MA294 Lecture

Timothy Kohl

Boston University

April 2, 2024

The Order of a Finite Field

Recall that in a field F there are no zero-divisors, that is if $x, y \in F$ where $x \neq 0$ and $y \neq 0$ then $xy \neq 0$.

Also, in a ring R, given $n \in \mathbb{Z}$, one may define $n \cdot 1$ as

$$\begin{cases} 1 + 1 + \cdots + 1 & n > 0 \\ (-1) + (-1) + \cdots + (-1) & n < 0 \\ 0 & n = 0 \end{cases}$$

and similarly, given $x \in R$, and $n \in \mathbb{Z}$, one has $n \cdot x = x + x + \cdots + x$ which has the property that $(n_1 x) + (n_2 x) = (n_1 + n_2)x$, and also $(n_1 x)(n_2 x) = n_1 n_2 x^2$.

Returning to 1 for a moment, under addition in R, the unity element 1 generates a cyclic subgroup that is either finite or infinite.

Definition

In a ring R if $|\langle 1 \rangle| = n$ (finite) then R has characteristic n, denoted $char(R) = n$, and if $|\langle 1 \rangle|$ is infinite, we say that R has characteristic zero, denoted $char(R) = 0$.

Basically, if $char(R) = n$ then $n \cdot 1 = 0$, but if $char(R) = 0$, then the only multiple of 1 that is 0, *is* 0.

Fact: If $char(R) = n$ then $nx = 0$ for *all* $x \in R$ since $nx = n \cdot (1 \cdot x) = (n \cdot 1) \cdot x = 0 \cdot x = 0$.

Theorem

If F is a finite field, then $char(F) = p$ for some prime p.

Proof.

Since F is finite, then $\langle 1 \rangle$ is a finite subgroup of $(F, +)$ so $|\langle 1 \rangle| = n$ for some finite n. If n is *not* prime then $n = ab$ for some $a, b \in \mathbb{Z}$ where $1 < a < n$ and $1 < b < n$ and so $a \neq 0$ and $b \neq 0$. However $char(F) = n$ means $(a \cdot b) \cdot 1 = n \cdot 1 = 0$ which means F has zero-divisors, which is impossible. So n must be a prime number. □

Beyond this, we can view finite fields as 'vector spaces' of a certain sort.

Theorem

If F is a finite field where $\text{char}(F) = p$ then $(F, +) \cong \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p \cong (\mathbb{Z}_p)^n$ for some $n > 0$.

We can outline how the proof works.

Let $v_1 \in F$ be a non-zero element, then it must be the case that $pv_1 = 0$ since $char(F) = p$ and, since F is a field, if $rv_1 = 0$ then, since F is a domain, it would imply that $r = 0$, i.e. $r = p$.

So, let $V_1 = \langle v_1 \rangle \leq F$, and if $V_1 = F$ then we're done, otherwise pick $v_2 \in F - V_1$ (which must be non-zero) and a similar argument shows that $V_2 = \langle v_2 \rangle$ also has p elements and is a subgroup of F.

Since F is an abelian group, $V_1 + V_2 = \{x + y \mid x \in V_1, y \in V_2\}$ is a subgroup, and since each has order p, then $V_1 \cap V_2 = \{0\}$ and so $|V_1 + V_2| = \frac{|V_1| \cdot |V_2|}{|V_1 \cap V_2|} = p^2$.

So we can check if $F = V_1 + V_2$, and if not, we can find a $V_3 \leq F$ of order p which also intersects V_1 and V_2 trivially and find that $V_1 + V_2 + V_3 \leq F$ which has order p^3 and see if it equals F etc.

Ultimately this process must stop since F is finite.

Basically, if F is a finite field where $char(F) = p$ then there exists elements $\vec{f}_1, \vec{f}_2, \ldots, \vec{f}_n \in F$ such that every element of F is of the form

$$a_1\vec{f}_1 + a_2\vec{f}_2 + \cdots + a_n\vec{f}_n$$

where $a_i \in \mathbb{Z}_p$, namely that $\{\vec{f}_1, \vec{f}_2, \ldots, \vec{f}_n\}$ is a 'basis' for F as a $\mathbb{Z}_p$ vector space.

Another point to make is this fact about groups.

Theorem (Cauchy)

If p is a prime and $p \mid |G|$ for a finite group G, then there exists an element $g \in G$ such that $|g| = p$.

This is a very important result which, in a way is somewhat like a converse to LaGrange's theorem, however it **doesn't** say that for every divisor m of $|G|$ that there is an element of G of order m.

For example, $|A_4| = 12$ but A_4 has no elements of order 4.

So for a finite field F (which is also an abelian group under addition) then $char(F) = p$ for some prime p.

So if $|F|$ is divisible by some prime $q \neq p$ then there exists $x \in F$ such that $|x| = q$ but since $char(F) = p$ then $p \cdot x = 0$ which means $q \mid p$ which is impossible!

As such $|F| = p^n$ for some n.

Constructing Finite Fields

Mimicking the example with $x^2 + 1 \in \mathbb{Z}_3[x] = \mathbb{F}_3[x]$ which was used to create $\mathbb{F}_9$ have the following.

Theorem

If $k(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ *is a monic irreducible polynomial in* $\mathbb{F}_p[x]$ *then the distinct remainders obtained when dividing any polynomial* $f(x) \in \mathbb{F}_p[x]$ *by* $k(x)$,

$$F = \{a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 \mid a_i \in \mathbb{F}_p\}$$

form a field, where addition is defined as ordinary polynomial addition, and where elements of F *are multiplied in the usual way at first, but then one makes the 'substitution'* $x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 = 0$, *which means*

$$x^n = (-c_{n-1}x^{n-1} - \cdots - c_1 x - c_0)$$

Example: $k(x) = x^2 + x + 1 \in \mathbb{F}_5[x]$ is irreducible since it has no roots in $\mathbb{F}_5$.

As such, the possible remainders when dividing a polynomial in $\mathbb{F}_5[x]$ by this polynomial are *all* the polynomials of degree one or less, namely

$$F = \{ax + b \mid a, b \in \mathbb{F}_5\}$$

which means there are 5^2 elements in F, (5 choices for 'a', and 5 for 'b') where the addition is simply

$$(ax + b) + (cx + d) = (a + c)x + (b + d)$$

but the multiplication is governed by the fact that $x^2 + x + 1 = 0$ which means that $x^2 = -x - 1$.

Namely $x^2 = 4x + 4$.

So, for example

$$\begin{aligned}(2x+1)(3x+2) &= 6x^2 + 4x + 3x + 2 \\ &= x^2 + 2x + 2 \\ &= (4x+4) + 2x + 2 \\ &= 6x + 6 \\ &= x + 1\end{aligned}$$

and we can even view F as the 'span' of the polynomials $\{x, 1\}$ since $F = \{ax + b \mid a, b \in \mathbb{F}_5\}$ namely all $\mathbb{F}_5$-linear combinations of $\{x, 1\}$

And in general, if $k(x) \in \mathbb{F}_p[x]$ is irreducible, and has degree n, the resulting 'field of remainders'

$$F = \{a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 \mid a_i \in \mathbb{F}_p\}$$

is the $\mathbb{F}_p$ span of $\{x^{n-1}, x^{n-2}, \ldots, x, 1\}$.

Also, we should say something about inverses of elements in F, since we wish to demonstrate that F is a field.

We mentioned earlier that, for integers, if $gcd(x, y) = 1$ then there exists integers a, b such that $ax + by = 1$, a similar fact is true for relatively prime elements of $\mathbb{F}_p[x]$.

So for $p(x) \in F$ since $k(x)$ is irreducible and $deg(p(x)) < deg(k(x))$ then certainly $gcd(p(x), k(x)) = 1$, so this means there exists polynomials $a(x), b(x)$ such that $a(x)p(x) + b(x)k(x) = 1$.

So, since $b(x)k(x) = 0 \mod k(x)$ then $a(x)p(x) + b(x)k(x) \mod k(x)$ is $a(x)p(x)$, but $a(x)p(x) + b(x)k(x) = 1$, so $a(x)p(x) \mod k(x)$ is 1, that is $a(x)$ is the multiplicative inverse of $p(x)$ in F.

The Primitive Element Theorem

Recall that $U(\mathbb{F}_9) = \langle 2x+1 \rangle$, namely a cyclic group of order $9-1$. This is true in general.

Theorem

If F is a finite field then there exists $u \in U(F)$ such that $U(F) = \langle u \rangle$, namely a (multiplicative) cyclic group, where $|U(F)| = |F| - 1$.

The proof is given in the text, but the basic idea is that if $z \in U(F)$ then $|z| = |\langle z \rangle|$ and so, by Lagrange's theorem, $|z| \big| |U(F)| = p^n - 1$, which means z is root of $f(x) = x^{p^n-1} - 1 \in F[x]$, but since their are at most $p^n - 1$ distinct roots of $x^{p^n-1} - 1$ then the elements of $U(F)$ are exactly the same as the roots of $f(x)$. And for an abelian group this can only happen if the group is cyclic.

Such a generator u is called a primitive element for the field.

For the case of $\mathbb{Z}_p = \mathbb{F}_p$ this is of special interest in number theory.

Example $U(\mathbb{F}_{11}) = \{1, 2, 3, \ldots, 10\}$ we find that one of the generators of this cyclic group is 2, i.e. $U(\mathbb{F}_{11}) = \langle 2 \rangle$.

What frequently seems to be the case is that 2 generates $U(\mathbb{F}_p)$ for many primes p, but not all the time, for example $U(\mathbb{F}_7) = \{1, 2, 3, 4, 5, 6\} = \langle 3 \rangle$ since $3^0 = 1$, $3^1 = 3$, $3^2 = 2$, $3^3 = 6$ $3^4 = 4$, $3^5 = 5$.

This leads to the definition of the *least primitive root*, namely the smallest integer r in $\mathbb{F}_p$ such that $U(\mathbb{F}_p) = \langle r \rangle$, and as mentioned, 2 is frequently the least primitive root.

The one subtlty to this, is that there is no 'forumula' to find the primitive element, either for $\mathbb{F}_p$, nor for any finite field in general.

We can give a small table which shows this pattern:

p	r
2	1
3	2
5	2
7	3
11	2
13	2
17	3
19	2
23	5
29	2
31	3
37	2

It seems that '2' is frequently the least primitive root, but it is not known if it ever 'stops' being the least primitive root after some point.

Indeed, looking further, there are many primes for which 2 is the least primitive root:

$3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, 139, 149, 163, 173, 179,$
$181, 197, 211, 227, 269, 293, 317, 347, 349, 373, 379, 389, 419, 421, 443, 461,$
$467, 491, 509, 523, 541, 547, 557, 563, 587, 613, 619, 653, 659, 661, 677, 701, 709$

Does this sequence (A001122 on http://oeis.org) stop? Who knows?

We close out the discussion of finite fields (for now) by mentioning the following.

Theorem

For each prime p there is exactly one finite field of order (size) p^n for any $n \geq 1$, up to isomorphism.

The basic idea is that if F is a finite field, then $char(F) = p$ for some prime p and $|F| = p^n$ for some n.

Moreover, if $1 \in F$ is the multiplicative identity, then $\langle 1 \rangle = \{0 \cdot 1, 1 \cdot 1, \ldots, (p-1) \cdot 1\}$ is a 'subfield' of F with p elements, which is isomorphic to $\mathbb{F}_p$. And as mentioned above the non-zero elements of F are the roots of the polynomial $f(x) = x^{p^n - 1} - 1$ and this is true for any finite field of size p^n which means these are all isomorphic.

Notation: $\mathbb{F}_{p^n}$ or $GF(p^n)$ where the latter stands for 'Galois Field', named for Evariste Galois.