Chapter 10

Dave

May 8, 2015

1 Composition Series and Solvable Groups

1. (a) If $n = 1$, then our group has prime order, so it's $\mathbb{Z}_p$, which is simple so it has the required composition series. If the hypothesis holds for all values of n up to $k-1$, then a group G of order p^k has a subgroup pG of order p^{k-1}, and pG is normal since for $x, y \in G, y(px)y^{-1} = p(yxy^{-1}) \in pG$, and $G/pG \cong \mathbb{Z}_p$ which is simple, so $\{1\} \subset \ldots \subset pG \subset G$ is a composition series for G in which successive quotients are $\mathbb{Z}_p$.

   (b) The primary decomposition of a finite abelian group gives $M \cong \oplus_i M[p_i]$, where $M[p_i]$ has order p_i^k for some $k \in \mathbb{N}$ and is normal in M. By part a, each of these $M[p_i]$ has a decomposition series where successive quotients are cyclic of prime order, $\{1\} \subset M[p_i]_1 \subset M[p_i]_2 \subset \ldots \subset M[p_i]$. So $\oplus_i\{1\} \subset M[p_1]_1 \oplus (\oplus_{i>1}\{1\}) \subset M[p_1]_2 \oplus (\oplus_{i>1}\{1\}) \subset \ldots \subset M[p_1] \oplus (\oplus_{i>1}\{1\}) \subset M[p_1] \oplus M[p_2]_1 \oplus (\oplus_{i>2}\{1\}) \subset \ldots \subset M[p_1] \oplus M[p_2] \oplus (\oplus_{i>2}\{1\}) \subset \ldots \subset \oplus_i M[p_i]$ is a composition series for M in which successive quotients are cyclic of prime order.

2. Three composition series of $\mathbb{Z}_{45}$ are $1 \subset \mathbb{Z}_3 \subset \mathbb{Z}_9 \subset \mathbb{Z}_{45}, 1 \subset \mathbb{Z}_5 \subset \mathbb{Z}_{15} \subset \mathbb{Z}_{45}$, and $1 \subset \mathbb{Z}_3 \subset \mathbb{Z}_{15} \subset \mathbb{Z}_{45}$.

3. The quotients of a composition series are abelian $\leftrightarrow$ they are cyclic of prime order $\leftrightarrow$ they are simple by exercise 1, so this follows from the definitions of "solvable" and "composition series".

4. $\{e\} \subset S_2; \{e\} \subset A_3 \subset S_3$; and $\{e\} \subset \{e, (12)(34)\} \subset \mathcal{V} \subset A_4 \subset S_4$ are composition series for S_2, S_3 and S_4.

2 Commutators and Solvability

1. We recall that D_n is defined by the elements D and R with $D^2 = R^n = 1$ and $DR = R^{n-1}D$. Since powers of R commute, the only not-necessarily-trivial elements of the commutator group are the elements $DR^kDR^{n-k} = R^{2(n-k)}$. Taking all $1 \leq k \leq n$,

we find that when n is odd, the commutator subgroup is the rotation subgroup, and when n is even, the commutator subgroup is the even powers of R.

2. The symmetric group of S_n is A_n because for $x, y \in S_n$, yxy^{-1} has the same cycle structure as x, so $x(yxy^{-1})$ has even cycle structure, so $G' \subset A_n$, and for any $\sigma \in A_n$, σ is the product of an even number of disjoint 2-cycles and the orbit of an arbitrary 2-cycle under A_n is the set of all disjoint 2-cycles since A_n is transitive, so every product of an even number of disjoint 2-cycles is in G', so $A_n \subset G'$.

3. (a) Let $h \in H, k \in K$, then $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) = hh'$ for some $h' \in H$ since H is normal. Similarly, $hkh^{-1}k^{-1} \in K$, so $[H, K] \subset H \cap K$. And $g(hkh^{-1}k^{-1})g^{-1} = gh(gg^{-1})k(gg^{-1})h^{-1}(gg^{-1})k^{-1}g^{-1} = (ghg^{-1})(gkg^{-1})(gh^{-1}g^{-1})(gk^{-1}g^{-1}) = h'k'(h')^{-1}(k')^{-1}$ for some $h' \in H, k' \in K$, so $[H, K]$ is normal in G.

   (b) Hyup.

   (c) Both the base case and the induction step are given by part b.

4. $(aba^{-1}b^{-1})(ba) = ab$, so $ab + X = ba + X \leftrightarrow aba^{-1}b^{-1} \in X$, so G', the set of all products $aba^{-1}b^{-1}$, is the smallest group X such that G/X is abelian.

5. The commutator of a subset of G is a subset of the commutator of G, so if $G^{(k)}$ is trivial for some k as in Theorem 10.2.2 then for $H \subset G, H^{(k)}$ is trivial too, so H is solvable.

6. A quotient of G by a subgroup of G is isomorphic to a subgroup of G, so this follows from the previous exercise.

7. The direct sum of solvable groups is solvable by the construction used in Exercise 10.1.1b, so since $G \cong N \oplus G/N$ it follows that G is solvable whenever N and G/N are.

3 Simplicity of the Alternating Groups

1. For $\sigma \in Z(S_n), \tau \in S_n$, we have $\tau\sigma\tau^{-1} = \tau\tau^{-1}\sigma = \sigma$, so the conjugacy class of σ is only σ. For $n > 2$, the only element in S_n with a single-element conjugacy class is the identity, so $Z(S_n)$ is trivial.

2. The orbit of each of its generators under conjugacy is contained in $\mathcal{V}$, so it is normal.

3. Let $x \in Z(a), a \in A, g \in G$, then $agxg^{-1} = (gg^{-1})agxg^{-1} = g(g^{-1}ag)xg^{-1} = gx(g^{-1}ag)g^{-1} = gxg^{-1}a$, so every element of A commutes with gxg^{-1}, so $Z(A)$ is normal in G.

4. (a) Same proof as in exercise 1, since A_4 is transitive.

(b) For $n > 4$, A_n contains an isomorphic copy of A_4, so it's not abelian.

(c) The center of A_n is normal in A_n, so it's normal in G by exercise 3, so it's $\{e\}$ or A_n since those are the normal subgroups of S_n for $n \geq 5$, but by part b the center is not A_n since A_n is not abelian, so it must be $\{e\}$.

5. Let $x \in M$, then for $g \in A_n$, $gxg^{-1} = \sigma(\sigma^{-1}(gxg^{-1})) = \sigma(\sigma^{-1}(g)\sigma^{-1}(x)\sigma^{-1}(g^{-1}))$. Since $\sigma^{-1}(x) \in N$ and N is normal, $\sigma^{-1}(g)\sigma^{-1}(x)\sigma^{-1}(g^{-1}) \in N$, so $\sigma(\sigma^{-1}(g)\sigma^{-1}(x)\sigma^{-1}(g^{-1})) \in M$, so M is normal.

6. A simple nonabelian group G is not solvable because in particular it is not cyclic of prime order, and since it has no normal subgroups its only composition series is $\{1\} \subset G$, which does not meet the criteria for solvability.

4 Cyclotomic Polynomials

1. $(\xi^r)^n = (\xi^n)^r = 1^r = 1$, and if $(\xi^r)^d = 1$ for some d then $\xi^{rd} = \xi^{rn} \to rd = 0 \mod n \to rd$ is divisible by $n \to n$ divides d since r and n are relatively prime. So n is the smallest power to which ξ is equal to 1.

2. $\psi_1(x) = x - 1; x^2 - 1 = \psi_1\psi_2 = \psi_2 * (x - 1) \to \psi_2 = x + 1; x^3 - 1 = \psi_1\psi_3 = \psi_3 * (x - 1) \to \psi_3(x) = x^2 + x + 1; x^4 - 1 = \psi_1\psi_2\psi_4 = \psi_4 * (x^2 - 1) \to \psi_4(x) = x^2 + 1$ etc.

3. Shure does/is.

4. $\mathbb{Q}[x] \subset \mathbb{C}[x]$ and $\mathbb{Q}[x] \subset \mathbb{Q}(x)$, so $\mathbb{Q}[x] \subset \mathbb{Q}(x) \cap \mathbb{C}[x]$. And if $p(x) \in \mathbb{Q}(x) \cap \mathbb{C}[x]$, then $p(x) = \frac{p_1(x)}{p_2(x)}$, where $p_1, p_2 \in \mathbb{Q}[x]$, but also $p(x) = p_3(x)$ where $p_3(x) \in \mathbb{C}[x]$, so $p_2(x)$ must equal 1 and $p_3(x) = p_1(x) = p(x) \in \mathbb{Q}[x]$.

5. ψ_n is irreducible $\leftrightarrow$ it is the minimal polynomial of ξ over $\mathbb{Q}$. Since ψ_n has the properties b, c, and d, the statement will follow if any of those implies a. The minimal polynomial f of ξ in part b divides ψ_n since it is minimal, and if ξ^p is a root of f for all p not dividing n then $(x - \xi^p)$ divides f for all such p, so since ψ_n is just the product of all such $(x - \xi^p)$ it follows that ψ_n divides f and hence is equal to it and hence is irreducible since f is minimal.

6. Since n is not divisible by the characteristic of K, the derivative of x^n, nx^{n-1}, is not uniformly zero over K, so $x^n - 1$ must have n distinct roots. There are only n nth roots of unity, some of which are primitive, so the splitting field E of $x^n - 1$ must contain a primitive nth root of unity ξ. Then the other primitive nth roots of unity are the powers of ξ^p where p does not divide n, and if $f \in \mathrm{Aut}_K(E)$ then $f(\xi)$ is a primitive root ξ^r since otherwise f wouldn't be an automorphism. f is entirely

defined by $f(\xi)$, since every nth root of unity is a power of ξ, so the Galois group of $x^n - 1$ is a subgroup of the group of units in $\mathbb{Z}_n$.

5 The Equation $x^n - b = 0$

1. Let f be the map in question, then for $\sigma, \tau \in \mathrm{Aut}_{K(u)}(E)$, we have $\sigma(a) = u^i a, \tau(a) = u^j a$, where $i, j \in \mathbb{N}, u$ is a primitive nth root of unity as in this section. So then $f(\sigma\tau) = (\sigma\tau)(a)a^{-1} = u^{i+j}aa^{-1} = u^{i+j} = u^i aa^{-1}u^j aa^{-1} = f(\sigma)f(\tau)$, so f is a homomorphism. And f is injective because $f(\tau) = 1$ precisely when $\tau(a) = a$, and τ is determined by its action on a so must be the identity in this case.

2. Let ξ be a primitive 13th root of unity, then this group is $\mathbb{Q}(\xi)$ with no subgroups.

3. Let ξ be a primitive 13th root of unity, then this group is $\mathbb{Q}(\xi, \sqrt{2})$ with subgroups $\mathbb{Q}(\xi)$ and $\mathbb{Q}(\sqrt{2})$.

4. By 10.4.5, the Galois group of $x^n - 1$ is congruent to $\Phi(n)$, and by 3.6.27, $\Phi(n) \cong \Phi(p_1^{m_1}) \times \Phi(p_2^{m_2}) \times \ldots \times \Phi(p_n^{m_n})$, which is isomorphic to the direct products of the Galois groups for $x^{p_i^{m_i}} - 1$ by 10.4.5 again. The other assertions then follow immediately.

6 Solvability by Radicals

That was easy.

7 Radical Extensions

1. $g(\sigma\tau) = (\sigma\tau)(a)a^{-1} = \sigma(\tau(a)a^{-1}a)a^{-1} = \sigma(\tau(a)a^{-1})\sigma(a)a^{-1} = (\sigma(a)a^{-1})\sigma(\tau(a)a^{-1}) = g(\sigma)\sigma(g(\tau))$.

2. $\prod_i \sigma^i(b) = 1$ since the Galois group is cyclic with generator σ and $N(b) = 1$, so f is well defined. Let $x = \sigma^i, y = \sigma^j$, then $f(xy) = f(\sigma^{i+j}) = \prod_{k=0}^{i+j-1} \sigma^k(b) = [\prod_{k=0}^{i-1} \sigma^k(b)][\prod_{l=i}^{i+j-1} \sigma^l(b)] = [\prod_{k=0}^{i-1} \sigma^k(b)][\sigma^i(\prod_{l=i}^{j-1} \sigma^l(b))] = f(x)xf(y)$.