Solution 21

Solvability by Radicals

1. Let be $(N, \cdot)$ and $(H, \cdot)$ be two groups and $\varphi : H \longrightarrow \mathrm{Aut}(N)$ a group homomorphism. Write $\varphi_h := \varphi(h) \in \mathrm{Aut}(N)$ for each $h \in H$. Define $G := N \rtimes_\varphi H$, the *(external) semidirect product of* N *and* H, as the set $N \times H$ with the binary operation

$$\forall n, n' \in N, \forall h, h' \in H,\ (n, h) \cdot_\varphi (n', h') = (n \cdot \varphi_h(n'), h \cdot h').$$

   (a) Check that $(N \rtimes_\varphi H, \cdot_\varphi)$ is a group.

   (b) Prove: there is a short exact sequence $1 \longrightarrow N \xrightarrow{j} N \rtimes_\varphi H \xrightarrow{\pi} H \longrightarrow 1$.

   (c) Deduce that $G = N \rtimes_\varphi H$ contains two subgroups N_0, H_0 with $N_0 \trianglelefteq G$, such that $N \cong N_0$ and $H \cong H_0$, satisfying the properties

$$\begin{cases} N_0 H_0 = G \\ N_0 \cap H_0 = \{1\}. \end{cases}$$

Conversely, let G be a group, $H \leqslant G$ a subgroup and $N \trianglelefteq G$ a normal subgroup. We say that G is the *(inner) semidirect product of* N *and* H, if

$$\begin{cases} NH = G \\ N \cap H = \{1\}. \end{cases}$$

In this case, we write $G = N \rtimes H$. Assume that this is the case.

   (d) Prove: there is a unique homomorphism $\alpha : G \longrightarrow H$ such that $\alpha|_H = \mathrm{id}_H$ and $\ker(\alpha) = N$.

   (e) Let $\varphi : H \longrightarrow \mathrm{Aut}(N)$ be the action of H on N by conjugation, that is, $\varphi(h)(n) := hnh^{-1}$ for all $h \in H$ and $n \in N$. Show that there is an isomorphism $\theta : G \xrightarrow{\sim} N \rtimes_\varphi H$ which satisfies $\theta|_N = j$ and $\alpha = \pi \circ \theta$. Draw a diagram containing two short exact sequences which explains the situation.

   (f) Let M be a normal subgroup of N. Show that $M \trianglelefteq G$ if and only if $hMh^{-1} = M$ for all $h \in H$.

Solution:

   (a) The formula given in the exercise is a well-defined binary operation on the set $N \times H$, since φ_h is an automorphism of N for each $h \in H$, so that $\varphi_h(n') \in N$ for each $n' \in N$ and then using the binary operations on N and H we know that $n \cdot \varphi_h(n') \in N$ and $h \cdot h' \in H$.

First, we check that the operation $\cdot_\varphi$ is associative. For each $n, n', n'' \in N$ and $h, h', h'' \in H$, we compute (omitting the sign $\cdot$ for the group operations in N and H and using associativity in those two groups by omitting parentheses when the group operation is performed several times)

$$\begin{aligned}((n,h)\cdot_\varphi (n',h'))\cdot_\varphi (n'',h'') &= (n\varphi_h(n'),hh')\cdot_\varphi (n'',h'')\\ &= (n\varphi_h(n')\varphi_{hh'}(n''),hh'h'') \overset{(*)}{=} (n\varphi_h(n')(\varphi_h\circ\varphi_{h'})(n''),hh'h'')\\ &= (n\varphi_h(n')\varphi_h(\varphi_{h'}(n'')),hh'h'') \overset{(**)}{=} (n\varphi_h(n'\varphi_{h'}(n'')),hh'h'')\\ &= (n,h)\cdot_\varphi (n'\varphi_{h'}(n''),h'h'') = (n,h)\cdot_\varphi ((n',h')\cdot_\varphi (n'',h''))\end{aligned}$$

so that $\cdot_\varphi$ is associative. In the step $(*)$ we use the assumption that φ is a group homomorphism, while in the step $(**)$ we use the assumption that φ_h is a group homomorphism.

We notice that $(1,1) = (1_N, 1_H)$ is the neutral element of $N \rtimes_\varphi H$. Indeed, we know that $\varphi_1 = \varphi(1) = \mathrm{id}$ since φ is a group homomorphism, while $\varphi_h(1) = 1$ for each $h \in H$ because φ_h is a group automorphism of N. Hence for every $h \in H$ and $n \in N$

$$\begin{aligned}(1,1)\cdot_\varphi (n,h) &= (1\cdot\varphi_1(n),1\cdot h) = (1\cdot n, 1\cdot h) = (n,h)\\ (n,h)\cdot_\varphi (1,1) &= (n\cdot\varphi_h(1),h\cdot 1) = (n\cdot 1,h\cdot 1) = (n,h).\end{aligned}$$

We look now for an inverse (n',h') of (n,h) with $n,n'\in N$ and $h,h'\in H$. We want to ensure that the equalities

$$\begin{cases}(1,1) \overset{!}{=} (n,h)\cdot_\varphi (n',h') = (n\varphi_h(n'),hh')\\ (1,1) \overset{!}{=} (n',h')\cdot_\varphi (n,h) = (n'\varphi_{h'}(n),h'h).\end{cases}$$

The second component coincides in both equalities by taking $h' = h^{-1}$. Comparing the first component in the second equality, we get $n' = \varphi_{h^{-1}}(n)^{-1} = \varphi_{h^{-1}}(n^{-1})$, which substituted in the first component in the first equation gives

$$1 \overset{?}{=} n\varphi_h(\varphi_{h^{-1}}(n^{-1})) = n\varphi_{hh^{-1}}(n^{-1}) = n\varphi_1(n^{-1}) = nn^{-1} = 1,$$

so that (n,h) has an inverse and we can conclude that $G = N \rtimes_\varphi H$ is a group.

(b) The map $j : N \longrightarrow N \rtimes_\varphi H$ sending $n \mapsto (n,1)$ is injective and it is a group homomorphism since for each $n,n' \in N$ we know that $(n,1)\cdot_\varphi (n',1) = (n\varphi_1(n'),1) = (nn',1)$. The projection map $\alpha : N \rtimes_\varphi H \longrightarrow H$ sending $(n,h) \mapsto h$ is surjective and is seen to be a group homomorphism by definition of $\cdot_\varphi$.

In order to conclude that j and α sits in a short exercise sequence, we need to check that $\ker(\pi) = \mathrm{im}(j)$, which is immediate by noticing that those two subgroups of $N \rtimes_\varphi H$ are both given by

$$N_0 := \{(n,1) : n \in N\} \subset N \rtimes_\varphi H. \tag{1}$$

(c) Since j is injective, it restricts to an isomorphism $N \cong \mathrm{im}(j) = N_0$ (as defined in (1)) and since $N_0 = \ker(\pi)$, it is a normal subgroup of G. The map $\iota : H \longrightarrow N \rtimes_\varphi H$ is seen to be an injective group homomorphism, so that H is isomorphic to

$$H_0 := \mathrm{im}(\iota) = \{(1,h) : h \in H\} \leqslant N \rtimes_\varphi H.$$

By construction,

$$N_0H_0 = \{(n,1)\cdot_\varphi (1,h) : n \in N, h \in H\} = \{(n\cdot\varphi_1(1),h) : n \in N, h \in H\} = G$$

and

$$N_0 \cap H_0 = \{(1,1)\}$$

so that N_0 and H_0 satisfy all the desired properties.

(d) Now we are working with a group G containg two subgroups $N \trianglelefteq G$ and $H \trianglelefteq G$ such that $NH = G$ and $N \cap H = G$. For each $g \in G$, there exist $n \in N$ and $h \in H$ for which $g = nh$. We claim that those are uniquely determined.

Suppose that $n, n' \in N$ and $h, h' \in H$ satisfy $nh = n'h'$. Then

$$h(h')^{-1} = n^{-1}n' \in H \cap N = \{1\}$$

so that $1 = h(h')^{-1} = n^{-1}n'$ which means that $h = h'$ and $n = n'$. This proves our claim.

Hence the assignment $nh \mapsto h$ is a well defined map $\alpha : G \longrightarrow H$, which is surjective since $h = 1 \cdot h \mapsto h$ for each $h \in H$. This also proves the desired property that $\alpha|_H = \mathrm{id}_H$. In order to prove that α is a group homomorphism, we need to check that $\alpha(nhn'h') = hh'$ for each $n, n' \in N$ and $h, h' \in H$. This is the case because

$$nhn'h' = n(hn'h^{-1})hh'$$

and $n(hn'h^{-1}) \in N$ because $N \trianglelefteq G$. Finally, $\ker(\alpha) = \{n \cdot 1, n \in N\} = N$ by definition of α.

For uniqueness, suppose that $\alpha : G \longrightarrow H$ is a group homomorphism such that $\alpha|_H = \mathrm{id}_H$ and $\ker(\alpha) = N$. Then, for each $g \in G$, write $g = nh$ for unique $n \in N$ and $h \in H$. We necessarily have

$$\alpha(nh) = \alpha(n)\alpha(h) = 1_G \cdot h = h,$$

which proves uniqueness of α.

(e) The map φ is well defined because $N \trianglelefteq G$ so that it is closed under conjugation by elements of H. It is easily checked to be a group homomorphism.

As we showed in the previous part, for each $g \in G$ there exist $n \in N$ and $h \in H$ such that $g = nh$. Hence there is a well defined bijection $\theta : G \longrightarrow$

$N \rtimes_\varphi H$ sending $nh \mapsto (n,h)$. This is a group homomorphism, since for each $n, n' \in N$ and $h, h' \in H$

$$\begin{aligned}\theta(nhn'h') = \theta(nhn'h^{-1}hh') = \theta(n\varphi_h(n')hh') = (n\varphi_h(n'), hh') \\ = (n,h) \cdot_\varphi (n', h') = \theta(nh) \cdot \theta(n'h').\end{aligned}$$

Then, for each $n \in N$ and $h \in H$, we see that $\theta(n) = (n,1) = j(n)$ and that $\alpha(nh) = h = \pi(n,h) = \pi(\theta(nh))$ so that θ satisfies all the desired properties. We have a commutative diagram

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, hook] \arrow[d, equal] & G \arrow[r, "\alpha"] \arrow[d, "\theta"] & H \arrow[r] \arrow[d, equal] & 1 \\ 1 \arrow[r] & N \arrow[r, "j"] & N \rtimes_\varphi H \arrow[r, "\pi"] & H \arrow[r] & 1 \end{tikzcd}$$

This can be said to be an isomorphism of short exact sequences. Since the vertical maps on the sides are identity maps, this is a special isomorphism, called an *equivalence* of group extensions.

(f) If $M \trianglelefteq G$, then it is stable under the conjugation of elements of H because $H \subset G$. Conversely, if $h_0 M h_0^{-1}$ for each $h_0 \in H$, then, for each $g \in G$, writing $g = nh$ with $n \in N$ and $h \in H$, we obtain

$$gMg^{-1} = nhMh^{-1}n^{-1} = nMn^{-1} = M,$$

where in the second step we used the assumption that $M \trianglelefteq N$.

2. Let p be a prime number and $n \geqslant 1$ an integer. Consider the natural action $\varphi : \mathrm{GL}_n(\mathbb{F}_p) \longrightarrow \mathrm{Aut}(\mathbb{F}_p^n)$. Let $G = \mathbb{F}_p^n \rtimes_\varphi \mathrm{GL}_n(\mathbb{F}_p)$ and embed $\mathbb{F}_p^n \hookrightarrow G$ via Exercise 1. Let $L \leqslant \mathbb{F}_p^n$ be a $\mathbb{F}_p$-linear subspace of $\mathbb{F}_p^n$. Show that L is subnormal in G and that $L \trianglelefteq G$ if and only if $L = 0$ or $L = \mathbb{F}_p^n$.

Solution: In the setup of Exercise 1, suppose that N and H are groups and $\varphi : H \longrightarrow \mathrm{Aut}(N)$ a group homomorphism. Let $G = N \rtimes_\varphi H$. Then as in part 1(c) we define $N_0 := N \times 1 \trianglelefteq N \rtimes_\varphi 1$ and $H_0 := 1 \times H \triangleleft 1 \times H$ and obtain that $G = N_0 \rtimes H_0$ (that is, N_0 and H_0 satisfy $N_0 H_0 = G$ and $N_0 \cap H_0 = 1$). Then, by part (e), $G \cong N_0 \rtimes_{\varphi'} H_0$ where $\varphi' : H_0 \longrightarrow \mathrm{Aut}(N_0)$ is the conjugation of N_0 by H_0 inside G. We claim that φ' corresponds to φ under the canonical identification $N \cong N_0$ and $H \cong H_0$. This is checked by letting $h \in H$ and $n \in N$ and computing

$$\varphi'_{(1,h)}(n,1) = (1,h)(n,1)(1,h^{-1}) = (\varphi_h(n), h)(1, h^{-1}) = (\varphi_h(n), 1).$$

Since a normal subgroup $M_0 \trianglelefteq N_0$ corresponds canonically to a normal subgroup $M \trianglelefteq N$ and it is normal in G if and only if the conjugation by H_0 preserves M_0, we deduce that M_0 is normal in G if and only if for $\varphi_h(M) \subset M$ for each $h \in H$.

In the situation of our exercise, this means that we just need to check that a linear subspace $L \subseteq \mathbb{F}_p^n$ is normal in $G = \mathbb{F}_p^n \rtimes_\varphi \mathrm{GL}_n(\mathbb{F}_p)$ if and only if it is stable under the action of $\mathrm{GL}_n(\mathbb{F}_p)$. By basic linear algebra, taking bases of two proper distinct subspaces of the same dimension, we see that there exists $g \in \mathrm{GL}_n(\mathbb{F}_p)$ mapping one to the other, so that the only subspaces of $\mathbb{F}_p^n$ stable under the action of $\mathrm{GL}_n(\mathbb{F}_p)$ are 0 and $\mathbb{F}_p^n$, as desired.

3. Let G be a finite group.

   (a) Suppose that G has a normal subgroup $N \trianglelefteq G$ such that G/N is abelian. Prove that G has a normal subgroup of prime index, which contains N.

   (b) Prove that G is solvable if and only if it has a normal series all whose factors are cyclic of prime order.

   Solution:

   (a) By the classification of finitely generated abelian groups we know that there exists a finite set of prime numbers P_0 and positive integers l_p and $r_{p,n}$ for $p \in P_0$ and $1 \leqslant n \leqslant l_p$ such that

   $$G/N \cong \prod_{p \in P_0} \prod_{n=1}^{l_p} \mathbb{Z}/p^{r_{p,n}}\mathbb{Z}.$$

   Isolating one of the factors we can write for some prime number p, an integer $n > 0$ and an abelian group H

   $$G/N \cong \mathbb{Z}/p^n\mathbb{Z} \times H. \tag{2}$$

   The subgroup $p\mathbb{Z}/p^n\mathbb{Z} \times H \leqslant \mathbb{Z}/p^n\mathbb{Z} \times H$ is seen to have index p and it is normal because we are working in an abelian group. Via (2) we can map this subgroup to a subgroup of G/N with the same features. Since subgroup of G/N are subgroups of G containing N, we know that there is a subgroup $M \trianglelefteq G$ such that (by the third isomorphism theorem for groups)

   $$[G : M] = [G/N : M/N] = p.$$

   (b) Assume that we are in the situation of part (a). Then, by induction on the index of N one can prove that there is a series a normal series

   $$N = M_n \trianglelefteq M_{n-1} \trianglelefteq \cdots \trianglelefteq M_1 \trianglelefteq M_0 = G$$

   such that each M_k/M_{k-1} is cyclic of prime order. Indeed, the subgroup M_1 is found as in part (a) and then

   $$[M_1 : N] = \frac{[G : N]}{[G : M_1]} < [G : N]$$

so that we can apply the inductive hypothesis.

Suppose that G is solvable. Then, by the argument we just outlined, a normal sequence with abelian factors of G can be refined into a normal sequence whose factors are cyclic of prime order.

Conversely, a group with such a sequence is solvable by definition because cyclic groups are abelian.

4. Let k be a field and $f \in k[X]$ a polynomial of prime degree p. Let $E = \mathrm{Sf}(f)$. Suppose that $\mathrm{Gal}(E/k)$ is cyclic of order p. Prove that f is irreducible.

   Solution: Let $q = \mathrm{card}(R(f)) \leqslant p$ and embed $\mathrm{Gal}(E/k)$ into S_q via its action on the roots of f. Since S_q contains an element of order p, then $p|\mathrm{Card}(S_q) = q!$, which can only be possible for $q \geqslant p$. Hence $q = p$ and f has p distinct roots. Let $\sigma \in S_p$ be a generator of $\mathrm{Gal}(E/k)$ so that σ is an element of order p. By Assignment 17, Exercise 4, σ is a p-cycle. Then the group $\mathrm{Gal}(E/k) =< \sigma >\leqslant S_p$ acts transitively on the roots of f, which in turn is irreducible by Corollary II.23.