Math 75 notes, Lectures 7 and 8

P. Pollack and C. Pomerance

We begin by establishing a few elementary properties of the order of an element in an abelian group. (Note: Most of what we say is valid in any group, not necessarily abelian.)

But first a comment about notation. If we write the group operation with multiplicative notation, then $g \circ g \circ \cdots \circ g$, where there are k copies of g, is abbreviated g^k. We have the usual laws of exponents as discussed in Lecture 6. And inverses enter when we use negative exponents. But what if we are writing the group additively? Then we abbreviate $g+g+\cdots+g$, where there are k copies of g, by kg. It looks like multiplication, but we are to think of it as repeated addition (sort of the way multiplication is first introduced in elementary school!). And the laws of "exponents" now show themselves as

$$k_1(k_2 g) = k_1 k_2 g, \quad (k_1 + k_2)g = k_1 g + k_2 g.$$

By convention, we take $0g$ as the group identity of the group, usually called "0" when additive notation is used. Further, if k is a positive integer, we have $(-k)g = k(-g) = -(kg)$, and the above displayed rules continue to hold when we allow k_1, k_2 to run over all integers.

It is strange that it looks like we are doing something entirely different, but additive notation is just a different notation! Note that it is common to use multiplicative notation when talking about a generic group; eg. see Theorem 1 below.

Let's look at some examples with both additive and multiplicative notation.

1. Suppose G is the multiplicative group of the finite field $\mathbb{Z}/(7)$. Then 3 has order 6, since $3^6 \equiv 1 \pmod 7$, but no smaller positive exponent will do. In fact, in the terminology of Lecture 6, we have that 3 is a generator of the group. Indeed, if we look at 3^j for $j = 0, 1, \ldots, 5$, we get the sequence of group elements $1, 3, 2, 6, 4, 5$, which is indeed every element of the group.

2. Suppose G is the additive group $\mathbb{Z}/(6)$. Then 1 has order 6, and the sequence $j1$ for $j = 0, 1, \ldots, 5$ is $0, 1, 2, 3, 4, 5$. So this group has a generator as well.

3. Suppose G is the group $\{1, 3, 5, 7\}$ with the operation being multiplication modulo 8. (It is the group of units of the ring $\mathbb{Z}/(8)$.) Then 1 has order 1, and the other elements have order 2. This group does not have a generator.

4. Suppose G is the multiplicative group of the finite field $(\mathbb{Z}/(3))[x]/(x^2+1)$. Then $[x]$ has order 4; it is not a generator. But $[x+1]$ has order 8; it is a generator of G.

The following result is due to Lagrange. We state it in multiplicative notation.

Theorem 1. *If G is an abelian group with n elements, and $g \in G$, then $g^n = e$.*

Proof. Let a be the element of G which consists of the product of every group element. The function that sends $b \in G$ to gb is one-to-one, and therefore onto. Thus,

$$a = \prod_{b \in G} b = \prod_{b \in G} (gb) = g^n \prod_{b \in G} b = g^n a.$$

Thus, multiplying both sides of this equation by a^{-1}, we get the result. □

You should compare this general result with Theorem 3 in the Lecture 4&5 notes. There we had the exact same proof, but it was applied specifically to the multiplicative group of a finite field. Though Lagrange's theorem holds also for groups that are not necessarily abelian, the above proof does not work in the general case; do you see where we used the commutative rule for the group operation?

We also shall need the following simple consequence of the division algorithm in $\mathbb{Z}$.

Proposition 1. *If g is an element in a group with finite order m, then $g^n = e$ if and only if $m \mid n$.*

Proof. If $n = dm$ for some integer d, then $g^n = g^{dm} = (g^m)^d = e^d = e$, so one direction is done. Now assume that $g^n = e$. Write $n = dm + r$ where the remainder r satisfies $0 \leq r < m$. Then

$$e = g^n = g^{dm} g^r = e g^r = g^r,$$

so that by definition of order, we cannot have $r > 0$. Thus, $r = 0$ and we have $m \mid n$. □

If this proof looks familiar, it should! We used the same idea in proving Lemmas 1 and 2 in Lecture 6. In fact, it is possible to interpret those Lemmas in this context so that they will follow from Proposition 1. For example, in Lemma 2, we are really dealing with the group of units of the ring $\mathbb{Z}/(q^m - 1)$, and q in this group has order m. Thus, the set of integers n for which $q^n \equiv 1 \pmod{q^m - 1}$ coincides with the multiples of m.

The additive group of a finite field

Suppose F is a finite field with q elements. By Lagrange's theorem (Theorem 1), we have that when we add $1 \in F$ to itself q times, we get $0 \in F$. Let m be the order of 1 in the additive group of F, so that $m \mid q$ by Proposition 1. Suppose p is a prime factor of m, and write $m = pd$. Then, by the additive version of the rules for exponents, we have

$$0 = m1 = (pd)1.$$

But note that by the distributive rule in the field F, we have

$$(pd)1 = (p1)(d1).$$

Putting the last two equations together, we see that we have the product of two field elements being 0, so that at least one of them is 0. Thus, by Proposition 1, we have $m \mid p$ or $m \mid d$. But, $0 < d < m$, so the second possibility does not hold. But also $p \leq m$, so $m \mid p$ implies that $m = p$. We have just learned an important fact about finite fields:

Proposition 2. *In a finite field F with q elements, there is a prime $p \mid q$ with $p1 = 0$.*

This prime p, which is the additive order of 1, is called the *characteristic* of the field F. We leave it as a homework assignment to prove that if F is a field with characteristic p, then $p\alpha = 0$ for all $\alpha \in F$.

The number of elements of a finite field

We can say more: The number of elements of a finite field is either a prime number or a power of a prime number.

Theorem 2. *If F is a finite field with q elements and characteristic p, then $q = p^j$ for some positive integer j.*

Proof. We first note that the finite field $\mathbb{Z}/(p)$ can be seen to be a subfield of F. This can be worked out easily by considering the subset $\{0, 1, 2, \ldots, p-1\}$ of F (think of it as adding $1 \in F$ to itself $0, 1, \ldots, p-1$ times) and showing that the addition and multiplication of F are the same as dealing with this set as if it were $\mathbb{Z}/(p)$.

Now we appeal to the viewpoint of linear algebra! Note that F is a *vector space* with the field of scalars being $\mathbb{Z}/(p)$. You should check this by reviewing the definition of vector space and seeing that all of the rules hold. (Note that this vector space has additional algebraic structure in that we can multiply vectors; we ignore this for now.) This vector space must be finite-dimensional since it has only finitely many vectors. Say the dimension is j, so that there is a basis $\alpha_1, \alpha_2, \ldots, \alpha_j$. That is, every element $\beta \in F$ has a unique representation as

$$\beta = s_1\alpha_1 + s_2\alpha_2 + \cdots + s_j\alpha_j,$$

where the "scalars" s_i come from the subfield $\mathbb{Z}/(p)$. This then allows us to actually count the number of elements of F, since there are p choices for each s_i, and different choices for the j-tuple $(s_1, s_2, \ldots, s_j)$ lead to different elements β in F. So, there are precisely p^j elements of F. □

Using this theorem, we have the following remarkable consequence, which might be dubbed, "the binomial theorem for bad students."

Corollary 1. *If F is a finite field with charactersitic p and if $\alpha, \beta \in F$, then*

$$(\alpha + \beta)^{p^k} = \alpha^{p^k} + \beta^{p^k}$$

for every nonnegative integer k.

Proof. The result clearly holds for $k = 0$. Let us show too that it holds for $k = 1$. By the binomial theorem (for good students!), we have

$$(\alpha + \beta)^p = \alpha^p + \frac{p!}{1!(p-1)!}\alpha^{p-1}\beta + \cdots + \frac{p!}{(p-1)!1!}\alpha\beta^{p-1} + \beta^p.$$

Consider a typical coefficient of one of the middle terms. It is $p!/(l!(p-l)!)$, where $1 \leq l \leq p-1$. But p is a prime number and p divides the numerator of this fraction. Since the fraction reduces to an integer and p does not divide the denominator, by unique factorization in $\mathbb{Z}$, we have that p divides the quotient. So, a typical middle term can be written as $p\gamma$ for some field element γ. This field element is 0 (using the homework assignment dealing with characteristic), so the right side of the above displayed equation simplifies to $\alpha^p + \beta^p$, which is the corollary in the case $k = 1$. Assume the corollary holds for some $k \geq 1$, and note that we have

$$(\alpha+\beta)^{p^{k+1}} = \left((\alpha+\beta)^{p^k}\right)^p = \left(\alpha^{p^k} + \beta^{p^k}\right)^p = \alpha^{p^{k+1}} + \beta^{p^{k+1}}.$$

Thus, the corollary follows by mathematical induction. □

The qth power map

This last result can be extended easily to $(\alpha+\beta+\gamma)^{p^k}$, etc. In fact, we have the following beautiful result, which uses this idea and also the proof of Corollary 1.

Theorem 3. *Suppose F is a finite field with q elements and suppose $f(x) \in F[x]$. Then*

$$f(x)^q = f(x^q).$$

Proof. Recall from Theorem 2 that $q = p^j$ for some positive integer j, where p is the characteristic of F. Write $f(x)$ out as $c_d x^d + c_{d-1}x^{d-1} + \cdots + c_0$. By the same proof as Corollary 1 extended to sums with possibly more than 2 summands, we have

$$\begin{aligned} f(x)^q = (c_d x^d + c_{d-1}x^{d-1} + \cdots + c_0)^q &= (c_d x^d)^q + (c_{d-1}x^{d-1})^q + \cdots + c_0^q \\ &= c_d^q x^{dq} + c_{d-1}^q x^{(d-1)q} + \cdots + c_0^q. \end{aligned}$$

But from Theorem 3 in Lectures 4&5, we have that $c^q = c$ for each $c \in F$, so that this last expression simplifies to $c_d x^{dq} + c_{d-1}x^{(d-1)q} + \cdots + c_0$, which is indeed $f(x^q)$. □

Irreducible divisors of $x^{q^d} - x$

We have seen that if F is a finite field with q elements and $f(x) \in F[x]$ is irreducible of degree j, then $f(x) \mid x^{q^d} - x$ when d is a multiple of j. We are now ready to prove the converse.

Theorem 4. *Suppose that F is a finite field with q elements and $f(x)$ is an irreducible factor in $F[x]$ of $x^{q^d} - x$. Then* $\deg(f) \mid d$.

Proof. Say $\deg(f) = j$. Let K be the finite field $F[x]/(f)$, so that K has q^j elements. Consider the function τ that takes an element $\beta \in K$ and sends it to β^q. Obviously

$$\tau(\beta_1\beta_2) = (\beta_1\beta_2)^q = \beta_1^q\beta_2^q = \tau(\beta_1)\tau(\beta_2), \tag{1}$$

since multiplication is commutative. What is striking is that we also have

$$\tau(\beta_1 + \beta_2) = \tau(\beta_1) + \tau(\beta_2). \tag{2}$$

We leave this property as a homework problem. Finally note that from Theorem 3 of Lectures 4&5 we have that

$$\tau(c) = c \quad \text{for} \quad c \in F. \tag{3}$$

We conclude using the three properties (1), (2), (3) of τ, that if $g(t) \in F[t]$, then for $\beta \in K$, we have

$$\tau(g(\beta)) = g(\tau(\beta)). \tag{4}$$

Let ι denote the identity map on K and note that $\tau^j = \iota$. (The power of τ is understood as repeated applications of τ; that is, τ composed with itself j times.) Indeed, $\tau^j(\beta) = \beta^{q^j}$, so the assertion follows from Theorem 3 in Lectures 4&5. Further, the *order* of τ is exactly j. (The order is in the group of one-to-one correspondences of K under compostition—since τ composed with itself j times is the identity function, it is clear that τ is a one-to-one correspondence on K.) Indeed, if $1 \leq k < j$ and $\tau^k = \iota$, then $\beta^{q^k} = \beta$ for all $\beta \in K$. Thus the polynomial $t^{q^k} - t \in K[t]$ has $\#K = q^j$ roots. A polynomial cannot have more roots than its degree, so we cannot have $\tau^k = \iota$ for $1 \leq k < j$. This proves our assertion that the order of τ is j.

We will next show that $\tau^d = \iota$, so that the conclusion $j \mid d$ will then follow from Proposition 1 in this lecture. To see that $\tau^d = \iota$, first note that for the element $\alpha = [x]$ of K we have

$$\tau^d(\alpha) = \alpha^{q^d} = [x]^{q^d} = [x^{q^d}].$$

But by the assumption that $f(x) \mid x^{q^d} - x$, we have $[x^{q^d}] = [x]$, so we conclude that $\tau^d(\alpha) = \alpha$. Thus, τ^d acts like the identity ι on the key element $\alpha = [x]$ of K. We'll now show it acts as the identity on every element β of K.

Each element $\beta \in K$ is uniquely representable as $[c_{j-1}x^{j-1} + \cdots + c_0]$ where each $c_i \in F$ (see Theorem 4 of Lecture 2). That is, $\beta = g(\alpha)$ where $g(t) \in F[t]$ has degree $\leq j - 1$ or is 0. Thus, by applying (4) d times, we have

$$\tau^d(\beta) = \tau^d(g(\alpha)) = g(\tau^d(\alpha)) = g(\alpha) = \beta.$$

We indeed have that $\tau^d = \iota$, and the proof of the theorem is complete. □