Math 404 HW 9 Solutions

Problem 9.1

Let p be a prime. Let $\rho = e^{2\pi i/p}$ be a primitive pth root of unity.

(a) Prove that $\mathbb{Q} \subset \mathbb{Q}(\rho)$ is a Galois field extension and that the Galois group $\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$ is isomorphic to the multiplicative group $(\mathbb{Z}/p)^\times$ of units in $\mathbb{Z}/p$.

(b) Let $L = \mathbb{Q}(\rho)$. Give the complete correspondence between intermediate field extensions $\mathbb{Q} \subset L' \subset L$ and subgroups $H \subset \mathrm{Gal}(L/\mathbb{Q})$.

Proof. Part (a) is exactly the same argument as in the last homework. That arugment yields an isomorphism $\varphi : (\mathbb{Z}/p)^\times \xrightarrow{\sim} \mathrm{Gal}(L/\mathbb{Q})$ determined by $\varphi(n)(\rho) = \rho^n$.

We also recall two group theoretic facts.

1. There is an isomorphism $(\mathbb{Z}/p)^\times \cong \mathbb{Z}/(p-1)$.

2. There is a bijection

$$\begin{aligned}\psi : \{\text{Subgroups of } \mathbb{Z}/(p-1)\} &\xrightarrow{\sim} \{\text{Divisors of } p-1\}\\ G &\mapsto |G|.\end{aligned}$$

   with the following properties:

   (a) $G \subset H$ if and only if $|G|$ divides $|H|$.

   (b) The inverse of ψ sends a divisor d of $p-1$ to $\langle \frac{p-1}{d} \rangle$, so in particular every subgroup is cyclic.

Combining this with the result of part (a) reduces us to the following problem.

Given an element $n \in (\mathbb{Z}/p\mathbb{Z})^\times$ of order m, determine the fixed field of $\langle n \rangle$.

To do this, let $\nu : \mathbb{Q}(\rho) \to \mathbb{Q}(\rho)$ be the automorphism over $\mathbb{Q}$ determined by $\nu(\rho) = \rho^n$. Define

$$\alpha = \rho + \rho^n + \rho^{(n^2)} + \cdots + \rho^{(n^{m-1})}.$$

I claim that the fixed field of $\langle \nu \rangle$ is exactly

$$\boxed{L^{\langle \nu \rangle} = \mathbb{Q}(\alpha).}$$

To see this, note that the orbit of ρ under $\langle \nu \rangle \subset \mathrm{Gal}(L/\mathbb{Q})$, corresponding to $\langle n \rangle \subset (\mathbb{Z}/p)^\times$, is $\{\rho, \rho^n, \rho^{(n^2)}, \ldots, \rho^{(n^{m-1})}\}$. As we remarked last week, if $s \in \mathbb{Q}[x_0, \ldots, x_{m-1}]$ is any symmetric polynomial, then $s(\rho, \ldots, \rho^{(n^{m-1})})$ will be fixed by $\langle \nu \rangle$. It turns out that $s = s_1 = x_0 + x_1 + \cdots + x_{m-1}$ generates the whole fixed field.

As a sanity check, we can first verify that α is indeed fixed by ν, which will imply that α is fixed by $\langle \nu \rangle$.

$$\begin{aligned}
\nu(\alpha) &= \nu(\rho + \rho^n + \rho^{(n^2)} + \cdots + \rho^{(n^{m-1})}) \\
&= \nu(\rho) + [\nu(\rho)]^n + [\nu(\rho)]^{(n^2)} + \cdots + [\nu(\rho)]^{(n^{m-1})} \\
&= \rho^n + [\rho^n]^n + [\rho^n]^{(n^2)} + \cdots + [\rho^n]^{(n^{m-1})} \\
&= \rho^n + \rho^{(n^2)} + \rho^{(n^3)} + \cdots + \rho^{(n^m)}.
\end{aligned}$$

Since we assumed that n was of order m in $(\mathbb{Z}/p)^\times$, we have the congruence $n^m \equiv 1 \pmod{p}$. Since $\rho^p = 1$, this yields that $\rho^{(n^m)} = \rho^1 = \rho$. Thus, the above computation yields

$$\nu(\alpha) = \rho^n + \rho^{(n^2)} + \rho^{(n^3)} + \cdots + \rho^{(n^{m-1})} + \rho = \alpha,$$

as desired.

Either this computation or the reasoning preceding it yields that $\alpha \in L^{\langle \nu \rangle}$, so $\mathbb{Q}(\alpha) \subset L^{\langle \nu \rangle}$. Now it remains to show the containment $L^{\langle \nu \rangle} \subset \mathbb{Q}(\alpha)$. Since the Galois correspondence is bijective and reverses inclusions, it is equivalent to show that $\langle \nu \rangle \supset \mathrm{Gal}(L/\mathbb{Q}(\alpha))$. So suppose that $\tau \in \mathrm{Gal}(L/\mathbb{Q}(\alpha))$. Our goal is to show that $\tau \in \langle \nu \rangle$.

To see this, let $t \in (\mathbb{Z}/p)^\times$ be the element corresponding to τ, so that $\tau(\rho) = \rho^t$. Then by assumption we have

$$\begin{aligned}\rho + \rho^n + \rho^{(n^2)} + \cdots + \rho^{(n^{m-1})} &= \alpha \\ &= \tau(\alpha) \\ &= \rho^t + \rho^{tn} + \rho^{(tn^2)} + \cdots + \rho^{(tn^{m-1})}.\end{aligned}$$

Since $t \in (\mathbb{Z}/p)^\times$, the elements $t, tn, tn^2, \ldots tn^{m-1}$ are all distinct residues mod p. Since ρ is a primitive pth root of unity, we have that the value of ρ^s depends exactly on the residue class of s mod p. So α and $\tau(\alpha)$ are both sums of m distinct powers of ρ. Since the elements $1, \rho, \rho^2, \ldots, \rho^{p-1}$ are all linearly independent over $\mathbb{Q}$, we must have that these are both sums over the same powers of ρ, that is we must have an equality

$$\{1, n, n^2, \ldots, n^{m-1}\} = \{t, tn, tn^2, \ldots, tn^{m-1}\}$$

in $\mathbb{Z}/p$. In particular, we must have that $t = n^i$ mod p, which is true if and only if $t \in \langle n \rangle \subset (\mathbb{Z}/p)^\times$. Thus, in the Galois group, we must have that $\tau \in \langle \nu \rangle$, as desired.

□

Problem 9.2

Let N and H be finite groups. Denote by $\mathrm{Aut}(N)$ the group of automorphisms of N (**remark for later, this yields an action of H on N**). Let $\varphi : H \to \mathrm{Aut}(N)$ be a group homomorphism. Define the following group operation on the set $N \times H$ via

$$(n_1, h_1) \bullet (n_2, h_2) = (n_1 \varphi(h_1)(n_2), h_1 h_2)$$

(a) Show that $N \times H$ is a group with the operation $\bullet$. We call this the semi-direct product of N and H via φ and denote it by $N \rtimes_\varphi H$.

(b) Show that H and N are naturally subgroups of $N \rtimes_\varphi H$.

(c) Show that N is a normal subgroup.

(d) Show that the dihedral group

$$D_{2n} = \left\{\sigma, \tau \mid \sigma^n = \tau^2 = \mathrm{id}, \sigma\tau = \tau\sigma^{-1}\right\}$$

is isomorphic to the semi-direct product $\mathbb{Z}/n \rtimes_\varphi \mathbb{Z}/2$ where $\varphi : \mathbb{Z}/2 = \{0, 1\} \to \mathrm{Aut}(\mathbb{Z}/n)$ is the group homomorphism where $\varphi(0) : \mathbb{Z}/n \to \mathbb{Z}/n$ is the identity and $\varphi(1) : \mathbb{Z}/n \to \mathbb{Z}/n$ sends $x \mapsto -x$.

(a) Let e_N and e_H be the identity elements for N and H, respectively. We show that (e_N, e_H) is an identity element for $\bullet$. Since φ is a group homomorphism, we must have that $\varphi(e_H)$ is the identity automorphism of N. With this in mind, we compute

$$\begin{aligned}(e_N, e_H) \bullet (n, h) &= (e_N \varphi(e_H) n, e_h h) \\ &= (\mathrm{id}_H(n), h) \\ &= (n, h).\end{aligned}$$

The computation for the other order of multiplication is similar.

Now we show that inverses exist. Let $(n, h) \in N \times H$. Since $\varphi(h) \in \mathrm{Aut}(N)$, there exists a unique $n' \in N$ so that $\varphi(h)(n') = n^{-1}$. I claim that (n', h^{-1}) is an inverse for (n, h) under $\bullet$. To see this, we compute

$$\begin{aligned}(n, h) \bullet (n', h^{-1}) &= (n\varphi(h)(n'), hh^{-1}) \\ &= (nn^{-1}, e_H) \\ &= (e_N, e_H).\end{aligned}$$

For the other order of multiplication, we compute

$$\begin{aligned}(n', h^{-1}) \bullet (n, h) &= (n'\varphi(h^{-1})(n), h^{-1}h) \\ &= (n'\varphi(h^{-1})(n), e_H).\end{aligned}$$

So we just need to show

$$n'\varphi(h^{-1})(n) = e_N.$$

To see this, we compute

$$\begin{aligned}n'\varphi(h^{-1})(n) &= n'[\varphi(h)]^{-1}(n) && \text{(as } \varphi \text{ is a group homomorphism)} \\ &= [\varphi(h)]^{-1}(n^{-1})[\varphi(h)]^{-1}(n) && \text{(apply } [\varphi(h)]^{-1} \text{ to } \varphi(h)(n') = n^{-1}\text{)} \\ &= [\varphi(h)]^{-1}(n^{-1}n) && \text{(as } [\varphi(h)]^{-1} \text{ is a homomorphism)} \\ &= [\varphi(h)]^{-1}(e_N) \\ &= e_N,\end{aligned}$$

as $[\varphi(h)]^{-1}$ is a homomorphism. Phew!

Now for associativity. Let $n_1, n_2, n_3 \in N$ and $h_1, h_2, h_3 \in H$. We omit excess parentheses for computations within N and H as multiplication in those groups is associative by assumption. We compute

$$\begin{aligned}\Big[(n_1, h_1) \bullet (n_2, h_2)\Big] \bullet (n_3, h_3) &= \Big(n_1\varphi(h_1)(n_2), h_1h_2\Big) \bullet (n_3, h_3) \\ &= \Big(n_1\varphi(h_1)(n_2)\varphi(h_1h_2)(h_3), h_1h_2h_3\Big).\end{aligned}$$

We similarly compute

$$\begin{aligned}(n_1, h_2) \bullet \Big[(n_2, h_2) \bullet (n_3, h_3)\Big] &= (n_1, h_1) \bullet (n_2\varphi(h_2)(n_3), h_2h_3) \\ &= \Big(n_1\varphi(h_1)\big[n_2\varphi(h_2)(n_3)\big], h_1h_2h_3\Big).\end{aligned}$$

So we have reduced down to showing the following equality

$$n_1\varphi(h_1)(n_2)\varphi(h_1h_2)(h_3) = n_1\varphi(h_1)\big[n_2\varphi(h_2)(n_3)\big]. \tag{1}$$

We compute

$$\begin{aligned} n_1\varphi(h_1)(n_2)\varphi(h_1h_2)(h_3) &= n_1\varphi(h_1)(n_2)\big[\varphi(h_1)\circ\varphi(h_2)\big](h_3) && \text{(as } \varphi \text{ is a homomorphism)} \\ &= n_1\varphi(h_1)\big[n_2\varphi(h_2)(h_3)\big] && \text{(as } \varphi(h_1) \text{ is a homomorphism.)} \end{aligned}$$

This is the desired equality, and so associativity holds. Since this is the last of three group axioms, we have a group! Huzzah!

□

(b) Let $\iota_N : N \to N \rtimes_\varphi H$ and $\iota_H : H \to N \rtimes_\varphi H$ be the functions given by

$$\begin{aligned} \iota_N(n) &= (n, e_H) \\ \iota_H(h) &= (e_N, h). \end{aligned}$$

(think ι for i for inclusion). Since ι_N and ι_H are both clearly injective, we just need to show that they are homomorphisms. We compute

$$\begin{aligned} \iota_N(n)\iota_N(n') &= (n, e_H) \bullet (n', e_H) \\ &= (n\varphi(e_H)n', e_He_H) \\ &= (nn', e_H) \\ &= \iota_N(nn'). \end{aligned}$$

The third equality holds as φ, being a homomorphism, sends the identity of H to the identity automorphism of N. Thus, ι_N is a homomorphism.

For ι_H, we compute

$$\begin{aligned} \iota_H(h)\iota_H(h') &= (e_N, h) \bullet (e_N, h') \\ &= (e_N\varphi(h)(e_N), hh') \\ &= (e_Ne_N, hh') \\ &= (e_N, hh') \\ &= \iota_H(hh'). \end{aligned}$$

The third equality holds as $\varphi(h)$, being an automorphism of N, preserves the identity. Thus, ι_H is a homomorphism, and the result holds.

□

(c) One way to do this is to note that the definition of multiplication in the semidirect product shows that $\pi : N \rtimes_\varphi H \to H$ given by $\pi(n,h) = h$ is a surjective homomorphism. Furthermore, we have that $N = \ker\varphi$, and since kernels of homomorphisms are normal, we have that N is normal.

We can also verify this by direct computation. First, we note that for any $(n,h) \in N \rtimes_\varphi H$, we have

$$(n, e_H) \bullet (e_N, h) = (n\varphi(e_H)e_N, e_H h) = (n, h).$$

Thus, we have that $N \rtimes_\varphi H = NH$. That is, any subgroup of $N \rtimes_\varphi H$ containing both N and H must be the whole group.

So, let K be the normalizer of N in $N \rtimes_\varphi H$. Since we automatically have $N \subset K$, if we can show $H \subset K$, then we will have $K = N \rtimes_\varphi H$, meaning that N is a normal subgroup.

So let $(n, e_H) \in N$ and $(e_N, h) \in H$. Since the embedding $\iota_H : H \to N \rtimes_\varphi H$ is a homomorphism, we have that

$$(e_N, h)^{-1} = \iota_H(h)^{-1} = \iota_H(h^{-1}) = (e_N, h^{-1}).$$

Thus, we compute

$$\begin{aligned}(e_N, h) \bullet (n, e_H) \bullet (e_N, h^{-1}) &= (e_N, h) \bullet (n, h^{-1}) \qquad \text{(see the beginning of (c))}\\ &= (e_N\varphi(h)(n), hh^{-1})\\ &= (\varphi(h)(n), e_H) \in N\end{aligned}$$

Thus, N is normal. Furthermore, this computation reveals something important about the semidirect product that's worth highlighting

The action φ of H on N in $N \rtimes_\varphi H$ is exactly conjugation of N by H in $N \rtimes_\varphi H$.

(d) First a technical lemma we will use later. This is very much in the same spirit that the elements fixed by a subgroup of the Galois group of a field extension form a field.

Lemma 1. *Let G be a group, and let $\gamma : G \to G$ be a homomorphism (also called an endomorphism in this case where the domain and codomain are the same). Define*

$$H = \{g \in G : \gamma(g) = g\}.$$

Then H is a subgroup of G

Prove this yourself! It really does follow directly from the definitions. The same argument yields the following result, of which the previous lemma is a special case, which isn't needed for this homework but is worthwhile in its own right.

Optional exercise *Let $\gamma : G \to K$ and $\delta : G \to K$ be homomorphisms. Let H the set of all $g \in G$ such that $\gamma(g) = \delta(g)$. Then H is a subgroup of G.*

Now for the task at hand! Let $\alpha : D_{2n} \to \mathbb{Z}/n \rtimes_\varphi \mathbb{Z}/2$ be the map determined by

$$\alpha(\sigma) = (1, 0)$$
$$\alpha(\tau) = (0, 1).$$

This is a fairly natural choice, singling out an element of order n and an element of order 2 in $\mathbb{Z}/n \rtimes \mathbb{Z}/2$. We will show later that α induces a well-defined homomorphism.

This can yield the desired result in one of two ways. Since $(1, 0)$ and $(0, 1)$ are both in the image of α, and these elements generate $\mathbb{Z}/n \rtimes_\varphi \mathbb{Z}/2$, we get that α is surjective. If we already know that D_{2n} is a group on $2n$ elements with exactly these relations, then α is a surjective homomorphism between two finite groups of the same size, and so it is an isomorphism. If you accept this, then in the section to follow called "Showing α and β are homomorphisms", feel free to ignore the part about β, and you can ignore the rest of this section.

If you haven't already shown that the group with these generators and relations is of order $2n$ (which in my opinion is pretty hard to show directly), then we can actually prove that here by building an inverse to α explicitly, and then just noting that $\mathbb{Z}/n \times \mathbb{Z}/2$ has $2n$ elements.

So carrying on, let's try to build an inverse $\beta : \mathbb{Z}/n \rtimes_\varphi \mathbb{Z}/2 \to D_{2n}$. To be an inverse to α we are forced to define $\beta(1,0) = \sigma$ and $\beta(0,1) = \tau$. For β to be a homomorphism, since $(i,0)$ is $(1,0)$ multiplied by itself i times, we must have $\beta(i,0) = \sigma^i$ and also $\beta(0,j) = \tau^j$. We would then also have to have

$$\beta(i,j) = \beta\Big((i,0) \bullet (0,j)\Big) = \beta(i,0)\beta(0,j) = \sigma^i\tau^j.$$

So we define β by this formula and later we'll show that this is indeed a homomorphism. Note that since $\sigma^n = \mathrm{id}$ and $\tau^2 = \mathrm{id}$, the elements $\sigma^i\tau^j$ only depend on the residues of i mod n and j mod 2, so this does at least make sense as a function on $\mathbb{Z}/n \rtimes_\varphi \mathbb{Z}/2$, and further yields that β is a homomorphism when restricted to either $\mathbb{Z}/n$ or $\mathbb{Z}/2$.

For now, let us assume that both α and β are homomorphisms, and show that they are inverses.

First we show that $\beta \circ \alpha : D_{2n} \to D_{2n}$ is the identity. By the lemma, the elements fixed by $\beta \circ \alpha$ form a subgroup of D_{2n}. Since σ and τ generate D_{2n}, if we can show that $\beta \circ \alpha$ fixes these elements, then $\beta \circ \alpha$ must fix everything. That is, $\beta \circ \alpha = \mathrm{id}$. But $\beta \circ \alpha$ fixes these elements by design, so indeed we get $\beta \circ \alpha = \mathrm{id}$

For the other composition, we again use that the elements fixed by $\alpha \circ \beta$ form a subgroup of $\mathbb{Z}/n \rtimes_\varphi \mathbb{Z}/2$, call this subgroup K. As we remarked at the beginning of part (c), to show that $K = \mathbb{Z}/n \rtimes_\varphi \mathbb{Z}/2$, we just have to show that $\mathbb{Z}/n \subset K$ and $\mathbb{Z}/2 \subset K$. Since $(1,0)$ generates $\mathbb{Z}/n$ and $(0,1)$ generates $\mathbb{Z}/2$, we just have to show that these elements are fixed by $\alpha \circ \beta$. But these elements are fixed by design, and so $\alpha \circ \beta = \mathrm{id}$.

Showing that α and β are homomorphisms

For α to be a homomorphism, we first recall a fact about groups given by generators and relations.

As a reminder, we have $D_{2n} = \langle \sigma, \tau : \sigma^n = \tau^2 = 1, \sigma\tau = \tau\sigma^{-1} \rangle$. Suppose we have a homomorphism $\gamma : D_{2n} \to G$, where G is any group. Then we have elements $g = \gamma(\sigma)$ and $h = \gamma(\tau)$. Since γ is a homomorphism, these elements must satisfy the same relations as σ and τ. Saying that D_{2n} is the group with these generators and relations says that supplying elements $g, h \in G$ satisfying the same relations as σ and τ yields a unique homomorphism $\gamma : D_{2n} \to G$ such that $\gamma(\sigma) = g$ and $\gamma(\tau) = h$.

So to show that α yields a homomorphism, we just need to show that $(1, 0)$ and $(0, 1) \in \mathbb{Z}/n \rtimes_\varphi \mathbb{Z}/2$ satisfy the same relations as σ and τ. We have that $(1, 0)^n == (n, 0) = (0, 0)$, and $(0, 1)^2 = (0, 2) = (0, 0)$. So we just need to check the commutativity relation.

Since $\tau^2 = e_{D_{2n}}$, the commutativity relation $\sigma\tau = \tau\sigma^{-1}$ is equivalent to the relation $\tau\sigma\tau^{-1} = \sigma^{-1}$. That is, conjugating σ by τ inverts σ. On the semidirect product side, this would be saying that conjugating $(1, 0)$ by $(0, 1)$ inverts $(1, 0)$. But as we remarked at the end of part (c), conjugating $(1, 0)$ by $(0, 1)$ yields

$$(\varphi(1)(1), 0) = (-1, 0) = (1, 0)^{-1}$$

So the conjugation relation also holds, and α yields a genuine homomorphism.

Now we show that β is a homomorphism. Let $(a, i), (b, j) \in \mathbb{Z}/n \rtimes_\varphi \mathbb{Z}/2$. We compute

$$\beta(a, i)\beta(b, j) = \sigma^a\tau^i\sigma^b\tau^j.$$

We also compute

$$\begin{aligned} \beta\Big((a, i) \bullet (b, j)\Big) &= \beta(a + \varphi(i)(b), i + j) \\ &= \sigma^{a+\varphi(i)(b)}\tau^{i+j} \\ &= \sigma^a\sigma^{\varphi(i)(b)}\tau^i\tau^j. \end{aligned}$$

So we wish to show

$$\begin{aligned} \sigma^a\tau^i\sigma^b\tau^j &= \sigma^a\sigma^{\varphi(i)(b)}\tau^i\tau^j \iff \\ \tau^i\sigma^b &= \sigma^{\varphi(i)(b)}\tau^i \iff \\ \tau^i\sigma^b\tau^{-i} &= \sigma^{\varphi(i)(b)}. \end{aligned}$$

If $i = 0$, then this last equality reads

$$\sigma^b = \sigma^{\varphi(0)(b)},$$

which is true. If $i = 1$, then we have

$$\tau\sigma^b\tau^{-1} = [\tau\sigma\tau^{-1}]^b = (\sigma^{-1})^b = \sigma^{-b} = \sigma^{\varphi(i)(b)},$$

as desired. Since this exhausts all possibilities for i and b, and our desired equality only depends on i and b, we have that β is a homomorphism, as desired.

Optional Exercise You can bootstrap the reasoning above about β to get a method for building homomorphisms out of semidirect products. The idea is that since the semidirect product is built out of two subgroups, homomorphisms out of it are built out of homomorphisms of these two subgroups.

Indeed, if $\beta : N \rtimes_\varphi H \to G$ is a group homomorphism, then we get homomorphisms $\beta_N := \beta \circ \iota_N : N \to G$ and $\beta_H := \beta \circ \iota_H : N \to G$, fitting into a diagram

$$\begin{tikzcd}
N \arrow[dr, "\iota_N"'] \arrow[drr, bend left, "\beta_N"] & & \\
& N \rtimes_\varphi H \arrow[r, "\beta"] & G \\
H \arrow[ur, "\iota_H"] \arrow[urr, bend right, "\beta_H"'] & &
\end{tikzcd}$$

And in fact, these β_N and β_H determine β uniquely. We can compute

$$\beta(n,h) = \beta((n,1) \bullet (1,h)) = \beta(n,1)\beta(1,h) = \beta_N(n)\beta_H(h).$$

So knowledge of these component homomorphisms β_N and β_H determine β uniquely. So a natural question to ask is can we go the other way? If someone hands us homomorphisms $\beta_N : N \to G$ and $\beta_H : H \to G$, do we get a homomorphism $\beta : N \rtimes_\varphi H \to G$ defined by $\beta(n,h) = \beta_N(n)\beta_H(h)$? Can we fill in the following diagram?

$$\begin{tikzcd}
N \arrow[dr, "\iota_N"'] \arrow[drr, bend left, "\beta_N"] & & \\
& N \rtimes_\varphi H \arrow[r, dashed, "\exists\beta?"] & G \\
H \arrow[ur, "\iota_H"] \arrow[urr, bend right, "\beta_H"'] & &
\end{tikzcd}$$

See if you can alter the preceding computations to build a criterion on β_N and β_H for when the resulting β is a homomorphism. (Hint: it will involve relating φ to conjugation in G).

Problem 9.3

Prove the the Galois group of $x^p - 2$ over $\mathbb{Q}$ for a prime p is isomorphic to the semi-direct product

$$\mathbb{Z}/p \rtimes_\varphi (\mathbb{Z}/p)^\times$$

with $\varphi : (\mathbb{Z}/p)^\times \to \mathrm{Aut}(\mathbb{Z}/p)$ given by $\varphi(a)$ is the automorphism of $\mathbb{Z}/p$ defined by multiplication by a.

Proof. Let L be the splitting field of $x^p - 2$. Let ρ be a primitive pth root of unity. Arguments that at this point are familiar yield that $L = \mathbb{Q}(\rho, \sqrt[p]{2})$. Then we have a commutative diagram of field extensions with known degrees labeled

$$\begin{tikzcd}
 & L & \\
\mathbb{Q}(\sqrt[p]{2}) \arrow[ur] & & \mathbb{Q}(\rho) \arrow[ul] \\
 & \mathbb{Q} \arrow[ul, "p"] \arrow[ur, "p-1"'] &
\end{tikzcd}$$

We will show three things

1. $N := \mathrm{Gal}(L/\mathbb{Q}(\rho)) \cong \mathbb{Z}/p$
2. $H := \mathrm{Gal}(L/\mathbb{Q}(\sqrt[p]{2})) \cong (\mathbb{Z}/p)^\times$
3. $\mathrm{Gal}(L/\mathbb{Q}) \cong N \rtimes_\varphi H$ with φ being the action given in the problem statement under the precedeing isomorphisms.

Let's get started!

Since p and $p-1$ are relatively prime, the reasoning from homework 3 problem 5 in the subsection ”leveraging the multiplicative property of the degree” yields that $|\mathbb{Q}(\sqrt[p]{2}, \rho) : \mathbb{Q}| = p(p-1)$. The multiplicative property of the degree lets us complete the above diagram with all degrees known.

$$\begin{tikzcd}
 & L & \\
\mathbb{Q}(\sqrt[p]{2}) \arrow[ur, "p-1"] & & \mathbb{Q}(\rho) \arrow[ul, "p"'] \\
 & \mathbb{Q} \arrow[ul, "p"] \arrow[ur, "p-1"'] &
\end{tikzcd}$$

Let $f = x^{p-1} + x^{p-2} + \cdots + x + 1$, so that f is the minimal polynomial for ρ over $\mathbb{Q}$. Since $L = \mathbb{Q}(\sqrt[p]{2})(\rho)$ and $\deg f = |L : \mathbb{Q}(\sqrt[p]{2})|$, we have that f is irreducible over $\mathbb{Q}(\sqrt[p]{2})$ and $L \cong \mathbb{Q}(\sqrt[p]{2})[x]/f$. Thus, for every $i \in (\mathbb{Z}/p)^\times$ we have an automorphism $\tau_i \in \mathrm{Gal}(L/\mathbb{Q}(\sqrt[p]{2}))$ given by

$$\begin{aligned} \tau_i(\sqrt[p]{2}) &= \sqrt[p]{2} \\ \tau_i(\rho) &= \rho^i. \end{aligned}$$

These τ_i comprise the entirety of $\mathrm{Gal}(L/\mathbb{Q}(\sqrt[p]{2})$, as there are $p-1$ of the τ_i and the group in question is of order $p-1$. The reasoning that $\mathrm{Gal}(L/\mathbb{Q}(\sqrt[p]{2})) \cong (\mathbb{Z}/p)^\times$ is the same as in problem 1.

Similarly we have that $L \cong \mathbb{Q}(\rho)[x]/(x^p - 2)$. We get an automorphism $\sigma \in \mathrm{Gal}(L/\mathbb{Q}(\rho))$

$$\begin{aligned} \sigma(\rho) &= \rho \\ \sigma(\sqrt[p]{2}) &= \rho\sqrt[p]{2}. \end{aligned}$$

Since $\sigma \neq \mathrm{id}$, and $\# \mathrm{Gal}(L/\mathbb{Q}(\rho) = p$, we have that $\langle \sigma \rangle = \mathrm{Gal}(L/\mathbb{Q}(\rho) \cong \mathbb{Z}/p$. For any $m \in \mathbb{Z}/p$ and $i \in (\mathbb{Z}/p)^\times$ we compute

$$\begin{aligned} \sigma^m \circ \tau_i(\sqrt[p]{2}) &= \sigma^m(\sqrt[p]{2}) \\ &= \rho^m \sqrt[p]{2}, \end{aligned}$$

and similarly

$$\begin{aligned} \sigma^m \circ \tau_i(\rho) &= \sigma^m(\rho^i) \\ &= [\sigma^m(\rho)]^i \\ &= \rho^i \end{aligned}$$

Thus, the elements $\sigma^m \circ \tau_i \in \mathrm{Gal}(L/\mathbb{Q})$ are all distinct. Since there are $p(p-1)$ of these, and $p(p-1) = |L : \mathbb{Q}| = \#\,\mathrm{Gal}(L/\mathbb{Q})$, these elements comprise the Galois group. So we have a bijection of sets $\lambda : \mathbb{Z}/p \rtimes_\varphi (\mathbb{Z}/p)^\times \xrightarrow{\sim} \mathrm{Gal}(L/\mathbb{Q})$ given by $\lambda(m, i) = \sigma^m \circ \tau_i$. So now we just need to show that λ preserves the group structure. We compute

$$\begin{aligned}
[\lambda(m,i) \circ \lambda(n,j)](\rho) &= (\sigma^m \circ \tau_i) \circ (\sigma^n \circ \tau_j)(\rho) \\
&= (\sigma^m \circ \tau_i)(\rho^j) \\
&= \Big[(\sigma^m \circ \tau_i)(\rho)\Big]^j \\
&= (\rho^i)^j \\
&= \rho^{ij}.
\end{aligned}$$

We similarly compute

$$\begin{aligned}
[\lambda(m,i) \circ \lambda(n,j)](\sqrt[p]{2}) &= (\sigma^m \circ \tau_i) \circ (\sigma^n \circ \tau_j)(\sqrt[p]{2}) \\
&= (\sigma^m \circ \tau_i)(\rho^n \sqrt[p]{2}) \\
&= \Big[(\sigma^m \circ \tau_i)(\rho)\Big]^n \cdot \Big[(\sigma^m \circ \tau_i)(\sqrt[p]{2})\Big] \\
&= \rho^{in} \cdot \rho^m \sqrt[p]{2} \\
&= \rho^{m+in} \sqrt[p]{2}.
\end{aligned}$$

These two computations together yield

$$\begin{aligned}
[\lambda(m,i) \circ \lambda(n,j)] &= \sigma^{m+in} \circ \tau_{ij} \\
&= \lambda(m+in, ij).
\end{aligned}$$

Recall from the definition of the semidirect product that

$$(m,i) \bullet (n,j) = (m + \varphi(i)(n), ij) = (m + in, ij).$$

Combining all of the above computations yields

$$\lambda(m,i) \circ \lambda(n,j) = \lambda\Big((m,i) \bullet (n,j)\Big),$$

so that λ is a homomorphism. Since λ is bijective, it is an isomorphism, as desired.

□

Problem 9.4

Recall that a finite group G is said to be solvable if there exists a chain of subgroups

$$1 = H_0 \subseteq H_1 \subseteq H_2 \subseteq \cdots \subseteq H_{k-1} \subseteq H_k = G$$

such that for each $i = 0, \ldots, k-1$, the subgroup $H_i \subseteq H_{i+1}$ is normal and $H_{i+1}/H_i \cong \mathbb{Z}/p_i$ for some prime p_i

(a) Show that any subgroup H of a solvable group is also solvable.

(b) If H is a normal subgroup of a finite group G, show that G is solvable if and only if both H and G/H are solvable.

(c) Show that every finite abelian group is solvable.

(d) Use (c) to conclude that in the definition of solvable, it is equivalent to require that the quotients H_{i+1}/H_i be abelian.

Throughout the argument below we'll use non-standard terminology that a chain of subgroups demonstrating solvability of a given group will be called a *solvable chain.*

(a) Let

$$1 = N_0 \subset N_1 \subset N_2 \subset \cdots \subset N_{k-1} \subset N_k = G$$

be a solvable chain for G, so that $N_{i+1}/N_i \cong \mathbb{Z}/p_i$ for some prime p_i. Let $H_i = N_i \cap H$. Then $H_k = H$ and $H_0 = 1$. I claim that for all i we have $H_{i+1}/H_i \cong \mathbb{Z}/p_i$ or $H_i = H_{i+1}$. Deleting repeat occurences of subgroups from this chain will then yield a solvable chain for H.

To prove the claim, note that for any i we have a commutative diagram of group homomorphisms.

$$\begin{tikzcd}
H \cap N_i \arrow[r, hook] \arrow[d, hook] & H \cap N_{i+1} \arrow[d, hook, "\iota"] \arrow[dd, bend left, "\psi"] \\
N_i \arrow[r, hook] \arrow[dr, "0"'] & N_{i+1} \arrow[d, two heads, "\pi"] \\
& N_{i+1}/N_i
\end{tikzcd}$$

with the hooked arrows being inclusions, and the arrow marked 0 sending every element to the identity. I claim that $\ker(\psi) = H \cap N_i$. Indeed, since $\ker(\pi) = N_i$, we have that $h \in \ker(\psi)$ if and only if $h \in H \cap N_{i+1} \cap N_i = H \cap N_i$. Since kernels of group homomorphisms are normal, we have that $H \cap N_i$ is a normal subgroup of $H \cap N_{i+1}$. Furthermore, the first isomorphism theorem yields

$$\frac{H \cap N_{i+1}}{H \cap N_i} \cong \mathrm{im}(\psi) \subset \frac{N_{i+1}}{N_i} \cong \mathbb{Z}/p_i.$$

Since p_i is a prime, Lagrange's theorem yields that $\mathrm{im}(\psi)$ is either the trivial subgroup or all of $\mathbb{Z}/p_i$. The former means $H \cap N_{i+1} = H \cap N_i$. The latter yields a desired link in the solvable chain. This is the desired dichotomy, and so the result holds.

□

(b) Here's the idea. Let $\pi : G \to G/H$ be the canonical projection homomorphisms. If we have a chain of subgroups of G, then intersecting with H and applying π yields chains of subgroups. We we have a chain of subgroups of H and a chain of subgroups of G/H, then including the chain from H into G and then extending this chain by taking the preimage under π of the chain in G/H yields a chain in G. Then it turns out that these operations send solvable chains to solvable chains. Now for the actual proof.

First let's suppose that G is solvable. Part (a) yields that H is solvable, so it suffices to show that G/H is solvable.

Let $\pi : G \to G/H$ be the canonical projection homomorphism. Let

$$1 = N_0 \subset N_1 \subset N_2 \subset \cdots \subset N_{k-1} \subset N_k = G$$

be a solvable chain for G. Let $F_i = \pi(N_i)$. I claim that

$$1 = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_{k-1} \subset F_k = G/H$$

is a solvable chain for G/H. Indeed, since group homomorphisms preserve the identity, we have that $\pi(1) = 1$, and since π is surjective, we have that $\pi(G) = G/H$, so this chain does end where we say it does.

To see that this is a solvable chain, note that we have a commutative diagram

$$\begin{tikzcd}
N_i \arrow[r, hook] \arrow[d, two heads] & N_{i+1} \arrow[d, two heads, "\pi"'] \arrow[dd, two heads, bend left=60, "\delta"] \\
F_i \arrow[r, hook] \arrow[dr, "0"] & F_{i+1} \arrow[d, two heads, "\gamma"] \\
 & \frac{F_{i+1}}{F_i}
\end{tikzcd}$$

with the hooked arrows inclusions, and the double headed arrows surjective. (Note π_{i+1} and γ are surjective by definition, so δ is surjective as a composition of surjections). Since *surjective* homomorphisms send normal subgroups to normal subgroups, each F_i is normal in F_{i+1}. Commutativity of the diagram yields that $N_i \subset \ker(\delta)$. Explicitly, if $n \in N_i$, then $\pi(n) \in \pi(N_i) = F_i$, so

$$\gamma \circ \delta(n) = \delta(n) = 0.$$

Since $\ker(\delta) \supset N_i$, we get another commutative diagram (feel free to ask Jarod or come to office hours about this)

$$\begin{tikzcd}
 & N_{i+1} \arrow[d, two heads, "\varphi"] \arrow[dr, two heads, "\delta"] & \\
\mathbb{Z}/p_i \arrow[r, "\cong"] & N_{i+1}/N_i \arrow[r, "\widetilde{\delta}"'] & F_{i+1}/F_i
\end{tikzcd}$$

Since δ is surjective, so is $\widetilde{\delta}$. To see this, let $y \in F_{i+1}/F_i$. Since δ is surjective, there is an $x \in N_{i+1}$ with $\delta(x) = y$. Then $\widetilde{\delta}(\varphi(x)) = \delta(x) = y$, so y is in the image of $\widetilde{\delta}$. So then $\#F_{i+1}/F_i$ divides $\#N_{i+1}/N_i = p_i$. Since p_i is prime, either $\#F_{i+1}/F_i = p_i$ or $\#F_{i+1}/F_i = 1$. In the first case, we have $F_{i+1}/F_i \cong \mathbb{Z}/p_i$, a link in the solvable chain. In the latter case, we have $F_i = F_{i+1}$, and we can throw out this repeat occurence. Either way, we have built up a solvable chain.

So now let's suppose H and G/H are solvable, and build up a solvable chain for G. Again, let $\pi : G \to G/H$ be the canonical projection.

Let

$$1 = F_0 \subset F_1 \subset \cdots \subset F_{k-1} \subset F_k = G/H.$$

be a solvable chain for G/H. Let $N_i = \pi^{-1}(F_i)$. Note that $N_k = G$ and $N_0 = H$. Once again, we have a commutative diagram

$$\begin{tikzcd}
\pi^{-1}(F_i) = N_i \arrow[r, hook] \arrow[d, two heads] & N_{i+1} \arrow[d, two heads, "\pi"'] \arrow[dd, two heads, bend left, "\delta"] \\
F_i \arrow[r, hook] \arrow[dr, "0"] & F_{i+1} \arrow[d, two heads, "\gamma"] \\
& \frac{F_{i+1}}{F_i} \cong \mathbb{Z}/p_i
\end{tikzcd}$$

Since $N_i = \pi^{-1}(F_i)$, we have that $\ker(\delta) = N_i$. Since kernels are normal we have that N_i is normal in N_{i+1}. Since δ is surjective, the first isomorphism theorem yields

$$\frac{N_{i+1}}{N_i} \cong \frac{F_{i+1}}{F_i} \cong \mathbb{Z}/p_i.$$

So we have built up a chain of normal subgroups

$$H = N_0 \subset N_1 \subset \cdots \subset N_k = G,$$

with each N_i normal in the following and quotients of prime order. Since H is solvable it has a solvable chain of subgroups. Tacking on this chain at the beginning of the above chain yields a solvable chain for G.

□

(c) Let G be a finite abelian group. We prove that G is solvable by induction on the order of G. The base case of $\#G = 1$ is fine, as the trivial group is also solvable.

Now suppose $\#G > 1$, and let p be a prime dividing $\#G$. Then by one of Cauchy's theorems, there exists an element $g \in G$ of order p. Thus, we have $\mathbb{Z}/p \cong \langle g \rangle \subset G$ (you could also get such a subgroup using the fundamental theorem of finitely generated abelian groups). Since G is abelian, every subgroup is normal. Furthermore, $G/\langle g \rangle$ has smaller order than G, so by induction $G/\langle g \rangle$ is solvable. Since $\mathbb{Z}/p$ is solvable, part (b) yields that G is solvable, as desired.

□

(d) Let

$$1 = H_0 \subset H_1 \subset \cdots \subset H_{k-1} \subset H_k \subset G$$

be a chain of subgroups with H_i normal in H_{i+1} and H_{i+1}/H_i a finite abelian group (they're all finite because G is finite by assumption). We prove by induction on i that each H_i is solvable, so taking $i = k$ yields G is solvable.

The base case $i = 0$ is trivial. For the inductive step, we suppose that H_i is solvable, and show that H_{i+1} is solvable. Since H_{i+1}/H_i is finite abelian, part (c) yields that this quotient is solvable. Part (b) yields that H_{i+1} is solvable. Thus, the result holds by induction.

□

Problem 9.5

(a) In problem 2 we showed $D_8 \cong \mathbb{Z}/4 \rtimes \mathbb{Z}/2$. As we remarked in part (c) of problem 2, this yields $\mathbb{Z}/2 \cong D_8/(\mathbb{Z}/4)$. Since $\mathbb{Z}/4$ and $\mathbb{Z}/2$ are solvable (being finite abelian groups), D_8 is solvable by problem 4 part (b).

(b) Let H be the following subset of A_4.

$$H = \{\text{id}, (12)(34), (13)(24), (14)(23)\}.$$

So H is the identity together with all the products of two disjoint transpositions. A quick computation shows that H is a subgroup of A_4, and that $H \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, so H is solvable. Furthermore, since H consists of all the permutations of a given cycle type, and conjugation in S_4 doesn't change the cycle type of a permutation, we have that H is normal in S_4, so also normal in A_4.

Furthermore, since $\#A_4 = 4!/2 = 12$, we have that $\#(A_4/H) = 12/4 = 3$, which is prime, so $A_4/H \cong \mathbb{Z}/3$, which is solvable. Thus A_4 is solvable by problem 4 part (b).

(c) Consider the sign homomorphism $\mathrm{sgn} : S_4 \to \mathbb{Z}/2$. This is surjective and by definition of the alternating group we have $A_4 = \ker(\mathrm{sgn})$. Since A_4 and $\mathbb{Z}/2$ are solvable, problem 4 part (b) yields that S_4 is solvable.