\{f - g \cdot \xi \colon \xi \in K[X]\}$ having minimal degree.) □

12 Bézout's Lemma (for polynomials). *For all fields K, for all f and g in $K[X]$, not both* 0*, for every element h of the set*

$$\{f \cdot \xi + g \cdot \eta \colon \xi, \eta \in K[X]\}$$

having minimal degree,

(i) *$h \mid f$ and $h \mid g$;*

(ii) *if $k \in K[X]$ and $k \mid f$ and $k \mid g$, then $k \mid h$.*

Proof. Exercise. □

The polynomial h in the theorem is a greatest common divisor of f and g. It is unique up to multiplication by a nonzero scalar. Now we can show:

13 Euclid's Lemma (for polynomials). *For every field K, every irreducible f of $K[X]$ is prime, and consequently $K[X]/(f)$ is an integral domain.*

Proof. Exercise. □

If f in $\mathbb{F}_p[X]$ is irreducible of degree n, then $\mathbb{F}_p[X]$ is an integral domain of size p^n and is therefore a field. We shall show that such f exist for all positive degrees.

Every commutative ring R contains all of the sums

$$\underbrace{1+\dots+1}_{n},$$

where $n \in \mathbb{N}$. If the sum is 0 for some n, then the least such n is called the **characteristic** of R, or

$$\operatorname{char}(R).$$

If R is an integral domain, then $\operatorname{char}(R)$ must be a prime p. In this case, we may suppose $\mathbb{F}_p \subseteq R$; and then R is a vector space over $\mathbb{F}_p$.

14 Theorem. *The size of every finite field is a prime power.*

Proof. If K is a finite field, then, by what we have just seen, K is a vector space over some $\mathbb{F}_p$. As such, K has a basis of some finite size n; and then $|K| = p^n$. □

We shall give more details on Saturday.

5 Friday, January 20

15 Fermat's Theorem. *For all primes p and all a in $\mathbb{Z}$, if $p \nmid a$, then*

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

Proof. The claim is that, in $\mathbb{Z}_p$,

$$a \neq 0 \implies a^{p-1} = 1,$$

or equivalently, for all a in $\mathbb{Z}_p$,

$$a^p = a. \tag{3}$$

We can prove this by induction in $\mathbb{Z}_p$. Immediately (3) when $a = 1$. Suppose (3) is true when $a = b$, so $b^p = b$. Then

$$(b+1)^p = b^p + \sum_{i=1}^{p-1} \binom{p}{i} b^{p-i} + 1 = b^p + 1 = b + 1$$

in $\mathbb{Z}_p$ (see below), so (3) is true when $a = b+1$. By induction, (3) is true for all a in $\mathbb{Z}_p$. □

We have used:

16 Lemma. *When* $0 < k < p$, *then*

$$p \,\bigg|\, \binom{p}{k}.$$

Proof. We have

$$\binom{p}{k} = \frac{p!}{k! \cdot (p-k)!};$$

also, this is indeed a whole number, since it is a coefficient appearing in a polynomial over $\mathbb{Z}$, and also since it is the number of k-element subsets of a set of size p. We want to show

$$k! \cdot (p-k)! \mid (p-1)!. \tag{4}$$

By Euclid's Lemma, since $0 < k < p$ and p is prime,

$$p \nmid k! \cdot (p-k)!,$$

and then $\gcd\big(p, k! \cdot (p-k)!\big) = 1$. Consequently, by the *proof* of Euclid's Lemma (page 9), we have (4). □

We can also derive Fermat's Theorem as a special case Euler's Theorem below, which uses the definition

$$\varphi(n) = \left|\mathbb{Z}_n{}^\times\right|.$$

It follows again from the proof of Euclid's Lemma that

$$\mathbb{Z}_n{}^\times = \{[x] \in \mathbb{Z}_n \colon \gcd(n, x) = 1\}.$$

17 Euler's Theorem. *For all n in $\mathbb{N}$, for all a in $\mathbb{Z}$, if* $\gcd(a, n) = 1$, *then*

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

Proof. If $\gcd(a, n) = 1$, then $[a] \in \mathbb{Z}_n{}^\times$, so all powers of $[a]$ are in this group. But then for some k and m such that $0 \leqslant k < m \leqslant \varphi(n)$, we have

$$a^k \equiv a^m \pmod{n}, \qquad a^{m-k} \equiv 1 \pmod{n}.$$

If now j is minimal such that $0 < j \leqslant \varphi(n)$ and $a^j \equiv 1 \pmod{n}$, then $j \mid \varphi(n)$ [why?*]. This yields the claim. □

The same proof gives us:

18 Theorem. *If K is a finite field of size q, then*

$$K^\times = \{x \in K \colon x^{q-1} = 1\}, \qquad K = \{x \in K \colon x^q = x\}.$$

Now we shall be able to give a precise characterization of a finite field, thanks to the following.

*I may not have raised this question in class. On can appeal to the Lagrange Theorem or prove it for the present case: There will be some elements b of $\mathbb{Z}_n{}^\times$ such that the group is the disjoint union of the subsets $\{a^k b \colon 0 \leqslant k < j\}$, each having size j.

19 Theorem. *For any field K, for any f in $K[X] \smallsetminus \{0\}$,*

$$|\{x \in K \colon f(x) = 0\}| \leqslant \deg(f).$$

Proof. Suppose $f(\alpha) = 0$. By the Division Theorem for polynomials (Theorem 11), for some g in $K[X]$,

$$f = (X - \alpha) \cdot g.$$

If $\beta \neq \alpha$ and $f(\beta) = 0$, then $g(\beta) = 0$. Thus f can have at most one more zero than g has. If $\deg(g) = 0$, then g has no zeros. By induction, the proof is complete. □

An **algebraically closed field** is a field over which every irreducible polynomial has degree 1. This means *every* polynomial has a zero in the field.* An **algebraic closure** of a field K is an algebraically closed field that includes K and that embeds over K in any other algebraically closed field that includes K.

20 Theorem. *Every field has an algebraic closure.*

Proof. We prove this only for finite or countable fields K; the general case is similar, but requires *transfinite* recursion. Even in the special case, we are not yet going to give a complete proof.

Let $(f_i \colon i \in \omega)$ be a list of all of the irreducible polynomials over K having degree greater than 1. Let $K_0 = K$, and if K_m has been defined so as to include K, let

$$K_{m+1} = K_m[X]/(g_m),$$

*Except polynomials of degree 0.

where $g_m \in K_m[X]$ and is an irreducible factor of f_m. By recursion, we now have a chain

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots$$

We define

$$K^{\mathrm{alg}} = \bigcup_{i \in \omega} K_i;$$

this is the **algebraic closure** of K. For, it contains a zero of every irreducible polynomial over K. Moreover, it contains a zero of every polynomial over *itself* (though this has to be proved). Finally, K^{alg} embeds in every algebraically closed field in which K itself embeds (this too must be shown). $\square$

21 Theorem. *For each prime power p^n, the set*

$$\{x \in \mathbb{F}_p{}^{\mathrm{alg}} \colon x^{p^n} = x\}$$

is a field of size p^n. Every field of size p^n is isomorphic to this one.

Proof. Let f be the function $x \mapsto x^p$ from $\mathbb{F}_p{}^{\mathrm{alg}}$ to itself. The indicated set is

$$\{x \in \mathbb{F}_p{}^{\mathrm{alg}} \colon f^n(x) = x\},$$

where by definition $f^1 = f$ and $f^{k+1} = f \circ f^k$. We have $f(1) = 1$, and by the commutativity of multiplication, $f(xy) = f(x) \cdot f(y)$. Hence the indicated set is closed under multiplication and inversion. By Lemma 16, $f(x + y) = f(x) + f(y)$; so the indicated set is now a field. By the last three theorems, this field is unique (up to isomorphism) as a field of its size.* $\square$

*I did not write out this proof in class.

The field in the theorem can be called

$$\mathbb{F}_{p^n}.$$

We finally want to show that $K^\times$ is cyclic for all finite fields K. We consider first some examples.

In $\mathbb{F}_{17}$, the computations

x	0	1	2	3	4	5	6	7	8	
2^x	1	2	4	8	-1	-2	-4	-8	1	mod 17
3^x	1	3	-8	-7	-4	5	-2	-6	-1	mod 17
3^{8+x}	-1	-3	8	7	4	-5	2	6	1	mod 17

show that ${\mathbb{Z}_{17}}^\times$ is not $\langle 2\rangle$, but is $\langle 3\rangle$.

In $\mathbb{F}_2[X]$, let $f = X^3 + X + 1$, and let $\alpha = [X] = X + (f)$ in $\mathbb{F}_2[X]/(f)$, which field is therefore $\mathbb{F}_2[\alpha]$. Then $\alpha^3 = \alpha + 1$, so we can compute as follows.*

x	0	1	2	3	4	5	6	7
α^x	1	α	α^2	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2+1	1

Thus $\mathbb{F}_2[\alpha]^\times = \langle\alpha\rangle$. But this is no surprise: since the group has prime order, every nontrivial element generates it.

However, $X^2 + 1$ is irreducible over $\mathbb{F}_3$, since it has no zero in $\mathbb{F}_3$. Let $\beta = X + (X^2+1)$ in $\mathbb{F}_3[X]/(X^2+1)$. Then $\beta^2 = -1$ so $\beta^4 = 1$. Thus β cannot generate ${\mathbb{F}_\beta}^\times$, which has order 8. However, $\beta + 1$ does generate the group:

x	0	1	2	3	4
$(\beta+1)^x$	1	$\beta+1$	$-\beta$	$1-\beta$	-1
$(\beta+1)^{4+x}$	-1	$-(\beta+1)$	β	$\beta-1$	1

*I did not give this example in class.

Writing $\beta + 1$ as α, we have $\beta = \alpha - 1$, so $0 = (\alpha - 1)^2 + 1 = \alpha^2 + \alpha - 1$, so

$$\mathbb{F}_3[\beta] = \mathbb{F}_3[\alpha] = \mathbb{F}_3[X]/(X^2 + X - 1).$$

In fact

$$X^8 - 1 = (X - 1)(X + 1)(X^2 + 1)(X^4 + 1),$$

and over $\mathbb{F}_3$ we have

$$X^4 + 1 = (X^2 + X - 1)(X^2 - X - 1).$$

Any of the three irreducible polynomials X^2+1 and $X^2 \pm X - 1$ will give us $\mathbb{F}_9$.

It will be true generally that $X^{p^n-1} - 1$ has at least one irreducible factor over $\mathbb{F}_p$ of degree n, and none of higher degree.

6 Saturday, January 21

Detailed proof of Theorem 14. Let K be a finite field, and suppose $\operatorname{char}(K) = p$. Then $\mathbb{F}_p \subseteq K$. For some n in $\mathbb{N}$,

$$p^{n-1} < |K| \leqslant p^n.$$

By recursion, K has a subset $\{a_i \colon 0 \leqslant i < n\}$ such that, whenever $0 \leqslant m < n$,

$$a_m \notin \left\{ \sum_{i=0}^{m-1} a_i x_i \colon x_i \in \mathbb{F}_p \right\}.$$

This is so because, defining

$$V_m = \left\{ \sum_{i=0}^{m-1} a_i x_i \colon x_i \in \mathbb{F}_p \right\},$$

we have $|V_m| \leqslant p^m$. Now we show by induction

$$|V_m| = p^m, \tag{5}$$

whenever $m \leqslant n$. By definition, $\sum_{i=0}^{m-1} a_i x_i$ is 0, which is neutral with respect to addition, just as $0! = 1$, which is neutral for multiplication. Also

$$\sum_{i=0}^{m-1} 1 = m \cdot 1 = m;$$

it makes sense that this should be true even when $m = 0$. Suppose now $k < n$ and (5) holds when $m = k$. We have

$$V_k \cap \{a_k x \colon x \in \mathbb{F}_p\} = \{0\},$$

since if $a_k b \in V_k$, but $b \neq 0$, then $a_k b b^{-1} \in V_k$ (since this is a vector space over $\mathbb{F}_p$), but this means $a_k \in V_k$, contrary to the definition. So now the surjective function $(v, x) \mapsto v + a_k x$ from $V_m \times \mathbb{F}_p$ onto V_{k+1} is also injective, since if

$$v + a_k b = w + a_k c$$

for some v and w in V_k and b and c in $\mathbb{F}_p$, then

$$v - w = a_k(c - b),$$

so both sides are in $V_k \cap \{a_k x \colon x \in \mathbb{F}_p\}$, which means they are 0, so $v = w$ and $b = c$. Now we have

$$|V_{k+1}| = |V| \times |\mathbb{F}_p| = p^k \cdot p = p^{k+1},$$

so (5) is true when $m = k+1$. By induction it is true whenever $m \leqslant n$. In particular,

$$p^n = |V_n| \leqslant |K| \leqslant p^n,$$

so $|K| = p^n$. □

22 Theorem. *For all primes p, for all m and t in $\mathbb{N}$,*

$$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^t} \iff m \mid t.$$

Proof. By the same proof as when $K = \mathbb{F}_p$, if K and L are two finite fields such that $K \subseteq L$, then for some n in $\mathbb{N}$,

$$|L| = |K|^n.$$

In particular, if $|K| = p^m$, then $|L| = p^t$ for some t, where $m \mid t$.

Suppose conversely $m \mid t$. Then $t = mk$ for some k, and so

$$\begin{gathered}
p^t - 1 = (p^m)^k - 1 = (p^m - 1)\bigl((p^m)^{k-1} + \cdots + 1\bigr), \\
p^t - 1 = (p^m - 1), \\
\begin{aligned}
\mathbb{F}_{p^m} = \{0\} \cup {\mathbb{F}_{p^m}}^\times &= \{0\} \cup \{x \in \mathbb{F}_{p^t} \colon x^{p^m-1} = 1\} \\
&\subseteq \{0\} \cup \{x \in \mathbb{F}_{p^t} \colon x^{p^t-1} = 1\} \\
&= \{0\} \cup {\mathbb{F}_{p^t}}^\times = \mathbb{F}_{p^t}.
\end{aligned}
\end{gathered}$$

□

It remains to show ${\mathbb{F}_q}^\times \cong \mathbb{Z}_{q-1}$.

23 Theorem. *For all a and b in $\mathbb{N}$, if $d = \gcd(a, b)$, then*

1) *ab/d is a common multiple of a and b, and*
2) *if c is a common multiple of a and b, then $ab/d \mid c$.*

Proof. $a \mid a \cdot (b/d)$ and $b \mid (a/d) \cdot b$. Suppose $a \mid c$ and $b \mid c$. Then $c/a \in \mathbb{Z}$, and

$$\frac{b}{d} \biggm| c, \qquad \frac{b}{d} \biggm| \frac{c}{a} \cdot a, \qquad \frac{b}{d} \biggm| \frac{c}{a}$$

since $\gcd(b/d, a) = 1$, and therefore $ab/d \mid c$. □

Thus

$$\frac{ab}{\gcd(a,b)} = \operatorname{lcm}(a,b),$$

the least common multiple of a and b.

24 Theorem. *If an abelian group has elements g and h of orders a and b respectively, the the element*

$$\gcd(a,b) \cdot g + h$$

has order $\operatorname{lcm}(a,b)$*.*

Proof. Let $\gcd(a,b) = d$. Then $|dg| = a/d$ and $|h| = b$, and $\gcd(a/d, b) = 1$. By the proof of Euler's Theorem (Theorem 17), since every element of $\langle dg \rangle$ or $\langle h \rangle$ has order dividing that of the respective group,

$$\langle dg \rangle \cap \langle h \rangle = \{0\}.$$

As in the proof of Theorem 14 above, if $c(dg+h) = 0$, then $cdg = -ch$, so each side belongs to $\langle dg \rangle \cap \langle h \rangle$ and is therefore 0. Then $a \mid cd$, so $a/d \mid c$; but also $b \mid c$, and therefore $ab/d \mid c$, since $\gcd(a/d, b) = 1$. Conversely

$$\frac{ab}{d}(dg+h) = bag + abh = 0.$$

Thus $|dg+h| = \operatorname{lcm}(a,b)$. □

25 Theorem. *For all prime powers q,*

$$\mathbb{F}_q{}^{\times} \cong \mathbb{Z}_{q-1}.$$

Proof. Let a be an element of ${\mathbb{F}_q}^\times$ of maximal order. If $b \in {\mathbb{F}_q}^\times$, then the group has an element of order $\operatorname{lcm}(|a|, |b|)$, and therefore $|b|$ must divide $|a|$. If this order is n, then

$$ {\mathbb{F}_q}^\times = \{x \in \mathbb{F}_q \colon x^n = 1\}. $$

By Theorem 19,

$$ q - 1 = \left|{\mathbb{F}_q}^\times\right| \leqslant n, $$

so $n = q - 1$, and therefore ${\mathbb{F}_q}^\times = \langle a \rangle$. □

7 Sunday, January 22

$\mathbb{F}_q$ as splitting field; EDs, PIDs, and UFDs; induction and recursion.

Contents