CONSEQUENCES OF CAUCHY'S THEOREM

KEITH CONRAD

In this handout, we meet some basic consequences of Cauchy's theorem in group theory. These consequences do not depend on the proof of Cauchy's theorem, but only on the conclusion of the theorem.

1. Quick Consequences

Theorem 1.1. *For a finite group G and a prime p, $|G|$ is a power of p if and only if all elements of G have p-power order.*

What is special about prime powers for this theorem is that factors of a power of p are again powers of p.

Proof. If $|G|$ is a power of p, then the order of each element of G is a power of p since the order of each element divides the size of the group.

Conversely, assume all elements of G have p-power order. To show $|G|$ is a power of p, suppose it is not, so $|G|$ is divisible by a prime $q \neq p$. Then, by Cauchy, G has an element of order q, and that's a contradiction of our assumption. □

Theorem 1.2. *If all non-identity elements of G have the same order, this order is a prime p and $|G|$ is a power of p.*

Proof. If $|G|$ has two prime factors, say p and q, then G contains elements of orders p and q by Cauchy, which contradicts the hypothesis. Thus $|G|$ has only one prime factor, say $|G| = p^m$ for a prime p. The orders of a non-identity element could be $\{p, p^2, \ldots, p^m\}$. However, by Cauchy some $g \in G$ has order p, so the hypothesis tells us every non-identity element of G has order p. □

Example 1.3. Abelian groups fitting the hypothesis of Theorem 1.2 are easy to write down, *e.g*, $(\mathbf{Z}/(p))^n$ where p is prime. Every non-zero element has order p. For a nonabelian example, consider the Heisenberg group over $\mathbf{Z}/(p)$ when p is an odd prime. Every non-identity element has order p. Can you find a nonabelian example when $p = 2$?

Corollary 1.4. *The size of every finite field is a prime power.*

Proof. Let F be a finite field. Its size is at least 2 (since $1 \neq 0$ in F). We are going to think about F as an additive group.

Each pair of non-zero elements a and b in F (possibly equal) have the same additive order, since the function $f(x) = (b/a)x$ is additive and invertible, and f sends a to $f(a) = b$. Thus $|F|$ is a prime power by Theorem 1.2. □

Theorem 1.5. *Let G be a finite group and $k \in \mathbf{Z}$. The function $f(x) = x^k$ on G is a bijection if and only if $(k, |G|) = 1$.*

When G is nonabelian, the kth power map is usually not a homomorphism. Nevertheless, one can ask if it is a bijection or not.

Proof. Set $n = |G|$. First assume $(k, n) = 1$. Then we can solve $k\ell \equiv 1 \bmod n$. Writing $k\ell = 1 + nm$, every $x \in G$ satisfies $x^{k\ell} = xx^{nm} = x$. This shows the function $x \mapsto x^k$ on G has inverse function $x \mapsto x^\ell$, since $(x^k)^\ell = x$ and $(x^\ell)^k = x$ for $x \in G$. In particular, since the kth power map on G admits an inverse function it is a bijection. Notice we did not use Cauchy's theorem for this direction.

Now assume $(k, n) > 1$. We will show the k-th power map on G is not a bijection. Since k and n have a non-trivial common factor, they have a common prime factor, say p. Since $p \mid n$, Cauchy's theorem says G has an element of order p, say g. Then, since $p \mid k$, we have $g^k = (g^p)^{k/p} = e^{k/p} = e$. (Why does it matter that k/p is an integer?) Thus the kth power map is not a bijection, since it is not one-to-one: g and e both have kth power e. □

Example 1.6. Check that cubing on D_7 is a bijection while squaring is not, and raising to the 5-th power is a bijection on A_4.

2. Decomposing Abelian Groups

As a more involved use of Cauchy's theorem, we describe how to decompose a finite abelian group into subgroups of prime power size.

Theorem 2.1. *Let G be finite abelian with $|G| = ab$, where $(a, b) = 1$. Then G is isomorphic to a direct product $A \times B$, where $|A| = a$ and $|B| = b$.*

Proof. If either a or b is 1, the result is clear: take A or B to be the trivial group.

Since $|G| = ab$, every $g \in G$ satisfies $g^{ab} = e$. For each $m \geq 1$ the elements g satisfying $g^m = e$ form a subgroup since G is abelian. Set

$$A = \{g \in G : g^a = e\}, \quad B = \{g \in G : g^b = e\}.$$

These are both subgroups of G. (Note A is *not* the set of a-th powers in G. It is the elements whose a-th power is the identity.)

We now show $G = AB$, *i.e.*, every element of G is the product of an element of A and an element of B. By Bezout, the relative primality of a and b lets us write

$$1 = ar + bs$$

for some r and s in $\mathbf{Z}$. Therefore each $g \in G$ can be written as

$$g = g^{ar+bs} = (g^r)^a(g^s)^b.$$

Notice $(g^r)^a \in B$ since $((g^r)^a)^b = (g^r)^{ab} = e$, and similarly $(g^s)^b \in A$. Therefore, re-ordering the terms as

$$g = (g^s)^b(g^r)^a$$

expresses each $g \in G$ as the product of an element of A and an element of B, so $G = AB$.

Now we show G is isomorphic to the direct product $A \times B$. Let $f\colon A \times B \to G$ by multiplication: $f(x, y) = xy$. This is a homomorphism, since

$$f((x, y)(x', y')) = f(xx', yy') = xx'yy' = (xy)(x'y') = f(x, y)f(x', y').$$

Note we used commutativity in the third equation. The previous paragraph showed $G = AB$, so f is onto. To see f is one-to-one, we check the kernel is trivial. Suppose $f(x, y) = e$. Then $xy = e$, so $x = y^{-1}$. This equation shows x and y lie in $A \cap B$. The intersection $A \cap B$ is trivial, since every element of A has order dividing a, every element of B has order dividing b, and $(a, b) = 1$. Thus x and y are trivial, so $(x, y) = (e, e)$ is the identity element of $A \times B$. That proves f has trivial kernel.

Now that we know f is an isomorphism of $A \times B$ with G, we can show $|A| = a$ and $|B| = b$. Because f is a bijection, $|A \times B| = |G|$, so

$$|A||B| = ab. \tag{2.1}$$

We now show $(|A|, b) = 1$. For this we bring in (at last!) Cauchy's theorem. If $(|A|, b) \neq 1$ then some prime p dividing b will divide $|A|$. Then Cauchy tells us A has an element of order p. But every element of A has order dividing a, and p does not divide a (since $p \mid b$ and $(a, b) = 1$). Thus $(|A|, b) = 1$. Similarly, $(|B|, a) = 1$. From (2.1), $|A| \mid ab$, so in fact $|A| \mid a$. Arguing similarly, $|B| \mid b$. Therefore, by (2.1), $|A| = a$ and $|B| = b$. □

Corollary 2.2. *Every finite abelian group is isomorphic to a direct product of finite abelian groups with prime-power size.*

Proof. Let G be a finite abelian group, with size $n = p_1^{e_1} \cdots p_r^{e_r}$. We can suppose $n > 1$ and each e_i is non-zero. Taking $a = p_1^{e_1}$ and $b = n/a$, we have $(a, b) = 1$, so Theorem 2.1 tells us G is isomorphic to a direct product $A \times B$, where $|A| = a = p_1^{e_1}$ and $|B| = b = n/a$. Since $a > 1$, by induction on the size of the finite abelian group we can say B is isomorphic to a direct product of groups of size $p_2^{e_2}, \ldots, p_r^{e_r}$. □

3. Groups of Size pq

The rest of this handout provides a deeper use of Cauchy's theorem. We will classify all groups having size pq, where p and q are different primes. The classification, due to Netto [1, pp. 146–148], says there are at most two possibilities up to isomorphism and describes the two choices when they occur.

Theorem 3.1. *Let p and q be distinct primes, with $p < q$. If $q \not\equiv 1 \bmod p$, then all groups of size pq are cyclic. In particular, all groups of size pq are isomorphic. If $q \equiv 1 \bmod p$, then up to isomorphism there are two groups of size pq: one is cyclic and one is nonabelian.*

Example 3.2. Every group of size 15 is cyclic. Use $p = 3$ and $q = 5$, and $5 \not\equiv 1 \bmod 3$.

Example 3.3. When $p = 2$ and $q = 3$, we already know two non-isomorphic groups of size 6: $\mathbf{Z}/(6)$ and S_3. The first is cyclic and the second is not (it is non-abelian). Theorem 3.1 says every group of size 6 is isomorphic to one of these. Here is a table listing four examples each of abelian and nonabelian groups of order 6. The groups in each column are isomorphic to each other.

Abelian	Nonabelian
$\mathbf{Z}/(6)$	S_3
$\mathbf{Z}/(2) \times \mathbf{Z}/(3)$	D_3
$(\mathbf{Z}/(9))^\times$	$\mathrm{Aff}(\mathbf{Z}/(3))$
μ_6	$\mathrm{GL}_2(\mathbf{Z}/(2))$

Our proof of Theorem 3.1 will use the following lemma.

Lemma 3.4. *Let G be a group of size pq, where p and q are prime with $p < q$. There is only one subgroup of G with size q.*

Notice the hypotheses are not symmetric in p and q; the lemma is about subgroups with the larger prime order.

Proof. By Cauchy, there is a subgroup of G with size q. This subgroup has prime size and therefore is cyclic. Write it as $\langle g\rangle$.

In order to show $\langle g\rangle$ is the only subgroup with size q, assume otherwise. Then there is some $h \in G$ having order q such that $h \notin \langle g\rangle$. Then $\langle h\rangle \cap \langle g\rangle$ is trivial: this intersection is a subgroup of $\langle h\rangle$ that can't be everything (because $h \notin \langle g\rangle$), so it must be trivial because the only proper subgroup of $\langle h\rangle$ is trivial.

Consider the left cosets of $\langle g\rangle$ represented by powers of h:

$$\langle g\rangle, h\langle g\rangle, h^2\langle g\rangle, \ldots, h^{q-1}\langle g\rangle. \tag{3.1}$$

There are q cosets in this list. The total number of different left $\langle g\rangle$-cosets is $[G : \langle g\rangle] = (pq)/q = p$. Since $p < q$, two of the cosets in (3.1) must be equal, say $h^i\langle g\rangle = h^{i'}\langle g\rangle$ with $0 \leq i < i' \leq q-1$. Then $h^{i'-i} \in \langle g\rangle$, so we have a power of h other than the identity equal to a power of g. This contradicts the previous paragraph, so h can't exist. That is, every element of G with order q lies in $\langle g\rangle$, so $\langle g\rangle$ is the only subgroup with order q. □

Example 3.5. Consider the group D_5, of size 10. Here $q = 5$. There is one subgroup of size 5: the rotations.

Now we are ready to prove part of Theorem 3.1.

Theorem 3.6. *Let p, q be primes where $p < q$. Each abelian group of size pq is cyclic. If $q \not\equiv 1 \bmod p$, then each group of size pq is cyclic.*

Examples satisfying the condition $q \not\equiv 1 \bmod p$ are $15 = 3 \cdot 5$, $35 = 5 \cdot 7$, 33, 65, 77, and 95. Every group with these sizes is cyclic.

Proof. Let G be a finite group with $|G| = pq$. By Cauchy's theorem, G has an element a of order p and an element b of order q. If G is abelian then ab has order pq, so G is cyclic.

The rest of the proof is devoted to showing that, when $q \not\equiv 1 \bmod p$, a and b must commute even if we don't assume in advance that G is abelian, so again we get that ab has order pq and G is cyclic.

Write the desired condition $ab = ba$ as: $aba^{-1} = b$. This is what we will show. Since aba^{-1} is a conjugate of b, it has order q. Thus, by Lemma 3.4, aba^{-1} is a power of b, say

$$aba^{-1} = b^k$$

for some integer k. By induction, $a^m ba^{-m} = b^{k^m}$ for all $m \geq 1$. Taking $m = p$ gives

$$b = b^{k^p}.$$

Since b has order q, this equality implies $k^p \equiv 1 \bmod q$, so $k \bmod q$ has order either 1 or p in $(\mathbf{Z}/(q))^\times$, a group of size $q-1$. If the order is p, then $p \mid (q-1)$, so $q \equiv 1 \bmod p$. But $q \not\equiv 1 \bmod p$ by hypothesis (aha). Thus the order of k in $(\mathbf{Z}/(q))^\times$ is 1, so $k \equiv 1 \bmod q$ and

$$aba^{-1} = b^k = b^1 = b,$$

which means $ab = ba$. □

So far we proved Theorem 3.1 if $q \not\equiv 1 \bmod p$ and partially (*i.e.*, for abelian groups) if $q \equiv 1 \bmod p$. What about nonabelian groups of size pq for primes $p < q$ if $q \equiv 1 \bmod p$?

There is always a nonabelian group of size pq when $q \equiv 1 \bmod p$. Here is one, constructed as a subgroup of the affine group $\mathrm{Aff}(\mathbf{Z}/(q))$:

$$A_{p,q} = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \in \mathrm{Aff}(\mathbf{Z}/(q)) : x^p = 1 \text{ in } \mathbf{Z}/(q) \right\}. \tag{3.2}$$

The reader can check this is a subgroup of $\mathrm{Aff}(\mathbf{Z}/(q))$. To count its size, note there are q choices for y, since we imposed no constraints on y. How many choices are there for x? Since $x \in (\mathbf{Z}/(q))^\times$ and $p \mid (q-1)$ by hypothesis, Cauchy's theorem tells us there is an element of order p in $(\mathbf{Z}/(q))^\times$, and thus its powers give at least p solutions to $x^p = 1$ in $\mathbf{Z}/(q)$. There can be no more than p solutions (see Theorem A.1), so there are exactly p solutions. Thus, the solutions to $x^p = 1$ in $(\mathbf{Z}/(q))^\times$ are a cyclic group of size p. Therefore $|A_{p,q}| = pq$.

The group $A_{p,q}$ is nonabelian, since the matrices $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right)$ don't commute, where x is an element of order p in $(\mathbf{Z}/(q))^\times$.

Example 3.7. When $p = 3$ and $q = 7$, $q \equiv 1 \bmod p$. The solutions to $x^3 \equiv 1 \bmod 7$ are 1, 2, and 4, so a nonabelian group of order 21 is

$$A_{3,7} = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} : x = 1, 2, 4 \text{ in } \mathbf{Z}/(7), y \in \mathbf{Z}/(7) \right\}.$$

Now we are ready to complete the proof of Theorem 3.1 with an analysis of the nonabelian case when $q \equiv 1 \bmod p$.

Theorem 3.8. *Let p and q be primes with $p < q$ and $q \equiv 1 \bmod p$. Up to isomorphism, the group $A_{p,q}$ in (3.2) is the only nonabelian group of size pq.*

Proof. Let G be a nonabelian group with size pq. By Cauchy, there is $a \in G$ with order p and $b \in G$ with order q. If a and b commute, then ab has order pq, so G is cyclic. Since G is nonabelian, a and b do not commute. Since $\langle a, b\rangle$ has subgroups of size p and q, $\langle a, b\rangle$ is divisible by pq, so $\langle a, b\rangle = G$.

By Lemma 3.4 (here we use the condition $p < q$), all elements of order q in G are powers of b, so $aba^{-1} = b^t$ for some t. We have $t \not\equiv 1 \bmod q$, as otherwise $aba^{-1} = b$, which would imply $ab = ba$, but a and b do not commute.

For each $k \geq 0$, conjugating b by a a total of k times gives

$$a^k b a^{-k} = b^{t^k}. \tag{3.3}$$

Taking $k = p$, $b = b^{t^p}$, so $t^p \equiv 1 \bmod q$. Therefore t has order p in $(\mathbf{Z}/(q))^\times$. Moreover, raising both sides of (3.3) to an arbitrary integer power ℓ yields

$$a^k b^\ell a^{-k} = b^{\ell t^k},$$

so

$$a^k b^\ell = b^{\ell t^k} a^k. \tag{3.4}$$

This means each (non-negative) power of a to the left of a power of b can be placed on the right side at the cost of changing the exponent of b. Thus,

$$G = \langle a, b\rangle = \{b^n a^m : m, n \geq 0\}. \tag{3.5}$$

Now we look at the group $A_{p,q}$ in (3.2). The upper left entry of a matrix in this group is an element of $(\mathbf{Z}/(q))^\times$ with order dividing p. Because the solutions to $x^p = 1$ in $(\mathbf{Z}/(q))^\times$ form a subgroup of size p and t has order p in $(\mathbf{Z}/(q))^\times$, these solutions are exactly the powers of t. Therefore each matrix in $A_{p,q}$ has the following form, where $m, n \geq 0$:

$$\begin{aligned} \begin{pmatrix} t^m & n \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t^m & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix}^m. \end{aligned}$$

This suggests, since $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ has order q (like b) and $\left(\begin{smallmatrix} t & 0 \\ 0 & 1 \end{smallmatrix}\right)$ has order p (like a), the following function $f\colon A_{p,q} \to G$:

$$f\left(\begin{array}{cc} t^m & n \\ 0 & 1 \end{array}\right) = b^n a^m.$$

This function f is well-defined, since m and n in $\left(\begin{smallmatrix} t^m & n \\ 0 & 1 \end{smallmatrix}\right)$ only matter modulo p and q, respectively.

To check f is an isomorphism, we must show it is a homomorphism ($f(AB) = f(A)f(B)$ for all A and B in $A_{p,q}$), one-to-one, and onto.

For the homomorphism property, pick $A = \left(\begin{smallmatrix} t^m & n \\ 0 & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} t^{m'} & n' \\ 0 & 1 \end{smallmatrix}\right)$ in $A_{p,q}$. Then

$$\begin{aligned} f(AB) &= f\left(\left(\begin{array}{cc} t^m & n \\ 0 & 1 \end{array}\right)\left(\begin{array}{cc} t^{m'} & n' \\ 0 & 1 \end{array}\right)\right) \\ &= f\left(\begin{array}{cc} t^{m+m'} & t^m n' + n \\ 0 & 1 \end{array}\right) \\ &= b^{t^m n' + n} a^{m+m'} \\ &= b^n b^{t^m n'} a^m a^{m'} \\ &= b^n a^m b^{n'} a^{m'} \quad \text{by (3.4)} \\ &= f(A)f(B). \end{aligned}$$

The reason f is onto is (3.5), which shows every element of G is a value of f.

That $f\colon A_{p,q} \to G$ is one-to-one is now automatic since f is onto and $|A_{p,q}| = |G|$. So there is nothing more we need to do, but for the sake of illustrating technique we will check f is one-to-one directly by showing its kernel is trivial. If $f\left(\begin{smallmatrix} t^m & n \\ 0 & 1 \end{smallmatrix}\right) = 1$ then $b^n a^m = 1$, so

$$a^m = b^{-n} \in \langle a \rangle \cap \langle b \rangle.$$

This intersection is trivial since $\langle a \rangle$ and $\langle b \rangle$ are nontrivial groups whose sizes are relatively prime, so $a^m = 1$ and $b^n = 1$. Thus $p \mid m$ and $q \mid n$, so $\left(\begin{smallmatrix} t^m & n \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, which shows f has a trivial kernel. □

Corollary 3.9. *For odd primes q, each group of order $2q$ is either cyclic or dihedral: it is isomorphic to $\mathbf{Z}/(2q)$ or to D_q.*

Proof. Taking $p = 2$ in Theorem 3.8, the subgroup $A_{p,q}$ of $\mathrm{Aff}(\mathbf{Z}/(q))$ is one of the matrix models for D_q. □

Remark 3.10. When $p = q$, groups of order $pq = p^2$ can be classified up to isomorphism and as in Theorem 3.1 there are two such groups, but both are abelian: one is cyclic and the other is $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$.

Remark 3.11. Recalling the definition $D_2 = \mathbf{Z}/(2) \times \mathbf{Z}/(2)$, Corollary 3.9 is true at $q = 2$ since each group of order 4 is isomorphic to $\mathbf{Z}/(4)$ or $\mathbf{Z}/(2) \times \mathbf{Z}/(2)$. So Corollary 3.9 is valid for all primes q.

Appendix A. Root Counting

We prove here a result on polynomials used to count the size of the group $A_{p,q}$ in (3.2).

Theorem A.1. *Let $f(x)$ be a non-constant polynomial with coefficients in $\mathbf{Z}/(p)$, of degree d. Then $f(x)$ has at most d roots in $\mathbf{Z}/(p)$.*

To prove Theorem A.1, we use a lemma connecting roots and linear factors.

Lemma A.2. *Let $f(x)$ be a non-constant polynomial with coefficients in $\mathbf{Z}/(p)$. For a in $\mathbf{Z}/(p)$, $f(a) = 0$ if and only if $x - a$ is a factor of $f(x)$.*

Example A.3. When the coefficients are $\mathbf{Z}/(5)$ the polynomial $f(x) = x^3 - 2$ has $f(3) = 0$ and $x^3 - 2 = (x - 3)(x^2 + 3x - 1)$.

Proof. If $x - a$ is a factor of $f(x)$, then $f(x) = (x - a)h(x)$. Substituting a for x shows $f(a) = 0$.

Conversely, suppose $f(a) = 0$. Write the polynomial as

$$f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0, \tag{A.1}$$

where $c_j \in \mathbf{Z}/(p)$ and $c_n \neq 0$. Then

$$0 = c_n a^n + c_{n-1}a^{n-1} + \cdots + c_1 a + c_0. \tag{A.2}$$

Subtracting (A.2) from (A.1), the terms c_0 cancel and we get

$$f(x) = c_n(x^n - a^n) + c_{n-1}(x^{n-1} - a^{n-1}) + \cdots + c_1(x - a). \tag{A.3}$$

Since

$$x^j - a^j = (x - a)(x^{j-1} + ax^{j-2} + \cdots + a^i x^{j-1-i} + \cdots + a^{j-2}x + a^{j-1}),$$

each term on the right side of (A.3) has an $x - a$ in it. Factor it out of each term in (A.3) and obtain $f(x) = (x - a)g(x)$ where $g(x)$ is a polynomial with coefficients in $\mathbf{Z}/(p)$. □

Now we prove Theorem A.1.

Proof. We induct on the degree d of $f(x)$. Note $d \geq 1$.

A polynomial of degree 1 has the form $f(x) = ax + b$, where a and b are in $\mathbf{Z}/(p)$ and $a \neq 0$. This has exactly one root in $\mathbf{Z}/(p)$, namely $-b/a$, and thus *at most* one root in $\mathbf{Z}/(p)$. That settles the theorem for $d = 1$.

Now assume the theorem is true for all polynomials with coefficients in $\mathbf{Z}/(p)$ of degree d. We verify the theorem for all polynomials with coefficients in $\mathbf{Z}/(p)$ of degree $d + 1$.

A polynomial of degree $d + 1$ is

$$f(x) = c_{d+1}x^{d+1} + c_d x^d + \cdots + c_1 x + c_0, \tag{A.4}$$

where $c_j \in \mathbf{Z}/(p)$ and $c_{d+1} \neq 0$. If $f(x)$ has no roots in $\mathbf{Z}/(p)$, then we're done, since $0 \leq d + 1$. If $f(x)$ has a root in $\mathbf{Z}/(p)$, say r, then Lemma A.2 tells us $f(x) = (x - r)g(x)$, where $g(x)$ is a polynomial with coefficients in $\mathbf{Z}/(p)$ of degree d. We can therefore apply the inductive hypothesis to $g(x)$ and conclude that $g(x)$ has at most d roots in $\mathbf{Z}/(p)$. Since $f(a) = (a - r)g(a)$ for all $a \in \mathbf{Z}/(p)$ and a product of numbers in $\mathbf{Z}/(p)$ is 0 only when one of the factors is 0 (this would be *false* if our modulus were composite rather than prime!), we see that each root of $f(x)$ in $\mathbf{Z}/(p)$ is either r or is a root of $g(x)$. Thus, $f(x)$ has at most $d + 1$ roots in $\mathbf{Z}/(p)$. As $f(x)$ was an arbitrary polynomial of degree $d + 1$ with coefficients in $\mathbf{Z}/(p)$, we are done with the inductive step. □

References

[1] E. Netto, *The Theory of Substitutions and its Applications to Algebra*, Register Publ. Co., Ann Arbor, 1892. Online at https://archive.org/details/theoryofsubstitu00nett/page/146.