Module MA3411: Abstract Algebra
Galois Theory
Appendix
Michaelmas Term 2013

D. R. Wilkins

Copyright © David R. Wilkins 1997–2013

Contents

A Cyclotomic Polynomials

A.1 Minimum Polynomials of Roots of Unity

Proposition A.1 *If a monic polynomial with integer coefficients factors as a product of monic polynomials with rational coefficients, then those polynomials have integer coefficients.*

Proof Let $f(x)$ be a monic polynomial with integer coefficients, and suppose that $f(x) = f_1(x)f_2(x)\cdots f_r(x)$, where $f_1, f_2, \ldots, f_r$ are monic polynomials with rational coefficients. Then there exist unique rational numbers $a_1, a_2, \ldots, a_r$ such that the polynomial $a_j f_j(x)$ is a primitive polynomial with integer coefficients for $j = 1, 2, \ldots, r$. Moreover each rational number a_j must be an integer, because it is the leading coefficient of a polynomial $a_j f_j(x)$ whose coefficients are integers. Now Gauss's Lemma (Lemma 3.7) ensures that a product of primitive polynomials with integer coefficients is itself a primitive polynomial. Therefore the polynomial

$$a_1 a_2 \cdots a_r f_1(x) f_2(x) \cdots f_r(x)$$

is a primitive polynomial with integer coefficients, and therefore its coefficients are not all divisible by any integer greater than one. Thus $a_1 a_2 \cdots a_r = 1$, and therefore $a_j = \pm 1$ for $j = 1, 2, \ldots, r$. This then ensures that each factor $f_j(x)$ of $f(x)$ has integer coefficients, as required. ∎

Corollary A.2 *Let $f(x)$ be a monic polynomial with integer coefficients. Then the minimum polynomial of every root of $f(x)$ over the field $\mathbb{Q}$ of rational numbers has integer coefficients.*

Proof If $m(x)$ is the minimum polynomial over $\mathbb{Q}$ of some root of $f(x)$ then $f(x) = m(x)g(x)$ for some monic polynomial $g(x)$ with rational coefficients. It then follows from Proposition A.1 that the polynomials $m(x)$ and $g(x)$ have integer coefficients. ∎

Let p be a prime number, let $\mathbb{F}_p$ be the field of congruence classes of integers modulo p, and let $\nu_p \colon \mathbb{Z} \to \mathbb{F}_p$ be the ring homomorphism that sends each integer k to its congruence class $[k]_p$ modulo p. Then each polynomial f with integer coefficients determines a corresponding polynomial $\nu_{p*}f$ with coefficients in $\mathbb{F}_p$, where

$$\nu_{p*}(a_0 + a_1 x + a_2 x^2 + \cdots a_n x^n) = [a_0]_p + [a_1]_p x + [a_2]_p x^2 + \cdots + [a_n]_p x^n.$$

for all polynomials $a_0 + a_1 x + a_2 x^2 + \cdots a_n x^n$ with integer coefficients. The polynomial $\nu_{p*}f$ is thus obtained from the polynomial f by replacing each

coefficient of $f(x)$ by its congruence class modulo p. The function $\nu_p\colon \mathbb{Z}[x] \to \mathbb{F}_p[x]$ is a ring homomorphism.

Corollary A.3 *Let p be a prime number, and let $\nu_p\colon \mathbb{Z} \to \mathbb{F}_p$ be the ring homomorphism from the ring $\mathbb{Z}$ of integers to the field $\mathbb{F}_p$ of congruence classes of integers modulo p that sends each integer k to its congruence class $[k]_p$ modulo p. Let f and g be monic polynomials with integer coefficients and let $\nu_{p*}f$ and $\nu_{p*}g$ be the polynomials obtained on replacing the coefficients of $f(x)$ and $g(x)$ by their congruence classes modulo p. Suppose that f divides g in the polynomial ring $\mathbb{Q}(x)$. Then $\nu_{p*}f$ divides $\nu_{p*}g$ in $\mathbb{F}_p(x)$.*

Proof The polynomial f divides the polynomial g in the polynomial ring $\mathbb{Q}[x]$, and therefore there exists some monic polynomial $h(x)$ with rational coefficients such that $g(x) = f(x)h(x)$. But Proposition A.1 then ensures that the monic polynomial $h(x)$ has integer coefficients. It follows that $(\nu_{p*}f)(x) = (\nu_{p*}g)(x)(\nu_{p*}h)(x)$, and thus $\nu_{p*}f$ divides $\nu_{p*}g$ in $\mathbb{F}_p[x]$. ∎

Lemma A.4 *Let p be a prime number, and let $u(x)$ be a polynomial with coefficients in the field $\mathbb{F}_p$ of congruence classes of integers modulo p. Then $u(x^p) = u(x)^p$.*

Proof The Commutative, Associative and Distributive Laws satisfied in any commutative ring ensure that

$$(u_1(x) + u_2(x))^p = \sum_{j=0}^{p} \binom{p}{j} (u_1(x))^{p-j}(u_2(x))^j = (u_1(x))^p + (u_2(x))^p$$

for all polynomials u_1 and u_2 with coefficients in the field $\mathbb{F}_p$, because the binomial coefficient $\binom{p}{j}$ is divisible by p when $0 < j < p$ (see the proof of Lemma 6.10). It follows by induction on r that $\left(\sum_{j=1}^{r} u_j(x)\right)^p = \sum_{j=1}^{r} (u_j(x))^p$ for all polynomials $u_1, u_2, \ldots, u_r$ with coefficients in $\mathbb{F}_p$. Also $c^p = c$ for all $c \in \mathbb{F}_p$, because Fermat's Little Theorem ensures that $k^p \equiv k$ modulo p for all integers k. Let

$$u(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n^p x^n,$$

where $c_0, c_1, \ldots, c_n \in \mathbb{F}_p$. Then

$$\begin{aligned}(u(x))^p &= c_0^p + c_1^p x^p + c_2^p x^{2p} + \cdots + c_n^p x^{np} \\ &= c_0 + c_1 x^p + c_2 x^{2p} + \cdots + c_n x^{np} \\ &= u(x^p),\end{aligned}$$

as required. ∎

Proposition A.5 *Let m be a positive integer, let p be a prime number that does not divide m, and let ξ be a complex number satisfying $x^m = 1$. Then the numbers ξ and ξ^p have the same minimum polynomial over the field $\mathbb{Q}$ of rational numbers.*

Proof Let $f(x)$ and $g(x)$ be the minimum polynomials of ξ and ξ^p respectively over the field $\mathbb{Q}$ of rational numbers. The complex numbers are roots of the polynomial $x^m - 1$. It follows from Corollary A.2 that the monic polynomials $f(x)$ and $g(x)$ have integer coefficients. Moreover $g(\xi^p) = 0$, and thus ξ is a root of the polynomial $g(x^p)$. It follows that the minimum polynomial $f(x)$ of ξ divides $g(x^p)$ in $\mathbb{Q}[x]$. Corollary A.2 then ensures that $f(x)$ divides $g(x^p)$ in $\mathbb{Z}[x]$. We aim to show that $f(x) = g(x)$.

Let $\mathbb{F}_p$ be the field of congruence classes of integers modulo p, let $\nu_p \colon \mathbb{Z} \to \mathbb{F}_p$ be the ring homomorphism that sends each integer k to its congruence class $[k]_p$ modulo p, and let $\overline{f}(x)$ and $\overline{g}(x)$ be the polynomials with coefficients in $\mathbb{F}_p$ obtained from the polynomials $f(x)$ and $g(x)$ respectively by replacing each coefficient of those polynomials by its congruence class modulo p, so that $\overline{f} = \nu_{p*} f$ and $\overline{g} = \nu_{p*} g$. Then $\overline{f}(x)$ divides $\overline{g}(x^p)$, because $f(x)$ divides $g(x^p)$. But $\overline{g}(x^p) = \overline{g}(x)^p$, by Lemma A.4. Thus $\overline{f}(x)$ divides $\overline{g}(x)^p$. It follows that all irreducible factors of $\overline{f}(x)$ in $\mathbb{F}_p[x]$ divide $\overline{g}(x)^p$ and are thus irreducible factors of $\overline{g}(x)$.

Suppose that it were the case that $f \neq g$. Then the polynomial $x^m - 1$ would be divisible by $f(x)g(x)$, and therefore the corresponding polynomial $x^m - [1]_p$ in $\mathbb{F}_p[x]$ would be divisible by $\overline{f}(x)\overline{g}(x)$. But we have shown that each irreducible factor of $\overline{f}(x)$ is also a factor of $\overline{g}(x)$. Thus, given any irreducible factor $v(x)$ of $\overline{f}(x)$, its square $v(x)^2$ would divide $x^m - [1]_p$ in $\mathbb{F}_p[x]$. Thus there would exist some polynomial $w \in \mathbb{F}_p[x]$ with coefficients in $\mathbb{F}_p$ such that $x^m - [1]_p = v(x)^2 w(x)$. But calculating the formal derivative in $\mathbb{F}_p[x]$ of both sides of this identity shows that

$$\begin{aligned} [m]_p x^{m-1} &= m.[1]_p x^{m-1} = D(x^m - [1]_p) = D(v(x)^2 w(x)) \\ &= 2v(x)(Dv)(x)w(x) + v(x)^2 (Dw)(x), \end{aligned}$$

and moreover $[m]_p \neq [0]_p$, because the prime number p does not divide m. It would therefore follow that the irreducible polynomial $v(x)$ would divide x^{m-1}, and would therefore divide x. But this is impossible, because $[0]_p$ is not a root of $x^m - [1]_p$ and thus could not be a root of $v(x)$. Thus the hypothesis that $f \neq g$ leads to a contradiction. Therefore $f = g$, as required. ∎

A.2 Cyclotomic Polynomials and Cyclotomic Fields

Let m be a positive integer. A complex number z is an mth *root of unity* if $z^m = 1$. It is a *primitive* mth *root of unity* if m is the smallest positive integer for which $z^m = 1$.

Definition The mth *cyclotomic polynomial* $\Phi_m(x)$ is the monic polynomial whose roots are the primitive mth roots of unity.

Now ω_m is a primitive mth root of unity, where $\omega_m = e^{2\pi\sqrt{-1}/m}$. Moreover ω^a is a primitive mth root of unity if and only if the integer a is coprime to m. Indeed an integer j satisfies $\omega^{ja} = 1$ if and only if ja is divisible by m. If a is coprime to m then ja is divisible by m if and only if j is itself divisible by m, and therefore ω^a is a primitive mth root of unity. On the other hand if the greatest common divisor (a, m) of a and m is greater than 1, then $\omega^{da} = 1$ where $d = m/(a, m) < m$ and therefore ω^a is not a primitive mth root of unity. Thus

$$\Phi_m(x) = \prod_{\substack{0 \le a < m \\ (a,m)=1}} (x - \omega_m^a) = \prod_{\substack{0 \le a < m \\ (a,m)=1}} (x - e^{2\pi\sqrt{-1}\,a/m}),$$

i.e., Φ_m is the product of the polynomials $x - \omega_m^a$ taken over all integers a satisfying $0 \le a < m$ that are coprime to m.

Definition The mth *cyclotomic field* is the field obtained by adjoining the mth roots of unity to the field $\mathbb{Q}$ of rational numbers.

Now the field $\mathbb{Q}(\omega_m)$ contains all mth roots of unity, because those primitive mth roots of unity are powers of ω_m. It follows that the field $\mathbb{Q}(\omega_m)$ is the mth cyclotomic field.

Now each mth root of unity is a primitive dth root of unity for some divisor d of m. It follows that

$$x^m - 1 = \prod_{d|m} \Phi_d(x),$$

where the product of the cyclotomic polynomials $\Phi_d(x)$ is taken over all divisors d of m.

The *Euler Totient Function* φ is the function on the positive integers whose value at each positive integer m is the number of non-negative integers less than m that are coprime to m. This function satisfies the identity $\sum_{d|m} \varphi(d) = m$ for all positive integers m, where the sum is taken over the divisors d of m (see Lemma 6.13).

Theorem A.6 *For each positive integer m, the mth cyclotomic polynomial $\Phi_m(x)$ is a monic irreducible polynomial of degree $\varphi(m)$ with integer coefficients, where $\varphi(m)$ denotes the number of non-negative integers less than m that are coprime to m. Moreover the mth cyclotomic field $\mathbb{Q}(e^{2\pi\sqrt{-1}/m})$ is a finite extension of $\mathbb{Q}$ of degree $\varphi(m)$.*

Proof The image of any primitive mth root of unity under an automorphism of $\mathbb{Q}(\omega_m)$ must itself be a primitive mth root of unity. It follows that the Galois group $\Gamma(\mathbb{Q}(\omega_m)\colon\mathbb{Q})$ of the Galois extension $\mathbb{Q}(\omega_m)\colon\mathbb{Q}$ permutes the primitive mth roots of unity amongst themselves, and therefore permutes the factors $x - \omega_m^a$ of the cyclotomic polynomial $\Phi_m(x)$ amongst themselves. It follows that the coefficients of the cyclic polynomial $\Phi_m(x)$ are in the fixed field of the Galois group $\Gamma(\mathbb{Q}(\omega_m)\colon\mathbb{Q})$. This fixed field is the field $\mathbb{Q}$ of rational numbers (Theorem 6.21). Thus the cyclotomic polynomial $\Phi_m(x) \in \mathbb{Q}(x)$ is a polynomial of degree $\varphi(d)$ with rational coefficients.

Now the monic polynomial $x^m - 1$ is the product of the cyclotomic polynomials $\Phi_d(x)$, where this product is taken over all divisors d of m. Moreover each of these cyclotomic polynomials is a monic polynomial with rational coefficients. It therefore follows from Proposition A.1 that each of the factors of $x^m - 1$ has integer coefficients. Thus each cyclotomic polynomial $\Phi_m(x)$ has integer coefficients.

Each integer a coprime to m factors as a product $p_1 p_2 \cdots p_k$ of prime numbers that do not divide m. It follows from successive applications of Proposition A.5 that ω_m, $\omega_m^{p_1}$, $\omega_m^{p_1 p_2}$, …, $\omega_m^{p_1 p_2 \cdots p_k}$ share the same minimum polynomial over the field of rational numbers. It follows that the cyclotomic polynomial $\Phi_m(x)$ is the minimum polynomial of each of its roots and is thus irreducible.

The mth cyclotomic field is the field $\mathbb{Q}(\omega_m)$ obtained by adjoining the complex number ω_m to the field $\mathbb{Q}$ of rational numbers. Moreover the cyclotomic polynomial $\Phi_m(x)$ is the minimum polynomial of ω_m over the field $\mathbb{Q}$ of rational numbers. It follows from Theorem 4.5 that

$$[\mathbb{Q}(\omega_m)\colon\mathbb{Q}] = \deg \Phi_m = \varphi(m),$$

as required. ∎

If m is a prime number then all mth roots of unity with the exception of the number 1 itself are primitive mth roots of unity, and therefore

$$\Phi_m(x) = \frac{x^m - 1}{x - 1} = \sum_{j=0}^{m-1} x^j \quad \text{(provided that } m \text{ is prime)}$$

A.3 Examples of Cyclotomic Polynomials

We now list the first eight cyclotomic polynomials:

$$\begin{aligned}
\Phi_1(x) &= x-1,\\
\Phi_2(x) &= x+1,\\
\Phi_3(x) &= (x-\omega_3)(x-\omega_3^2) = x^2+x+1,\\
\Phi_4(x) &= (x-\sqrt{-1})(x+\sqrt{-1}) = x^2+1,\\
\Phi_5(x) &= x^4+x^3+x^2+x+1,\\
\Phi_6(x) &= (x-\omega_6)(x-\omega_6^5) = x^2-x+1,\\
\Phi_7(x) &= x^6+x^5+x^4+x^3+x^2+x+1,\\
\Phi_8(x) &= (x-\omega_8)(x-\omega_8^3)(x-\omega_8^5)(x-\omega_8^7) = x^4+1.
\end{aligned}$$

Example We calculate $\Phi_8(x)$. Now

$$\begin{aligned}
\omega_8 e^{2\pi\sqrt{-1}/8} &= (1+i)/\sqrt{2},\\
\omega_8^3 e^{2\pi\sqrt{-1}/8} &= (-1+i)/\sqrt{2},
\end{aligned}$$

where $i=\sqrt{-1}$. Moreover $\omega - 8^4 = -1$. It follows that

$$\begin{aligned}
\Phi_8(x) &= (x-\omega_8)(x-\omega_8^3)(x-\omega_8^5)(x-\omega_8^7)\\
&= \left(x-\frac{1+i}{\sqrt{2}}\right)\left(x-\frac{-1+i}{\sqrt{2}}\right)\left(x+\frac{1+i}{\sqrt{2}}\right)\left(x+\frac{-1+i}{\sqrt{2}}\right)\\
&= \left(x^2-\frac{(1+i)^2}{2}\right)\left(x^2-\frac{(-1+i)^2}{2}\right) = (x^2-i)(x^2+i)\\
&= x^4+1.
\end{aligned}$$

A direct calculation shows that

$$\begin{aligned}
\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) &= (x-1)(x+1)(x^2+x+1)(x^2-x+1)\\
&= (x^2-1)((x^2+1)^2-x^2)\\
&= (x^2-1)(x^4+x^2+1)\\
&= x^6-1.
\end{aligned}$$

This verifies that x^6-1 is indeed the product of the cyclotomic polynomials $\Phi_d(x)$ taken over all divisors d of 6.

A.4 Cyclotomic Fields and Constructibility of Regular Polygons

Let $\mathbb{K}$ denote the set of all real numbers x for which the point $(x, 0)$ is constructible from the points $(0, 0)$ and $(0, 1)$ by means of a geometrical construction using straightedge and compasses alone. Then $\mathbb{K}$ is a subfield of the field of real numbers, and a point (u, v) of the plane is constructible using straightedge and compass alone if and only if $u \in \mathbb{K}$ and $v \in \mathbb{K}$. Moreover if $u \in \mathbb{K}$ and $u > 0$ then $\sqrt{u} \in \mathbb{K}$. (These results follow from Theorem 5.3.) Moreover if $u \in \mathbb{K}$ then $[\mathbb{Q}(u) : \mathbb{Q}] = 2^r$ for some non-negative integer r (Theorem 5.7).

Suppose that a constructible point (u, v) lies on the unit circle, so that $u^2 + v^2 = 1$. Then $[\mathbb{Q}(u, v, \sqrt{-1}) : \mathbb{Q}(u)]$ is equal to 1, 2 or 4, because $v^2 = 1 - u^2$ and therefore $[\mathbb{Q}(u + iv) : \mathbb{Q}]$ is a power of 2. Now a regular m-sided polygon inscribed in the unit circle is constructible if and only if the point $(\cos(2\pi/m), \sin(2\pi/m))$ is constructible. It follows that if this regular m-sided polygon is constructible then $[\mathbb{Q}(e^{2\pi\sqrt{-1}/m}) : \mathbb{Q}] = 2^r$ for some non-negative integer r, and thus $\varphi(m) = 2^r$ for some integer r, where φ denotes the Euler Totient Function.

Suppose that $m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ where $p_1, p_2, \ldots, p_k$ are distinct prime numbers and $r_1, r_2, \ldots, r_k$ are positive integers. It follows from well-known results of elementary number theory that

$$\varphi(m) = p_1^{r_1 - 1}(p_1 - 1) p_2^{r_2 - 1}(p_2 - 1) \cdots p_r^{r_k - 1}(p_k - 1).$$

Thus $\varphi(m)$ is a power of 2 if and only if $r_j = 1$ and $p_j - 1$ is a power of two whenever the prime p_j is odd. Moreover if $p_j - 1 = 2^t$ for some integer t then t cannot have any odd divisors, because the polynomial $x + 1$ divides $x^n + 1$ for all odd positive integers n and therefore $2^s + 1$ divides $2^{ns} + 1$ for all odd positive integers n and positive integers s. Thus if $p_j - 1$ is a power of 2 then p_j must be of the form $2^{2^{n_j}} + 1$ for some non-negative integer n_j. Prime numbers of this form are known as *Fermat primes*. We conclude that a positive integer m satisfies $\varphi(m) = 2^r$ for some non-negative integer r if and only if either m is a power of 2 or else m is a power of 2 multiplied by a product of distinct Fermat primes.

The five known Fermat primes are 3, 5, 17, 257 and 65537.

The theory of straightedge and compass constructions thus shows that if an m-sided regular polygon is constructible using straightedge and compasses then $[\mathbb{Q}(\omega_m) : \mathbb{Q}]$ must be a power of 2. The converse result is also true.

Indeed suppose that $[\mathbb{Q}(\omega_m) : \mathbb{Q}]$ is a power of 2. The splitting field extension $\mathbb{Q}(\omega_m) : \mathbb{Q}$ is a Galois extension, and therefore its Galois group

$\Gamma(\mathbb{Q}(\omega_m)\colon\mathbb{Q})$ is a finite group whose order is 2^r for some integer r. A standard result of group theory then ensures that the Galois group $\Gamma(\mathbb{Q}(\omega_m)\colon\mathbb{Q})$ has subgroups $H_0, H_1, \ldots, H_r$, where $|H_j| = 2^{r-j}$ for $j = 0, 1, \ldots, r$ and H_j is a normal subgroup of H_{j-1} for $j = 1, 2, \ldots, r$. (This result is a special case of Corollary A.9 below.) Let the subfield L_j of $\mathbb{Q}(\omega_m)$ be the fixed field of H_j for $j = 0, 1, \ldots, r$. It then follows from the Galois Correspondence (see Theorem 6.25) that $[L_j\colon\mathbb{Q}] = 2^j$ for $j = 0, 1, \ldots, r$ and $L_{j-1} \subset L_j$ for $j = 1, 2, \ldots, r$. Then $[L_j\colon L_{j-1}] = 2$, and therefore $L_j = L_{j-1}(\alpha_j)$ for some element α_j satisfying $\alpha_j^2 \in L_{j-1}$. Let $\mathbb{K}$ be the subfield of $\mathbb{R}$ consisting of those real numbers u for which the point $(u, 0)$ is constructible. Then $\sqrt{u} \in \mathbb{K}$ for all $u \in K$. It follows that that if $L_{j-1} \subset \mathbb{K}(\sqrt{-1})$ then the real and imaginary parts of α_j belong to $\mathbb{K}$, and therefore $L_j \subset \mathbb{K}(\sqrt{-1})$. We conclude from this that $\mathbb{Q}(\omega_m) \subset \mathbb{K}(\sqrt{-1})$, and thus the real and imaginary parts of each element of $\mathbb{Q}(\omega_m)$ are the Cartesian coordinates of a constructible point in the Euclidean plane.

We conclude therefore that if $\varphi(m)$ is a power of 2 then a regular m-sided polygon inscribed in the unit circle is constructible using straightedge and compasses.

We now discuss the results from group theory that ensure that any finite group whose order is a power of 2 contains a finite sequence of subgroups, where each proper subgroup in the sequence is a normal subgroup of the preceding group in the sequence whose order is half that of the preceding subgroup. These results are special cases of results that apply to any finite group whose order is a power of a prime number.

A.5 Groups whose Order is a Prime Power

Definition Let p be a prime number. A *p-group* is a finite group whose order is some power p^k of p.

Lemma A.7 *Let p be a prime number, and let G be a p-group. Then there exists a normal subgroup of G of order p that is contained in the centre of G.*

Proof Let $|G| = p^k$. Then p^k divides the order of G but does not divide the order of any proper subgroup of G. It follows from Proposition 8.2 that p divides the order of the centre of G. It then follows from Cauchy's Theorem (Theorem 8.3) that the centre of G contains some element of order p. This element generates a cyclic subgroup of order p, and this subgroup is normal since its elements commute with every element of G. ∎

Proposition A.8 *Let G be a p-group, where p is some prime number, and let H be a proper subgroup of G. Then there exists some subgroup K of G such that $H \triangleleft K$ and K/H is a cyclic group of order p.*

Proof We prove the result by induction on the order of G. Thus suppose that the result holds for all p-groups whose order is less than that of G. Let Z be the centre of G. Then ZH is a well-defined subgroup of G, since Z is a normal subgroup of G.

Suppose that $ZH \neq H$. Then H is a normal subgroup of ZH. The quotient group ZH/H is a p-group, and contains a subgroup K_1 of order p (Lemma A.7). Let $K = \{g \in ZH : gH \in K_1\}$. Then $H \triangleleft K$ and $K/H \cong K_1$, and therefore K is the required subgroup of G.

Finally suppose that $ZH = H$. Then $Z \subset H$. Let $H_1 = \{hZ : h \in H\}$. Then H_1 is a subgroup of G/Z. But G/Z is a p-group, and $|G/Z| < |G|$, since $|Z| \geq p$ (Lemma A.7). The induction hypothesis ensures the existence of a subgroup K_1 of G/Z such that $H_1 \triangleleft K_1$ and K_1/H_1 is cyclic of order p. Let $K = \{g \in G : gZ \in K_1\}$. Then $H \triangleleft K$ and $K/H \cong K_1/H_1$. Thus K is the required subgroup of G. ∎

Repeated applications of Proposition A.8 yield the following result.

Corollary A.9 *Let G be a finite group whose order is a power of some prime number p. Then there exist subgroups $G_0, G_1, \ldots, G_n$ of G, where G_0 is the trivial subgroup and $G_n = G$, such that $G_{i-1} \triangleleft G_i$ and G_i/G_{i-1} is a cyclic group of order p for $i = 1, 2, \ldots, n$.*