Problem §1

(a) Let N and H be groups and suppose that $\phi : H \to \mathrm{Aut}(N)$ is a homomorphism from H to the group of automorphisms of N. For $a \in H$, we write ϕ_a to denote the corresponding automorphism, so that $\phi_a(n) \in N$ for each $n \in N$. Now let $G = N \times H$ be the cartesian product of N and H and consider the following operation:

$$(n_1, h_1) \cdot_\phi (n_2, h_2) := (n_1 \phi_{h_1}(n_2), h_1 h_2).$$

Verify the following statements:

(a) The set G with $\cdot_\phi$ is a group.

(b) The set of elements of the form (n, e_H) is a **normal** subgroup of G isomorphic to N, and the set of elements of the form (e_N, h) is a subgroup (not necessarily normal) of G isomorphic to H.

The group G is called the **semi-direct product of** N **and** H and is denoted $N \rtimes_\phi H$. Note that the special case where ϕ is the identity automorphism gives rise to the usual direct product.

(b) Suppose that G is a group, N is a normal subgroup and H is a subgroup for with $G = NH$ and $N \cap H = \{e\}$. Let $\phi : H \to \mathrm{Aut}(N)$ be given by $\phi_h(g) = hgh^{-1}$, as worked through in Exercise 6.24(e). Prove that the map

$$\begin{aligned} f : N \rtimes_\phi H &\longrightarrow G \\ (n, h) &\longmapsto nh \end{aligned}$$

is an isomorphism. In this case, we say that G decomposes as the semi-direct product of N and H.

Solution:

(a) (a) Since ϕ_{h_1} is an isomorphism on N, $\phi_{h_1}(n_2) \in N$, so $n_1 \phi_{h_1}(n_2) \in N$ as well, and $\cdot_\phi$ is closed.
Let $(n_1, h_1), (n_2, h_2), (n_3, h_3) \in G$. Then

$$((n_1, h_1) \cdot_\phi (n_2, h_2)) \cdot_\phi (n_3, h_3) = (n_1 \phi_{h_1}(n_2), h_1 h_2) \cdot_\phi (n_3, h_3) = (n_1 \phi_{h_1}(n_2) \phi_{h_1 h_2}(n_3), h_1 h_2 h_3),$$

and

$$(n_1, h_1) \cdot_\phi ((n_2, h_2) \cdot_\phi (n_3, h_3)) = (n_1, h_1) \cdot_\phi (n_2 \phi_{h_2}(n_3), h_2 h_3) = (n_1 \phi_{h_1}(n_2 \phi_{h_2}(n_3)), h_1 h_2 h_3)).$$

But we know ϕ_{h_i} is an isomorphism, so

$$\phi_{h_i}(n_1 n_2) = \phi_{h_i}(n_1) \phi_{h_i}(n_2).$$

Additionally, ϕ is a homomorphism, so

$$\phi_{h_1 h_2} = \phi(h_1 h_2) = \phi(h_1)\phi(h_2) = \phi_{h_1}\phi_{h_2}.$$

Together, we then get

$$\phi_{h_1}(n_2 \phi_{h_2}(n_3))) = \phi_{h_1}(n_2) \phi_{h_1 h_2}(n_3).$$

Thus

$$((n_1, h_1) \cdot_\phi (n_2, h_2)) \cdot_\phi (n_3, h_3) = (n_1, h_1) \cdot_\phi ((n_2, h_2) \cdot_\phi (n_3, h_3)),$$

and so $\cdot_\phi$ is associative in G.
Since ϕ is a homomorphism, $\phi(e_H) = \phi_{e_H}$, the identity isomorphism in $\mathrm{Aut}(N)$. Then for any $(n, h) \in G$,

$$(e_N, e_H) \cdot_\phi (n, h) = (e_N \phi_{e_H}(n), e_H h) = (n, h).$$

Thus G has an identity element, namely $(e_N, e_H) \in G$.

Finally, for any $(n,h) \in G$, choose $(n^{-1}, h^{-1}) \in G$ (both of which exist since N, H are groups). Since ϕ is a homomorphism,

$$\phi(h)\phi(h^{-1}) = \phi(hh^{-1}) = \phi(e_H) = \phi_{e_H},$$

and similarly for $\phi(h^{-1})\phi(h)$. Thus

$$(n,h) \cdot_\phi (n^{-1}, h^{-1}) = (n\phi_{hh^{-1}}(n^{-1}), hh^{-1}) = (nn^{-1}, e_H) = (e_N, e_H),$$

and analogously for $(n^{-1}, h^{-1}) \cdot_\phi (n,h)$. Thus every element in G has an identity.

Therefore G with $\cdot_\phi$ is a group.

(b) Consider the subset of G,

$$G_N = \{(n, e_H) \in G \mid n \in N\}.$$

We first show this is a normal subgroup. Clearly, it is closed (since $n_1 n_2 \in N$ for any $n_1, n_2 \in N$), and it has the identity element $(e_N, e_H) \in G_N \subseteq G$ (since $e_N \in N$); finally, every $(n, e_H) \in G_N$ has a corresponding inverse $(n^{-1}, e_H) \in G_N$ (which is the inverse, as shown in part (a)(a) and since $e_H^{-1} = e_H$). To see why this is a normal subgroup, consider any $(n,h) \in G$, which has inverse $(n^{-1}, h^{-1}) \in G$. Then for any $(n', e_H) \in G_N$,

$$\begin{aligned}(n,h) \cdot_\phi (n', e_H) \cdot_\phi (n^{-1}, h^{-1}) &= (n\phi_h(n'), h) \cdot_\phi (n^{-1}, h^{-1}) \\ &= (n\phi_h(n')\phi_h(n^{-1}), hh^{-1}) \\ &= (n\phi_h(n'n^{-1}), e_H) \in G_N,\end{aligned}$$

since $\phi_h(n'n^{-1}) \in N$ and $n \in N$, so its product $n\phi_h(n'n^{-1}) \in N$ as well. Hence G_N is a normal subgroup of G. Isomorphism is simple; simply define a mapping

$$\psi : G_N \longrightarrow N,\ (n, e_H) \longmapsto n.$$

This is clearly an isomorphism (I spare the trivial demonstration of injectivity and surjectivity), so G_N is isomorphic to N.

Now, consider the subset of G,

$$G_H = \{(e_N, h) \in G \mid h \in H\}.$$

Clearly, it is closed: for any $(e_N, h_1), (e_N, h_2) \in G_H$,

$$(e_N, h_1) \cdot_\phi (e_N, h_2) = (e_N\phi_{h_1}(e_N), h_1 h_2) = (e_N, h_1 h_2) \in G_H$$

(isomorphisms, even homomorphisms, preserve the identity). Moreover, $(e_N, e_H) \in G_H$, since $e_H \in H$. Finally, every $(e_N, h) \in G_H$ has a corresponding inverse $(e_N, h^{-1}) \in G_H$. Hence G_H is a subgroup of G (note that it's not necessarily normal; for any non-identity $h' \in H$ and non-identity $(n,h) \in G$, the resulting first product from $(n,h)(e_N,h')(n^{-1},h^{-1})$ is $n\phi_{hh'}(n^{-1})$, which is not equal to e_N unless $\phi_{hh'} = \phi_{e_H}$, the identity automorphism). Isomorphism is analogous; a mapping

$$\psi : G_H \longrightarrow H,\ (e_N, h) \longmapsto h$$

is clearly an isomorphism, so G_H is isomorphic to H.

(b) Let G be a group, $N \trianglelefteq G$, and $H \leq G$ such that $G = NH$ and $N \cap H = \{e\}$. Let

$$\begin{aligned}\phi : H &\longrightarrow \mathrm{Aut}(N) \\ h &\longmapsto \phi_h,\ \phi_h(g) = hgh^{-1}\end{aligned}$$

be a group homomorphism from H to $\mathrm{Aut}(N)$ (since N is a normal subgroup), and consider the map

$$\begin{aligned}f : N \rtimes_\phi H &\longrightarrow G \\ (n,h) &\longmapsto nh.\end{aligned}$$

We first prove that f is a homomorphism.

Let $(n_1, h_1), (n_2, h_2) \in N \rtimes_\phi H$. Then

$$(n_1, h_1) \cdot_\phi (n_2, h_2) = (n_1 \phi_{h_1}(n_2), h_1 h_2).$$

We thus have

$$\begin{aligned} f(n_1 \phi_{h_1}(n_2), h_1 h_2) &= n_1 h_1 n_2 h_1^{-1} h_1 h_2 \\ &= n_1 h_1 n_2 h_2 \\ &= (n_1 h_1)(n_2 h_2) \\ &= f(n_1, h_1) \cdot f(n_2, h_2). \end{aligned}$$

Hence f is a group homomorphism.

For any $nh \in G$, simply choose $(n, h) \in N \rtimes_\phi H$; then

$$f(n, h) = nh,$$

and so f is surjective.

Next, we show that in general, if the intersection of two groups N and H, $N \cap H$, is trivial, then every element $nh \in NH$ is uniquely expressed by $n \in N$ and $h \in H$ (this directly shows injectivity of f, but is also applicable in future problems). Consider $n_1, n_2 \in N$ and $h_1, h_2 \in H$ such that $n_1 h_1 = n_2 h_2$. Then

$$n_2^{-1} n_1 h_1 h_1^{-1} = n_2^{-1} n_2 h_2 h_1^{-1} \implies n_2^{-1} n_1 = h_2 h_1^{-1} \in N \cap H = \{e\},$$

so $n_1 = n_2$ and $h_1 = h_2$. Thus every element $nh \in NH = G$ is uniquely expressed by $n \in N$ and $h \in H$. This also proves injectivity of f, since if $f(n_1, h_1) = n_1 h_1 = n_2 h_2 = f(n_2, h_2)$, then we need $(n_1, h_1) = (n_2, h_2)$.

Therefore f is an isomorphism, and so G decomposes as the semi-direct product of N and H.

Problem §2 Let G be a group of order $2p$ where p is some odd prime number. Prove that G is isomorphic to the cyclic group $\mathcal{C}_{2p}$ or to the dihedral group $\mathcal{D}_p$.

Solution: Suppose G has order $2p$; then G has 2-Sylow subgroups and p-Sylow subgroups. Inspecting the p-Sylow subgroups, let k be the number of p-Sylow subgroups of G. Sylow's theorem tells us that

$$k \mid 2p \text{ and } k \equiv 1 \mod p.$$

Hence $k = 1$; that is, G has a unique p-Sylow subgroup, say H_p. H_p is also normal, since for any $g \in G$ the conjugate subgroup $g^{-1} H_p g$ is also a subgroup of order p, and so equals H_p.

Next, Sylow's theorem also says that there exists at least one 2-Sylow subgroup, say H_2. From Remark 6.33, we have $H_2 \cap H_p = \{e\}$, so we can write

$$H_2 = \{e, a\}, \ H_p = \{e, b, b^2, \dots, b^{p-1}\}$$

(since all prime-order groups are cyclic); moreover, the only shared element is e.

Consider $aba^{-1} \in aH_p a^{-1} = H_p$; then

$$aba^{-1} = b^j \text{ for some } 0 \le j \le j-1.$$

We then get

$$\begin{aligned} b &= a^{-1} b^j a \\ &= (a^{-1} b a)^j \\ &= (a^{-1} a^{-1} b^j a a)^j \\ &= (a^{-2} b^j a^2)^j \\ &= b^{j^2}. \end{aligned}$$

Hence $b^{j^2} = b$, so $b^{j^2-1} = e$. Since b has order j, we get

$$j^2 \equiv 1 \pmod p, \text{ or } j^2 - 1 \equiv (j+1)(j-1) \equiv 0 \pmod p.$$

Thus $j = 1$ or $p-1$ (since $\mathbb{Z}/p\mathbb{Z}$ is an integral domain, or since d-degree polynomials in polynomial rings $F[x]$—where F is a field—have at most d distinct roots, etc).

If $j = 1$, then $aba^{-1} = b$, or $ab = ba$. Since every element of G is a power of a times a power of b, and elements in H_2 commute with elements in H_p, G is thus Abelian. Moreover, the element ab has order $2p$:

$$\begin{aligned} e = (ab)^k = a^k b^k &\implies a^k = b^{-k} \in H_2 \cap H_p = \{e\} \\ &\implies a^k = b^k = e \\ &\implies 2 \mid k \text{ and } p \mid k \\ &\implies 2p \mid k, \end{aligned}$$

where the last implication is true since p odd, so $\gcd(2,p) = 1$. Hence ab generates G, and so G is a cyclic group of order $2p$; that is, G is isomorphic to $\mathcal{C}_{2p}$.

If $j = p-1$, then $aba^{-1} = b^{p-1} = b^{-1}$. Since again, powers of a times powers of b completely form G, G thus has $2p$ elements of the form $a^i b^j$, $0 \le i \le 1$, $0 \le j \le p-1$, which have the following properties:

$$a^2 = e,\ b^p = e,\ ab^{-1} = ba,$$

which exactly defines the dihedral group $\mathcal{D}_p$.

Therefore, any group G with order $2p$ is isomorphic to either the cyclic group of order $2p$, $\mathcal{C}_{2p}$, or the dihedral group $\mathcal{D}_p$.

Problem §3

(a) If G is a group of order 60 that has a normal 3-Sylow subgroup, prove that G also has a normal 5-Sylow subgroup.

(b) If G is a non-cylic group of order 21, how many 3-Sylow subgroups does G have?

Solution:

(a) We start with three lemmas:

Lemma 1. *A p-Sylow subgroup of a group G is normal if and only if it is unique.*

Proof. Let G be a group, and suppose a p-Sylow subgroup H of G is normal. Suppose H' is another p-Sylow subgroup. By Sylow's theorem, any p-Sylow subgroups H_1 and H_2 are conjugates; that is, for some $g \in G$,

$$H_2 = g^{-1} H_1 g.$$

Thus

$$H' = g^{-1} H g$$

for some $g \in G$; but H is normal, so $g^{-1}Hg = H$ for any $g \in G$. Therefore $H = H'$, so H is the unique p-Sylow subgroup of G.

Conversely, suppose H is the unique p-Sylow subgroup of G. For any $g \in G$, the conjugate group $g^{-1}Hg$ is also a p-Sylow subgroup (since it has the same order), so uniqueness of p-Sylow subgroups forces

$$H = g^{-1} H g$$

for every $g \in G$. Thus H is normal. □

Lemma 2. *Suppose G is a group and N is a normal subgroup of G with order k. If the quotient group G/N has a normal subgroup of order m, then G has a normal subgroup of order km.*

Proof. Let $H = \{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_m\}$ be a normal subgroup of G/N with order m, where each $\mathcal{C}_i$ represent a distinct coset. Recall the natural group homomorphism

$$\phi : G \longrightarrow G/N, \ \phi(g) = gN.$$

We claim that the pre-image of H, say "$\phi^{-1}(H)$"$\subseteq G$, is a normal subgroup of G. Technically, this is an abuse of notation; there isn't a well-defined inverse function ϕ^{-1}, since ϕ isn't isomorphic, so when we say $\phi^{-1}(H)$ we really mean

$$\phi^{-1}(H) = \{g \in G \mid \phi(g) = gN \in H\} = \mathcal{C}_1 \cup \mathcal{C}_2 \cup \ldots \cup \mathcal{C}_m \subseteq G;$$

that is, the set of all $g \in G$ that are sent to some coset $\mathcal{C}_i$ in H. Since each coset has k elements, $\phi^{-1}(H)$ has km elements.

We first show that $\phi^{-1}(H)$ is closed. Let $g_1, g_2 \in \phi^{-1}(H)$, and consider $\phi(g_1 g_2) = g_1 g_2 N$. This is exactly equal to $g_1 N \cdot_{G/N} g_2 N$, and since $g_1 N, g_2 N \in H$ and H is a subgroup, we have $g_1 g_2 N \in H$ as well. Thus $g_1 g_2 \in \phi^{-1}(H)$.

Every coset of G/N has the identity element, including those in H, so $e \in \phi^{-1}(H)$. Since for any $gN \in H$ with $g \in \phi^{-1}(H)$, its inverse $g^{-1}N \in H$ as well (since $gNg^{-1}N = N = e_{G/H}$, and H is a subgroup), we have $g^{-1} \in \phi^{-1}(H)$ for any $g \in \phi^{-1}(H)$. Therefore $\phi^{-1}(H)$, the set of all elements in G are in some coset in H, is a subgroup of G with order km.

Since H is normal in G/N,

$$(aN)H(a^{-1}N) = H \text{ for any } aN \in G/N.$$

Additionally, recall that $G = \mathcal{C}_1 \cup \mathcal{C}_2 \cup \ldots \cup \mathcal{C}_{|G|/k}$, where $\mathcal{C}_i \in G/N$ are all elements of G/N; that is, G is the (disjoint) union of all cosets of N. This means that any element $a \in G$ has a corresponding coset $aN = \mathcal{C}_j \in G/N$ for some $\mathcal{C}_j \in G/N$. Together, this means that for any $gN \in H$, $aNgNa^{-1}N = aga^{-1}N \in H$ for any $a \in G$.

However, this means that for any $g \in \phi^{-1}(H)$, $aga^{-1} \in \phi^{-1}(H)$ for any $a \in G$ as well. Equivalently, $\phi^{-1}(H)$ is normal in G, as desired.

Therefore, if $|N| = k$ and G/N has a normal subgroup with order m, then G has a normal subgroup of order km. $\square$

Lemma 3. *Let H be a normal subgroup of a group G, and suppose H_p is a normal p-Sylow subgroup of H. Then H_p is a normal p-Sylow subgroup of G.*

Proof. Since H is normal in G, then $gHg^{-1} = H$ for every $g \in G$. Since H_p is a subgroup of H, then $gH_pg^{-1} \subseteq gHg^{-1} = H$. From Proposition 6.10(b) and since any subgroup H_p of a subgroup H of G is a subgroup of G itself, the conjugate set gH_pg^{-1} is a subgroup of G.

Indeed, the conjugate set gH_pg^{-1} is a subgroup of H, since gH_pg^{-1} already contains an identity and inverses for every element, all of which are in H, due to $gH_pg^{-1} \subseteq H$ and gH_pg^{-1} being a subgroup of G. Closure also holds: for any $gh_1g^{-1}, gh_2g^{-1} \in gH_pg^{-1}$, the product

$$gh_1g^{-1}gh_2g^{-1} = gh_1h_2g^{-1} = gh'g^{-1} \in gH_pg^{-1},$$

where $h_1, h_2 \in H$ and $h' = h_1h_2 \in H$.

Thus, gH_pg^{-1} is a subgroup of H for any $g \in G$; moreover, gH_pg^{-1} has the same order as H_p, namely p. However, since H_p is a normal p-Sylow subgroup of H—and thus unique, by Lemma 1—we need $H_p = gH_pg^{-1}$. Since the choice of $g \in G$ was arbitrary, H_p is thus a normal p-Sylow subgroup of G as well. $\square$

Now, suppose G is a group of order 60 with a normal 3-Sylow subgroup, say H_3. Then the group G/H_3 is well-defined, and by Lagrange it has order 20. Since $5 \mid 20$, Sylow's theorem tells us that G/H_3 has a 5-Sylow subgroup, say H_5'. By Sylow's theorem, if k represents the number of 5-Sylow subgroups of G/H_3, we must also have

$$k \mid 20 \text{ and } k \equiv 1 \pmod 5;$$

in other words, $k = 1$, and H_5' is unique and thus normal, by Lemma 1. But then Lemma 2 tells us that G has a normal subgroup of order 15, say H_{15}; applying Sylow's again gives a normal 5-Sylow subgroup H_5 of H_{15}. Lemma 3 finally tells us that H_5 is a normal 5-Sylow subgroup in G, as desired.

Therefore, if G is a group of order 60 that has a normal 3-Sylow subgroup, then G also has a normal 5-Sylow subgroup.

(b) Suppose G is a non-cyclic group of order 21. Since $21 = 3 \cdot 7$, G has a 7-Sylow subgroup, say H_7; moreover, H_7 is unique, since (letting k_7 represent the number of distinct 7-Sylow subgroups in G) we need

$$k_7 \mid 21 \text{ and } k_7 \equiv 1 \pmod 7,$$

or equivalently, $k_7 = 1$. Lemma 1 then tells us that H_7 is normal.

Now, let k_3 represent the number of distinct 3-Sylow subgroups of G. Sylow requires

$$k_3 \mid 21 \text{ and } k_3 \equiv 1 \pmod 3;$$

in other words, $k_3 = 1$ or 7.

If $k_3 = 1$, then Lemma 1 says that the unique 3-Sylow subgroup, say H_3, is normal. Since $\gcd(3,7) = 1$ and both H_3 and H_7 are normal, Exercise 6.22 tells us that elements of H_3 and H_7 commute with each other. If we represent the subgroups as

$$H_3 = \{e, a, a^2\}, H_7 = \{e, b, b^2, \ldots, b^7\}, \text{ and } H_3 \cap H_7 = \{e\} \text{ by Remark 6.33 },$$

one can verify (following an identical procedure as Problem 2) that elements in G are all powers of a times powers of b; and since any a^i commutes with any b^j for $0 \le i \le 2$, $0 \le j \le 6$, G is thus Abelian. Moreover, $|ab| = 21$ (again by proceeding analogously as Problem 2, or even Example 6.36; I won't regurgitate here), so G is cyclic, a contradiction of G non-cyclic.

Thus we need $k_3 = 7$; that is, if G is a non-cyclic group of order 21, then there are 7 distinct 3-Sylow subgroups of G.

Problem §4 (8.9) Let F be a finite field with q elements, and let $m \mid q-1$.

(a) Prove that F^* has a unique subgroup of order m.

(b) Let $\alpha \in F^*$. Prove that the following are equivalent:

- α is an m-th power in F, i.e. $\alpha = \beta^m$ for some $\beta \in F^*$.
- $\alpha^{\frac{q-1}{m}} = 1$.

This is known as *Euler's criterion*.

(c) Suppose that q is odd. Prove that

$$-1 \text{ is a square in } F^* \iff q \equiv 1 \pmod 4.$$

Solution: We begin with a lemma about cyclic groups.

Lemma 4. *Let G be a cyclic group with order n. For any divisor k of n ($k \mid n$), G has a unique cyclic subgroup with order k.*

Proof. Let $g \in G$ be a generator of G; that is, $\langle g \rangle = G$. If $k \in \mathbb{Z}_{>0}$ is a divisor of n, then $kq = n$ for some $q \in \mathbb{Z}_{>0}$, $1 \le q \le n$. Then the element $g^q \in G$ has order k, and so forms a cyclic subgroup $\langle g^q \rangle$ of G with order k.

To show uniqueness, suppose $\langle g^s \rangle$ is another cyclic group with order k (one can easily check that all subgroups of a cyclic group are cyclic). Then for any $g^{is} \in \langle g^s \rangle$, by Corollary 2.42 we have $(g^{is})^k = g^{kis} = e$; further, $n \mid kis$, so $\alpha n = kis$ for some $\alpha \in \mathbb{Z}$. But $n = kq$, so

$$\alpha n = kis \iff \alpha kq = kis \iff \alpha q = is.$$

Thus $g^{is} = g^{\alpha q}$ for every $g^{is} \in \langle g^s \rangle$; that is, every $g^{is} \in \langle g^s \rangle$ is some power of g^q. Thus $\langle g^s \rangle \subseteq \langle g^q \rangle$; equality comes since they have the same order. Hence $\langle g^q \rangle$ is the unique cyclic subgroup of G with order k. □

(a) By Corollary 8.10 (and further Remark 8.12), the unit group F^* is cyclic; from Lemma 1, since $m \mid q-1 = |F^*|$, F^* has a unique (cyclic) subgroup of order m, as desired.

(b) Suppose $\alpha = \beta^m \in F^*$ and $m \mid q-1$. Then $\langle \alpha \rangle = \langle \beta^m \rangle$ forms a cyclic subgroup of F^* with order $\frac{q-1}{m}$. In particular, $\alpha^{\frac{q-1}{m}} = e_{F^*} = 1$.

For the other direction, $\langle \alpha \rangle$ forms a unique cyclic subgroup of F^* with order $\frac{q-1}{m}$. Let $\beta \in F^*$ be a generator; then $\langle \beta^m \rangle$ forms a cyclic subgroup of order $\frac{q-1}{m}$ as well. Uniqueness of $\langle \alpha \rangle$ means that $\langle \alpha \rangle = \langle \beta^m \rangle$, so we can find some $\beta^{km} \in \langle \beta^m \rangle$ with $\left|\beta^{km}\right| = \frac{q-1}{m}$ such that $\beta^{km} = \alpha$. Slightly abusing notation and relabeling $\beta^k = \beta$, we have $\alpha = \beta^m$ for some $\beta \in F^*$, as desired.

(c) Let q be odd, and suppose that -1 is a square in F^*; that is, $-1 = \beta^2$ for some $\beta \in F^*$. From (b), we get that $(-1)^{\frac{q-1}{2}} = 1$; but $(-1)^2 = 1$, so -1 has order 2 and $2 \mid \frac{q-1}{2}$ by Lagrange. In other words, $2k = \frac{q-1}{2}$, or $4k = q-1$, or $q - 1 \equiv 0 \pmod 4$, or $q \equiv 1 \pmod 4$.

Conversely, suppose $q \equiv 1 \pmod 4$. Then $q - 1 = 4k$, or $\frac{q-1}{2} = 2k$, or $2 \mid \frac{q-1}{2}$. By elementary properties of rings, $(-1)^2 = 1$; and since $2 \mid \frac{q-1}{2}$, $(-1)^{\frac{q-1}{2}} = 1$ as well. A direct application of (b) thus leaves us with our desired result: -1 is a square in F, i.e. $-1 = \beta^2$ for some $\beta \in F^*$.

Problem §5 (8.11)

(a) Let $f(x) = x^4 - 1 \in \mathbb{Q}[x]$. Factor $f(x)$ into irreducible factors in $\mathbb{Q}[x]$, and then prove that $\mathbb{Q}(\sqrt{-1})$ is the splitting field of $f(x)$ over $\mathbb{Q}$.

(b) Let $f(x) = x^6 - 1 \in \mathbb{Q}[x]$. Factor $f(x)$ into irreducible factors in $\mathbb{Q}[x]$, and then prove that $\mathbb{Q}(\sqrt{-3})$ is the splitting field of $f(x)$ over $\mathbb{Q}$.

Solution:

(a) For $f(x) = x^4 - 1 \in \mathbb{Q}[x]$, we factor into

$$f(x) = x^4 - 1 = (x^2+1)(x^2-1) = (x+1)(x-1)(x^2+1),$$

where x^2+1 is irreducible in $\mathbb{Q}[x]$. The quadratic equation (or rudimentary algebraic experience) tells us we need

$$\frac{0 \pm \sqrt{0-4}}{2} = \frac{2\sqrt{-1}}{2} = \sqrt{-1},$$

which would factor x^2+1 into $(x+\sqrt{-1})(x-\sqrt{-1})$. Thus, for any F with $\sqrt{-1} \notin F$, $f(x)$ will not split completely in F. Proposition 5.15 tells us that $\mathbb{Q}(\sqrt{-1})$ is the smallest extension field of $\mathbb{Q}$ that contains both $\mathbb{Q}$ and $\pm\sqrt{-1}$; thus $\mathbb{Q}(\sqrt{-1})$ is the splitting field of $f(x)$ over $\mathbb{Q}$.

(b) For $f(x) = x^6 - 1 \in \mathbb{Q}[x]$, we factor into

$$f(x) = (x^2-1)(x^4+x^2+1) = (x+1)(x-1)(x^2+x+1)(x^2-x+1),$$

where $x^2 \pm x + 1$ is irreducible in $\mathbb{Q}[x]$. Using the quadratic formula, we need

$$\frac{\mp 1 \pm \sqrt{1-4}}{2} = \frac{\mp 1 \pm \sqrt{-3}}{2}$$

in order to factor $x^2 \pm x + 1$. Hence any splitting field must have both $\mathbb{Q}$ and $\sqrt{-3}$; Proposition 5.15 tells us that $\mathbb{Q}(\sqrt{-3})$ is the smallest such extension field that satisfies this. Thus $\mathbb{Q}(\sqrt{-3})$ is the splitting field of $f(x)$ over $\mathbb{Q}$.

Problem §6 (8.17) Let K be a field with p^d elements, so in particular K contains a copy of $\mathbb{F}_p$.

(a) Prove that there exists an element $\gamma \in K$ so that the evaluation map

$$E_\gamma : \mathbb{F}_p[x] \longrightarrow K$$

is surjective.

(b) Prove that $FF_p[x]$ contains an irreducible polynomial of degree d. (Hint: take a generator for the kernel of the evaluation map in (a)).

(8.18) Let K be a field with p^d elements. Prove that the following are equivalent:

(a) K contains a subfield with p^e elements.

(b) $e \mid d$.

Solution: Apologies, I have not the time to finish these problems :(If time permits, I will re-submit this PDF with solutions.