ALGEBRA I HOMEWORK I

HOJIN LEE 2021–11045

Problem 1. *Show that $\mathcal{P}(X)$ is a monoid wrt the binary operation of intersection, with identity $X \in \mathcal{P}(X)$. Given $f : X \to Y$, show $f^* : \mathcal{P}(Y) \to \mathcal{P}(X)$ is a monoid homomorphism.*

Proof. Suppose we are given the fact that $\mathcal{P}(X)$ is a set, and is unique. Define a binary operation $\cap : \mathcal{P}(X) \times \mathcal{P}(X) \to \mathcal{P}(X)$ by $(A, B) \mapsto \{x \in X \mid x \in A \wedge x \in B\}$. Associativity of $\cap$ follows from the associativity of conjunction in logic which we will not prove. Since $A \cap X = X \cap A = A$ for all $A \subset X$, X is the identity element.

Define $f^* : A \mapsto f^{-1}(A)$. Since f is a function, $f^{-1}(Y) = X$, so the identity maps to the identity. Suppose $A, B \subset Y$. We claim $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$. Suppose $x \in f^{-1}(A \cap B)$. Then $f(x) \in A \cap B \subset A, B$ so $x \in f^{-1}(A)$ and $f^{-1}(B)$. Conversely, suppose $x \in f^{-1}(A) \cap f^{-1}(B)$. Then $f(x) \in A \cap B$. □

Problem 2. *Let $S(X)$ the free monoid on X of finite sequences in X, with natural map $\delta : X \to S(X)$. Show for any monoid N and a function $f : X \to N$ there exists a unique monoid homomorphism $\phi_f : S(X) \to N$ such that $\phi_f \circ \delta = f$.*

Proof. The natural map $\delta : X \to S(X)$ is given by sending elements of x to the one-element sequence $(x) \in S(X)$. Suppose we have a monoid N and a function $f : X \to N$. Define $\phi_f : S(X) \to N$ as $(x_1, \dots, x_n) \mapsto f(x_1) *_N \cdots *_N f(x_n)$, and the identity (empty sequence) maps to the identity of N. Then $\phi_f((x_1, \dots, x_n, x_{n+1}, \dots, x_m)) = f(x_1) *_N \cdots *_N f(x_n) *_N f(x_{n+1}) *_N \cdots *_N f(x_m) = \phi_f((x_1, \dots, x_n)) *_N \phi_f((x_{n+1}, \dots, x_m))$ so ϕ_f is a monoid homomorphism. Since $\delta(x) = (x)$, and $\phi_f((x)) = f(x)$, we have $\phi_f \circ \delta = f$. Suppose we have another monoid homomorphism $\phi'_f : S(X) \to N$ such that $\phi'_f \circ \delta = f$. We want to show that $\phi'_f = \phi_f$. By the commuting condition, we must have $\phi_f((x)) = \phi'_f((x))$ for all $x \in X$. Also since ϕ'_f is a monoid homomorphism, we must have $\phi'_f((x_1, \dots, x_n)) = \phi'_f((x_1) \cdots (x_n)) = \phi'_f((x_1)) *_N \cdots *_N \phi'_f((x_n))$. But this is just $\phi_f((x_1)) *_N \cdots *_N \phi_f((x_n)) = \phi_f((x_1, \dots, x_n))$, so $\phi'_f = \phi_f$. □

Problem 3. *Prove or provide counterexample:*

1. *If $\mathrm{Aut}(G)$ cyclic then G abelian.*
2. *If G group and $H \leq G$ has finite index, then there exists $N \trianglelefteq G$ of finite index with $N \leq H$.*

Proof. 1. Consider the inner automorphism group $\mathrm{Inn}(G)$, which is a subgroup of $\mathrm{Aut}(G)$. This is the group of automorphisms of G defined by conjugation. Since subgroups of cyclic groups are cyclic we conclude that $\mathrm{Inn}(G)$ is also cyclic. Define a group homomorphism $\phi : G \to \mathrm{Inn}(G)$ by $g \mapsto \phi_g$ where $\phi_g(x) = gxg^{-1}$ for all $x \in G$. Since $e \mapsto \phi_e = 1_G$ and $gh \mapsto \phi_{gh} = \phi_g \circ \phi_h$, this is indeed a group homomorphism. Suppose $\phi_g = 1_G$. Then $gxg^{-1} = x$ for all $x \in G$, so $\ker \phi = Z(G)$

Date: March 10, 2024.

where $Z(G) = \{z \in G \mid zg = gz \ \forall g \in G\}$. Since ϕ is surjective, by the first isomorphism theorem, we have $G/Z(G) \cong \mathrm{Inn}(G)$ which is cyclic, say $\langle gZ(G) \rangle$. It follows that any element of G is of the form $g^n z$ for $z \in Z(G)$ and some $n \in \mathbb{Z}$. Since $g \cdot g^n z = g^{n+1} z = g^n g z = g^n z \cdot g$ for all $z \in Z(G)$ and $n \in \mathbb{Z}$, we conclude that g itself is in $Z(G)$, so $gZ(G) = Z(G)$. Therefore $G/Z(G) \cong \{\bullet\}$, which implies $G = Z(G)$, i.e. G is abelian. □

Proof. 2. Suppose $[G : H] = n$. Write

$$G = \bigsqcup_{1 \le i \le n} x_i H$$

for $x_i \in G$. We define a group homomorphism $G \to S_{G/H}$, where $S_{G/H}$ is the symmetric group on the set of left cosets of H in G. Define it by $g \mapsto \phi_g$ where $\phi_g : G/H \to G/H$ is a function on the set G/H, given by $xH \mapsto gxH$. Suppose $gxH = gyH$. It is obvious that $xH = yH$, so ϕ_g is injective, thus bijective since $|G/H| = n < \infty$. Therefore ϕ_g is indeed an element of $S_{G/H}$. Now since $e \mapsto \phi_e = 1_{G/H}$ and $fg \mapsto \phi_{fg} = \phi_f \circ \phi_g$, it follows that $\phi : g \mapsto \phi_g$ is a group homomorphism.

We claim that $\ker \phi \le H$. Suppose $\phi_g = 1_{G/H}$, i.e. $gxH = xH$ for all $x \in G$. In particular, $gH = H$ must hold, so g must be in H. Therefore $\ker \phi \le H$. Also, by the first isomorphism theorem, $G/\ker \phi \cong \mathrm{im}(\phi) \le S_{G/H}$, so $\ker \phi$ is a finite index $(= |\mathrm{im}(\phi)|)$ normal subgroup of G which is also a subgroup of H. □

Problem 4. *Let $\phi : G \to G'$ be a group homomorphism.*

1. *Show Γ_ϕ is a subgroup of $G \times G'$.*
2. *Show ϕ factors as $p \circ i$ where $i : G \to H$ and $p : H \to G'$ are injective, surjective homomorphism resp.*

Proof. 1. Obviously a subset of $G \times G'$. The identity element of $G \times G'$ is $(e_G, e_{G'})$. Since ϕ is a group homomorphism, it sends identities to identities, so Γ_ϕ has the identity. Also, $(x, \phi(x)) \cdot (y, \phi(y)) = (xy, \phi(xy))$, so Γ_ϕ is multiplicatively closed. The inverse of $(x, \phi(x))$ is $(x^{-1}, \phi(x^{-1}))$. □

Proof. 2. We claim that $\phi : G \to G'$ factors as $G \xrightarrow{i} G \times G' \xrightarrow{p} G'$. Define $i : G \to G \times G'$ as $g \mapsto (g, \phi(g))$, whose kernel is trivial so is injective. This is a group homomorphism since it sends identity to identity, and preserves the group law. Now define $p : G \times G' \to G'$ as $(g, g') \mapsto g'$, the projection on the second coordinate. This too is a group homomorphism quite obviously, and is surjective by definition. Then we can observe that $(p \circ i)(x) = p(x, \phi(x)) = \phi(x)$, so $p \circ i = \phi$. □

Problem 5. *Prove*

1. *We can identify N_i with a normal subgroup of G_i.*
2. *The image of H in $G_1/N_1 \times G_2/N_2$ is the graph of an isomorphism $G_1/N_1 \xrightarrow{\sim} G_2/N_2$.*

Proof. 1. Denote by i_1, i_2 the inclusion maps $N_1 \hookrightarrow H$, $N_2 \hookrightarrow H$, respectively. Consider the following diagram

$$\begin{tikzcd}
G_2 \cong \{e_1\} \times G_2 \arrow[r, hook, "\iota_2"] & G_1 \times G_2 \arrow[r, "\pi_1"] & G_1 \\
& N_2 \arrow[u, hook] \arrow[ul, dashed, "\exists! p_2 \circ i_2"] &
\end{tikzcd}$$

where ι_i are inclusion maps from G_i to $G_1 \times G_2$. By definition, N_2 sent through π_1 is zero, so by the universal property of the kernel, there exists a unique morphism from N_2 to $\ker \pi_1 \cong G_2$ that makes the diagram commute. This morphism is injective since both $N_2 \to G_1 \times G_2$ and $G_2 \to G_1 \times G_2$ are. We want to show that this map is $p_2 \circ i_2$. To show this, it suffices to show that $\iota_2 \circ p_2 \circ i_2$ is the inclusion of N_2 into $G_1 \times G_2$.

Consider the following diagram

$$\begin{tikzcd}
 & G_1 \times G_2 \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\
G_1 & N_2 \arrow[l, "0"] \arrow[r, "p_2 \circ i_2"'] \arrow[u, dashed, "\exists!"] & G_2 \arrow[ul, bend right, "\iota_2"']
\end{tikzcd}$$

where by the universal property of products, there exists a unique morphism from N_2 into $G_1 \times G_2$ that commutes with projections and arrows into G_i. First note that the inclusion $N_2 \to G_1 \times G_2$ commutes with other arrows by definition. To show that $\iota_2 \circ p_2 \circ i_2$ is the inclusion, we show it commutes with π_2 and $p_2 \circ i_2$. Consider $\pi_2 \circ \iota_2 \circ p_2 \circ i_2$. Since $\pi_2 \circ \iota_2 = 1_{G_2}$, this is just $p_2 \circ i_2$. The commutativity of the left hand side is obvious. Hence, $\iota_2 \circ p_2 \circ i_2$ is equal to the inclusion $N_2 \hookrightarrow G_1 \times G_2$, so by uniqueness we conclude that the injective morphism $N_2 \to G_2$ derived from the kernel is in fact $p_2 \circ i_2$. Since this is injective, we may identify N_2 with its image in G_2, and since $\operatorname{im}(p_2 \circ i_2) = p_2(N_2)$ where $N_2 \trianglelefteq H$ and p_2 surjective, is a normal subgroup in G_2. Vice versa for N_1 in G_1. □

Proof. 2. The image of H in $G_1/N_1 \times G_2/N_2$ is (h_1N_1, h_2N_2) where $(h_1, h_2) \in H$. Since p_i are surjective, H surjects onto G_i. For us to define a function $G_1/N_1 \to G_2/N_2$, we need to check well-definedness. Suppose $h_1N_1 = h_1'N_1$. We want to show this implies $h_2N_2 = h_2'N_2$ for all $(h_1, h_2), (h_1', h_2') \in H$. Using the fact that $h_1^{-1}h_1' = (h_1^{-1}h_1', e_2) \in N_1 \subset H$, and $(h_1^{-1}h_1', h_2^{-1}h_2') \in H$, we conclude that $(h_1^{-1}h_1', h_2^{-1}h_2')(h_1^{-1}h_1', e_2)^{-1} = (e_1, h_2^{-1}h_2') \in H$. This is obviously in the kernel of p_1, so is in N_2. Hence $h_2^{-1}h_2' \in N_2$, so $G_1/N_1 \to G_2/N_2$ is well-defined. This also defines a homomorphism due to the group structure on H. We can make this construction backwards, $G_2/N_2 \to G_1/N_1$ which sends for $(h_1, h_2) \in H$ as h_2N_2 to h_1N_1, and it is obvious that these two homomorphisms are inverses of each other. Therefore $G_1/N_1 \xrightarrow{\sim} G_2/N_2$, and the image of H is the graph of this isomorphism. □

Problem 6. *Prove the following*

1. $[G, G]$ *is a normal subgroup of* G *and* G^{ab} *is abelian*
2. *For any group homomorphism* $\phi : G \to A$ *with* A *abelian, there exists a unique morphism* $\overline{\phi} : G^{\mathrm{ab}} \to A$ *such that* $\phi = \overline{\phi} \circ \pi$.

Proof. 1. By definition $[G, G]$ is a subgroup of G. We want to show $[G, G]$ is invariant under conjugation. Consider $c \in [G, G]$ and any $g \in G$. Then $gcg^{-1}c^{-1} \in [G, G]$ by definition. Since $[G, G]$ is a subgroup, we have $gcg^{-1} \in [G, G]$, so $[G, G]$ is indeed invariant under conjugation. If we have $x[G, G]$ and $y[G, G]$, then since $x^{-1}y^{-1}xy \in [G, G]$ we have $x^{-1}y^{-1}xy[G, G] = [G, G]$ so it follows that $xy[G, G] = yx[G, G]$. □

Proof. 2. By context we assume $\pi : G \to G/[G, G]$ is the canonical projection. Suppose c is any commutator in G. Then $\phi(c) = e_A$. Since $[G, G]$ is generated by the set of all commutators of G, it follows that $\phi([G,G]) = \{e_A\}$. Hence $[G,G] \subset \ker\phi$, so by the universal property of the quotient group there exists such unique $\overline{\phi} : G^{\mathrm{ab}} \to A$. $\square$

ALGEBRA I HOMEWORK II

HOJIN LEE 2021–11045

Problem 1. *Solve the following*

1. *Find an example of a group G with at least two distinct (but equivalent) composition series.*
2. *Find an example of groups $K \leq H \leq G$ with $H \trianglelefteq G$ and $K \trianglelefteq H$ but $K \ntrianglelefteq G$.*
3. *Find an example of a nonabelian group G such that every subgroup is normal.*

Proof. 1. Let $G = \mathbb{Z}/6\mathbb{Z}$. Then $\langle 6 \rangle \leq \langle 2 \rangle \leq \langle 1 \rangle$ and $\langle 6 \rangle \leq \langle 3 \rangle \leq \langle 1 \rangle$ are two different composition series. They are indeed composition series since their quotients are simple. □

Proof. 2. Consider the subgroup $H = \{e, (12)(34), (13)(24), (14)(23)\}$ of A_4. If $\sigma \in S_4$, then $\sigma(ab)(cd)\sigma^{-1}$ sends $\sigma(a)$ to $\sigma(b)$, $\sigma(c)$ to $\sigma(d)$ and vice versa. Either way, this becomes an element of H, obviously. Thus $H \trianglelefteq S_4$ so $H \trianglelefteq A_4$. Also, H is a group of order 4 such that every nontrivial element has order 2, so $H \cong V_4$. The subgroup $\{e, (12)(34)\}$ of H is normal since H is abelian. However, $(123)(12)(34)(123)^{-1} = (14)(23)$, so H is not normal in A_4. □

Proof. 3. Consider the quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$. Since $ij = -ji$, this group is nonabelian. The nontrivial subgroups are ± 1, $\langle i \rangle$, $\langle j \rangle$, and $\langle k \rangle$, but index 2 subgroups are automatically normal, and ± 1 obviously is invariant under conjugation. Hence all subgroups are normal. □

Problem 2. *Let G a group, $N \trianglelefteq G$.*

1. *If $H \leq G$ is a subgroup where $N \cap H = \{e\}$ and $NH = G$, then G is a semidirect product of H and N, and write $G = N \rtimes H$. In this case, show $H \cong G/N$. If $G = N \rtimes H$, also show $N \times H \to G$ given by $(n, h) \mapsto nh$ is bijective, and it is a group homomorphism if and only if the group homomorphism $\varphi : H \to \mathrm{Aut}(N)$ given by $\varphi(h)(n) = hnh^{-1}$ is trivial.*
2. *Let $1 \to N \to G \xrightarrow{\pi} H \to 1$ be a SES of groups. A splitting of the SES is a group homomorphism $s : H \to G$ such that $\pi \circ s = \mathrm{id}_H$. Show if $s : H \to G$ is a splitting, then $G = N \rtimes s(H)$.*

Proof. 1. Define $f : H \to G/N$ as $h \mapsto hN$. This is obviously a group homomorphism. We claim that f is bijective. We want to show for any $g \in G$, there exists some $h' \in H$ such that $h'N = gN$. Since $G = NH$, we may write $g = n'h'$. Then $gN = n'h'N = h'N$, so f is surjective. Now suppose $hN = N$, i.e. $h \in N$. Then $h = e$ since $N \cap H = \{e\}$. Therefore $H \cong G/N$.

Date: March 20, 2024.

The set map $(n, h) \mapsto nh$ is surjective, since $G = NH$. Suppose $nh = n'h'$. It follows that $n = n'h'h^{-1}$, so $h'h^{-1} \in N$, i.e. $h'h^{-1} = e$. Then $h' = h$. From right cancellation, it also follows that $n = n'$. Thus the set map is bijective.

Suppose $\varphi : H \to \mathrm{Aut}(N)$ is trivial, i.e. $hnh^{-1} = n$ for all $n \in N$ and $h \in H$. For the map to be a group homomorphism, we must have $nn'hh' = nhn'h'$ for all $n, n' \in N$ and $h, h' \in H$. This holds.

Conversely, if $nn'hh' = nhn'h'$ for all n, n', h, h', and take $n = h' = e$, then we get $n'h = hn'$ for all n' and all h. Thus $hnh^{-1} = n$ for all n, h, so φ is trivial. □

Proof. 2. Suppose $s : H \to G$ such that $\pi \circ s = \mathrm{id}_H$. We first show that $N \cap s(H) = \{e\}$ and $Ns(H) = G$. Suppose $g \in s(H) \cap N$. Then, $\pi(g) = e$ by exactness. But, $\pi \circ s = \mathrm{id}_H$, so if $h \in H$ such that $s(h) = g$, then $\pi(s(h)) = e = h$. Therefore $h = e$, so $g = s(e) = e$.

To show $G = Ns(H)$, it suffices to show that every coset gN of N in G can be represented by an element of $s(H)$. Consider the images through π, given by $g \mapsto \pi(g)$ and $s(\pi(g)) \mapsto \pi(s(\pi(g))) = \pi(g)$. It follows that $\pi(g^{-1}s(\pi(g))) = e$, so $g^{-1}s(\pi(g)) \in N$, i.e. $gN = s(\pi(g))N = Ns(\pi(g))$. Therefore, every element of G can be written as an element of $Ns(H)$. It follows that $G = N \rtimes s(H)$. □

Problem 3. *Let H and N be groups, and let $\varphi : H \to \mathrm{Aut}(N)$ be a group homomorphism.*

1. *Show that we can endow the set $N \times H$ with the structure of a group via*

$$(n, h)(n', h') = (n(\varphi(h)(n')), hh').$$

Write $N \rtimes_\varphi H$ for the resulting group. Observe $N \rtimes_\varphi H = N \times H$ preciesly when φ is trivial.

2. *Identifying N and H with the subgroups $N \times \{1\}$ and $\{1\} \times H$ of $G = N \rtimes_\varphi H$, show that*
   (a) *$nh = (n, h)$ for all $n \in N$ and $h \in H$,*
   (b) *$N \trianglelefteq G$ and*
   (c) *$\varphi(h)(n) = hnh^{-1}$ for all $h \in H$ and $n \in N$.*
   Conclude that $G = N \rtimes H$ and $(n, h)(n', h') = (nhn'h^{-1}, hh')$ for all $(n, h), (n', h') \in G$.

Proof. 1. We show that the operation has identity, is associative, and has inverse.

Consider $(e_N, e_H) \cdot (n, h)$. This is $(e_N(\varphi_{e_H}(n)), h) = (n, h)$. Also, $(n, h) \cdot (e_N, e_H) = (n(\varphi_h(e_N)), h) = (n, h)$, so (e_N, e_H) is the identity.

Now we show $(n_1, h_1) \cdot (n_2, h_2) \cdot (n_3, h_3)$ is well-defined. First, $(n_1, h_1) \cdot (n_2, h_2) = (n_1\varphi_{h_1}(n_2), h_1h_2)$, and multiplying again with (n_3, h_3) results in

$$(n_1\varphi_{h_1}(n_2)\varphi_{h_1h_2}(n_3), h_1h_2h_3).$$

Now in the other direction, $(n_2, h_2) \cdot (n_3, h_3) = (n_2\varphi_{h_2}(n_3), h_2h_3)$, and again multiplying with (n_1, h_1) on the left makes $(n_1\varphi_{h_1}(n_2)\varphi_{h_1h_2}(n_3), h_1h_2h_3)$. The two agree, so the operation is associative.

Now we claim that $(n, h)^{-1} = (\varphi_{h^{-1}}(n^{-1}), h^{-1})$. Multiply by (n, h) on the right to get $(\varphi_{h^{-1}}(n^{-1})\varphi_{h^{-1}}(n), h^{-1}h) = (e_N, e_H)$. The same holds on the left. Note that $n\varphi_h(n') = nn'$ for all n, n', h if and only if $\varphi_h = \mathrm{id}_N$ for all h, i.e. φ is trivial. □

Proof. 2. (a) $nh = (n, 1) \cdot (1, h) = (n\varphi_1(1), h) = (n, h)$.

(b) We show that $(n,h)\cdot N\cdot(n,h)^{-1}\subset N$. Suppose we have $(n',1)$. Then, $(n,h)\cdot(n',1)\cdot(n,h)^{-1}=(n\varphi_h(n'),h)\cdot(n,h)^{-1}=(n\varphi_h(n'),h)\cdot(\varphi_{h^{-1}}(n^{-1}),h^{-1})=(n\varphi_h(n')n^{-1},1)\in N$.

(c) $hnh^{-1}=(1,h)\cdot(n,1)\cdot(1,h)^{-1}=(1,h)\cdot(n,1)\cdot(\varphi_{h^{-1}}(1),h^{-1})=(1,h)\cdot(n,1)\cdot(1,h^{-1})=(\varphi_h(n),h)\cdot(1,h^{-1})=(\varphi_h(n),1)\sim\varphi_h(n)$.

Therefore, $N\cap H=\{1\}\times\{1\}$, and $NH=G$ by (a), so we have $G=N\rtimes H$. Also, since $\varphi_h(n)=hnh^{-1}$, we have $(n,h)\cdot(n',h')=(nhn'h^{-1},hh')$. □

Problem 4. *Let p,q be prime. Show that a group of order p^2 is abelian, and that there are only two such groups up to isomorphism.*

Proof. Using the class formula $|G|=|Z(G)|+\sum_x[G:G_x]$ where x runs through non central elements of G, and G acts on itself by conjugation, we conclude that since $|G|=p^2$, and each $[G:G_x]$ is divisible by p, that $|Z(G)|$ must be divisible by p. Thus $|Z(G)|$ is either of order p or order p^2. In the latter case, $G=Z(G)$ so G is abelian. In the former case, $G/Z(G)$ is a group of order p, hence cyclic. In homework I, we have proved that if $G/Z(G)$ is cyclic, then it must be trivial. Therefore the former case cannot even happen, so G is abelian. Since G is abelian in all cases, we may use the structure theory of finitely generated abelian groups to conclude there exist only two up to isomorphism, namely $\mathbb{Z}/p^2\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$. □

Problem 5. *Let p,q be distinct primes. Prove that a group of order p^2q is solvable, and one of its Sylow subgroups is normal.*

Proof. First assume $q<p$. Then q is the smallest prime dividing $|G|$. Also, by the Sylow theorems there exist a Sylow-p subgroup H. Then $[G:H]=q$, so by Lemma 6.7 we have $1\trianglelefteq H\trianglelefteq G$. By Problem 4, we know that H is abelian. Also, $|G/H|=q$, so $G/H\cong\mathbb{Z}/q\mathbb{Z}$. Hence G is solvable.

Now suppose $p<q$. Again by the Sylow theorems, there exists a subgroup H of order q, and $n_q\equiv 1 \mod q$. Note that $n_q=|\operatorname{orb}(H)|=[G:N_G(H)]$, where since $[G:H]=p^2$, n_q must divide p^2. Therefore, $n_q=1,p,p^2$. However $n_q\neq p$ since otherwise $p=1+nq$ for $n>0$, but by assumption $p<q$. Thus we have two possibilities; $n_q=1$ or $n_q=p^2$.

Suppose $n_q=1$. Since all Sylow q-subgroups are conjugate, H is self-conjugate, i.e. is normal. Therefore $1\triangleleft H\triangleleft G$, where $H\cong\mathbb{Z}/q\mathbb{Z}$ and G/H is abelian, again by Problem 4. In this case G is solvable.

Now suppose $n_q=p^2$. Then each of the p^2 Sylow q-subgroups has $q-1$ elements of order q, and in this case distinct Sylow q-subgroups intersect trivially, we conclude G has $p^2(q-1)$ elements of order q. Thus G has p^2 elements of order not q. We also know that there exists a Sylow p-subgroup of order p^2, and all elements of such subgroup must have order dividing p^2. If the order divides p^2, then it certainly is not q, so the p^2 elements having order not q are contained in a Sylow p-subgroup, and in fact they form this unique p-subgroup, since elements either have order q or not. Denote this Sylow p-subgroup as P. By uniqueness $1\trianglelefteq P\trianglelefteq G$, and $G/P\cong\mathbb{Z}/q\mathbb{Z}$, also P is of order p^2, hence abelian. □

Problem 6. *Let p,q be odd primes. Prove that a group of order $2pq$ is solvable.*

Proof. In the case $p=q$, the group G has a Sylow p-subgroup of index 2, which is normal. If we call this H, then H has order p^2, and $G/H\cong\mathbb{Z}/2\mathbb{Z}$ so G is solvable.

WLOG let $p < q$. By the Sylow theorems, there exists a subgroup of order q, and $n_q \equiv 1 \bmod q$, and n_q must divide $2p$. Thus n_q may be one of $1, 2, p, 2p$. Since 2 and p are impossible, $n_q = 1, 2p$.

Suppose $n_q = 1$. Then there exists a unique Sylow q-subgroup, which is normal. Call this H. Then we have $1 \trianglelefteq H \trianglelefteq G$, where G/H is of order $2p$. Order $2p$ groups are solvable, since by the Sylow theorems we have a subgroup of order p, and its index is 2, so it is normal. The quotients are $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$ respectively, thus G/H is solvable. Since G/H and H are solvable, G is solvable.

Now suppose $n_q = 2p$. There are $2p$ Sylow q-subgroups, each having $q - 1$ elements of order q, so G has $2p(q - 1)$ elements of order q. Therefore, G has $2p$ elements having order not q. Also, by the Sylow theorems, there exists a Sylow p subgroup, and $n_p = 1, q, 2q$. Since all Sylow p-subgroups intersect trivially (if they share a nontrivial element, they are the same, since they are cyclic) if we have $n_p = q$ or $2q$, then we would have $q(p - 1)$ or $2q(p - 1)$ elements having order p. We claim that $q(p - 1) > 2p$, which implies that $n_p = q$ or $2q$ cannot happen.

Since we assumed $p < q$, we know $q \geq 5$. Hence $q - 2 \geq 3 \Rightarrow \frac{2}{3} \geq \frac{2}{q-2} \Rightarrow 1 + \frac{2}{q-2} \leq \frac{5}{3}$, and also p is an odd prime so $p > 2$. Thererfore $1 + \frac{2}{q-2} \leq \frac{5}{3} < p \Rightarrow q < pq - 2p \Rightarrow 2p < q(p - 1)$.

Therefore $n_p = 1$, so there is a unique Sylow p-subgroup of G, say H. Then H is normal, so $1 \triangleleft H \triangleleft G$, where G/H is of order $2q$. As we argued above, order $2q$ groups are solvable. Therefore G is solvable. □

Problem 7. *Show every group of order* < 60 *is solvable, and find a non-solvable group of order 60.*

Proof. We consider the cases of order p^k, $p^k m$ where $1 < m < p$, and where $m! < p^k m$. We already know that all order p^k groups are solvable.

Now suppose $|G| = p^k m$ where $1 < m < p$. Then by Sylow theorems, there exists a Sylow p-subgroup where $n_p \equiv 1 \bmod p$, and n_p divides m. For this to happen, n_p must be 1, since otherwise n_p exceeds m. Therefore this Sylow p-subgroup is unique, hence normal, and the quotient group is of order m.

This time suppose $|G| = p^k m$ where $m! < |G|$. Let P denote the set of Sylow p-subgroups of G. Define a homomorphism $G \to S_P$ by conjugation action, where $|P|$ is at most m, so $|S_P| \leq m! < p^k m = |G|$. The kernel of this homomorphism must be nontrivial. If the kernel is all of G, then $|P| = 1$, so (by abuse of notation) $P \trianglelefteq G$, and G/P is of order m, and P is solvable.

In both cases, solvability of the group depends on the solvability of the group of order m. We want that m is again of the form $q^k m'$ for some prime q, and some m' satisfying either of the two conditions. Therefore, it is enough to check numbers below 60 that do not satisfy the above conditions.

First, numbers of the form pq for distinct primes, take the larger one to be p. For numbers $p^2 q$, we need not treat them since we already proved such groups are solvable in Problem 5. Now we look at numbers of the form $p^3 q$. If $q < p$, we are done. If $p < q$, we need $(q - 1)! < p^3$. Such (p, q) that are possible are $(2, 3), (2, 5), (2, 7)$, but $(2, 5)$ and $(2, 7)$ do not satisfy $(q - 1)! < p^3$ since $8 < 24$ and $8 < 6!$. Therefore we need special proofs for order 40, 56. Now look at numbers of the form $p^4 q$. Again, if $q < p$ we are done. If $p < q$, the only possible combination is $(2, 3)$, and since $2! < 2^4$ this satisfies the conditions.

Now we look at numbers of the form pqr, for $p < q < r$ primes. In this case, the only two possible combinations are $(2, 3, 5)$ and $(2, 3, 7)$ which are of the form $2pq$, which we know to be solvable. The smallest number not of the forms listed above is $60 = 2^2 \times 3 \times 5$, so all we need to prove is for order 40 and 56.

Since $40 = 5 \times 8$, we must have $n_5 \equiv 1 \mod 5$, and must divide 8, so $n_5 = 1$. Call this normal subgroup H, then G/H is of order 8, hence solvable, and H itself is cyclic so is solvable.

Now consider a group of order $56 = 2^3 \times 7$. We have $n_7 \equiv 1 \mod 7$, and must divide 8 so is either 1 or 7. If $n_7 = 1$, there is nothing else to prove. Suppose $n_7 = 8$. Then each Sylow 7-subgroup has 6 elements of order 7, so G has $6 \times 8 = 48$ elements of order 7. Therefore G has 8 elements of order not 7. Since this group has a Sylow 2-subgroup of order 8, such group must be unique, otherwise there are more than 8 elements of order not 7. Hence the Sylow 2-subgroup is unique, thus normal, and the quotient has order 7 thus cyclic. Therefore all groups of order < 60 are solvable!

We claim that A_5, of order 60, is not solvable. Since A_5 is nonabelian, it suffices to show that A_5 is simple. In class, we showed that A_5 is generated by 3-cycles, so it suffices to show that all 3-cycles of A_5 are conjugate, and show that every nontrivial normal subgroup contains a 3-cycle.

Suppose we have $(x_1x_2x_3)$ and $(y_1y_2y_3)$ as 3-cycles in A_5. Denote by x_4, x_5 and y_4, y_5 the remaining symbols, respectively. Note that there exists a permutation σ sending x_i to y_i for $1 \leq i \leq 5$, and if this σ has negative sign, then compose σ with (x_4x_5) to get an element of A_5. This still sends $(x_1x_2x_3)$ to $(y_1y_2y_3)$ since it doesn't interfere with $1 \leq i \leq 3$. Notice that $\sigma(x_1x_2x_3)\sigma^{-1} = (y_1y_2y_3)$ via checking where each y_i maps to.

Now suppose $1 \neq N \trianglelefteq A_5$. If N does not contain a 3-cycle, then it either contains the product of two disjoint transpositions, or a 5-cycle. This is because elements of A_5 are either the identity, a 3-cycle, a 5-cycle, or a proudct of two disjoint transpositions. If N contains a 5-cycle, then N contains all 5-cycles, since by the Sylow theorems we know that elements of order 5 are contained in Sylow 5-subgroups, and these subgroups are all conjugate to one another. Together with the fact that N is normal, this implies N contains all 5-cycles. Then just take $(12345)(12543) = (132) \in N$. If N contains the product of two disjoint transpositions, say $(ab)(cd)$, then for $\sigma \in A_5$, $\sigma(ab)(cd)\sigma^{-1}$ sends $\sigma(a)$ to $\sigma(b)$ and $\sigma(c)$ to $\sigma(d)$. Setting $\sigma(e) = e$ and by changing the alphabets, this can be the product of any two disjoint transpositions in A_5. Thus N contains all such elements. Then, take $(12)(34)(12)(35) = (354)$. $\square$

Problem 8. *Let G be a finite group.*

1. *Let H be a proper subgroup of G. Show G is not the union of all the conjugates of H.*
2. *Suppose G acts transitively on a set S with $|S| \geq 2$. Prove that there is an element $x \in G$ such that $xs \neq s$ for all $s \in S$.*

Proof. 1. Let $[G : H] = n$. We have $|G| = n|H|$ for $n > 1$. Also, conjugates gHg^{-1} of H are subgroups of G, since they contain the identity and are multiplicatively closed. Since conjugation is bijective on G, we conclude that there are at most n distinct gHg^{-1}'s. Since each gHg^{-1} contains the identity, there are at most

$n(|H|-1)+1$ distinct elements in $\bigcup_{g\in G} gHg^{-1}$. We assumed $1-n<0$ so this is strictly less than $n|H|=|G|$. $\square$

Proof. 2. Suppose each $g \in G$ has a fixed point. Therefore we have $\sum_{x\in S}|G_x| > |G|$, since each $g \in G$ belongs to one of the G_x, and each G_x all contains e (and $|S|>1$). By Problem 9, we know that $\sum_{x\in S}|G_x| = |G\backslash S||G|$, so $|G\backslash S|>1$. Therefore the G-action cannot be transitive. $\square$

Problem 9. *Let G be a finite group acting on a finite set S. For each $x \in G$ let $F(x) = |\{s \in S \mid xs = s\}|$. Show $|G\backslash S| = \frac{1}{|G|}\sum_{x\in G} F(x)$.*

Proof. We first construct a bijection between $\operatorname{orb}(x)$ and the set of left cosets G/G_x of the stabilizer subgroup G_x of x in G. Given gx in the orbit, send this to gG_x. If $gx = g'x$, then $g^{-1}g'x = x$, so $g^{-1}g' \in G_x$ which implies $gG_x = g'G_x$. Therefore, this function is well-defined. This is obviously surjective, and suppose $gG_x = g'G_x$. Then $g^{-1}g' \in G_x$, so $g^{-1}g'x = x$, so $g'x = gx$. Hence this correspondence is bijective.

Now, notice that

$$|G\backslash S| = \sum_{\text{orbit}\in G\backslash S} 1 = \sum_{\text{orbit}\in G\backslash S}\sum_{x\in\text{orbit}} \frac{1}{|\operatorname{orb}(x)|} = \sum_{x\in X}\frac{1}{|\operatorname{orb}(x)|}.$$

Also, by the bijective correspondence above, we have $|\operatorname{orb}(x)| = |G|/|G_x|$ so

$$\begin{aligned} |G\backslash S| &= \sum_{x\in X} |G_x|/|G| \\ &= \frac{1}{|G|}\sum_{x\in X}|G_x| \\ &= \frac{1}{|G|}\#(\{(g,x)\in G\times X \mid gx = x\}) \\ &= \frac{1}{|G|}\sum_{g\in G} F(g). \end{aligned}$$

$\square$

ALGEBRA I HOMEWORK III

HOJIN LEE 2021–11045

Problem 1. *Let $n \in \mathbb{N}$. Write down a formula for the order of the conjugacy class of an element of S_n with cycle type $\{k_1, \ldots, k_m\}$.*

Proof. By the lecture notes, we know that elements of S_n are conjugate if and only if they have the same cycle type. Assume $k_1 \leq k_2 \leq \cdots \leq k_m$. We wish to find the number of distinct elements of S_n that have the same cycle type. To do this, we partition a permutation sequence of 1 through n into m parts via $k_1, \ldots, k_m$, and divide out $n!$ by the number of duplicates. For each cycle of length k_i, there are k_i ways to write the same k_i-cycle, so we must first divide out by $\prod_{i=1}^{m} k_i$. Also, if we write a_i as the number of elements equal to i in the cycle type, we can find out that $\prod_{i=1}^{m} k_i = \prod_i (i)^{a_i}$. Also, for each i-cycle there are $a_i!$ ways to rearrange each i-cycle, so we must divide out by $\prod_i a_i!$. Combining these, we conclude that the order of the conjugacy class is $n!/\prod_i (i)^{a_i}(a_i!)$, where a_i is the number of i's in the cycle type. $\square$

Problem 2. *Let $n \in \mathbb{N}$. Solve the following:*

1. *Show $S_n = \langle (12), (13), \ldots, (1n) \rangle$.*
2. *Show $S_n = \langle (12), (23), \ldots, (n-1, n) \rangle$.*
3. *Show $S_n = \langle (12), (1 \cdots n) \rangle$.*
4. *Show that if n is prime, $\sigma \in S_n$ any n-cycle, and $\tau \in S_n$ any transposition, then $S_n = \langle \sigma, \tau \rangle$.*

Proof. 1. Elements of S_n have a cycle decomposition, and any cycle $(a_1 a_2, \ldots, a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_2)$. Therefore S_n is generated by transpositions, and it suffices to show that we can make any transposition with the given $(1k)$. Suppose we have a transposition (ab). Then, this is equal to $(1a)(1b)(1a)$, since $a \mapsto 1 \mapsto b$ and vice versa. Therefore, any transposition can be made, so S_n can be generated. $\square$

Proof. 2. Since $(k\ \ k+1) = (1\ \ k+1)(1\ \ k)(1\ \ k+1)$, we have $(23) = (12)(13)(12)$, $(34) = (13)(14)(13)$ and so on. Therefore we have $(13) = (12)(23)(12)$, $(14) = (13)(34)(13)$ and so on. Therefore, $(1k) \in \langle (12), (23), \ldots, (n-1, n) \rangle$ for all k, so it is S_n indeed. $\square$

Proof. 3. Note that $(1 \cdots n)(12)(1 \cdots n)^{-1} = (23)$, and in general $(1 \cdots n)(k\ \ k+1)(1 \cdots n)^{-1} = (k+1\ \ k+2)$. Therefore we may obtain $(12), (23), \ldots, (n-1, n)$ which generated S_n as we showed above. $\square$

Proof. 4. Suppose we have σ any n-cycle, and $\tau = (ab)$. Suppose $\sigma^k(a) = b$ for some k. Then since $\langle \sigma^k \rangle \leq \langle \sigma \rangle$, the order of σ^k must divide n, and since $\sigma^k \neq e$, we conclude that σ^k is of order n. Since n is prime, we conclude that σ^k is an n-cycle, since the order of an element equals the lcm of each cycle. Therefore,

Date: March 26, 2024.

by replacing σ with σ^k it suffices to show that $(ab), (abc\cdots)$ generates $S_{\{a,b,c,\ldots\}}$. Under the bijective correspondence $1 = a$, $2 = b$, $3 = c$ and so on, this is equivalent to showing the permutation group on $\{1, 2, \ldots, n\}$, i.e. S_n, is generated by (12) and $(1 \cdots n)$. This is what we showed above. $\square$

Problem 3. *Let $n \geq 3$.*

1. *For each $j \in J = \{1, \ldots, n\}$, let H_j be the stabilizer of j in A_n. Show that $[A_n : H_j] = n$, and that $H_j \cong A_{n-1}$ for all $j \in J_n$.*
2. *Suppose $H \leq A_n$ is a subgroup of index n. Show that $H \cong A_{n-1}$ by showing that the left translation action of A_n on A_n/H induces an isomorphism $H_1 \cong H$.*

Proof. 1. Elements of H_j are elements of A_n that leave j fixed, i.e. even permutations on the set $J \setminus \{j\}$. This is exactly A_{n-1}, so $H_j \cong A_{n-1}$. This automatically implies $[A_n : H_j] = n$. $\square$

Proof. 2. Consider the homomorphism $\psi : A_n \to S_{A_n/H}$ given by $x \mapsto \varphi_x$ where $\varphi_x(aH) = xaH$. Since $xaH = xbH$ implies $aH = bH$, φ_x is an injective map from $S_{A_n/H}$ to itself, thus bijective, and indeed $\varphi_x \in S_{A_n/H}$. In the previous homework, we showed that A_n is simple for $n \geq 5$, using the fact that it is generated by 3-cycles, all 3-cycles are conjugate, and every nontrivial normal subgroup contains a 3-cycle. (Frankly, I have only showed it for A_5, but this generalizes easily.) By the previous homework, we know that for a finite group, the whole group cannot be the union of the conjugates of a proper subgroup. Therefore, we know that $A_n \neq \bigcup_{a \in A_n} aHa^{-1}$, so there must exist some $x \in A_n$ such that $x \notin aHa^{-1}$ for all $a \in A_n$. Then, it follows that φ_x is not the identity, since $x \notin aHa^{-1} \Rightarrow xaH \neq aH \Rightarrow \varphi_x \neq \mathrm{id}_{S_{A_n/H}}$. Therefore the homomorphism ψ is not trivial, so $\ker \psi$ is a proper normal subgroup of A_n.

For $n \geq 5$, this implies that $\ker \psi = \{e\}$, i.e. ψ is injective. Then A_n can be identified with its image $\psi(A_n)$ in $S_{A_n/H}$, and same for $H \leq A_n$. Note that under the left multiplication action of A_n on A_n/H, the stabilizer of $H \in A_n/H$ is precisely φ_h for $h \in H$. Therefore, $\psi(H) \leq \psi(A_n)$ is the stabilizer subgroup in $S_{A_n/H}$ of H in A_n/H, hence is the stabilizer of H in $A_n \cong \psi(A_n) \leq S_{A_n/H}$. By the problem above, $\psi(H) \cong A_{n-1}$, so $H \cong A_{n-1}$.

Now we treat the cases $n = 3, 4$. For $n = 3$, subgroups of index 3 must have order 1, which is the trivial element. Obviously $e \cong A_2$. Now for $n = 4$, subgroups of index 4 must have 3 elements. Groups of order 3 are isomorphic to $\mathbb{Z}/3\mathbb{Z}$, which is again isomorphic to A_3. $\square$

Problem 4. *Let H be a simple group of order 60. Show that $H \cong A_5$ and compute $|\operatorname{Syl}_p(H)|$ for every prime p.*

Proof. We show that $H \leq A_6$. By the Sylow theorems, we have $n_5 \equiv 1 \bmod 5$, and $n_5 | 12$. The only possibilities are $n_5 = 1$ or $n_5 = 6$. Since H is assumed to be simple, $n_5 = 1$ cannot happen, so $n_5 = 6$. Also, we know that all Sylow 5-subgroups of H are conjugate. Therefore, we may consider a group homomorphism $\psi : H \to S_{\mathrm{orb}(K)}$ where K is a Sylow 5-subgroup of H, and $\mathrm{orb}(K)$ is the orbit set of K under conjugation by elements of H. The homomorphism is given by $h \mapsto \varphi_h$, where $\varphi_h(aKa^{-1}) = haKa^{-1}h^{-1}$ is a set map from $S_{\mathrm{orb}(K)}$ to itself. This set map is obviously injective, hence bijective since $|\mathrm{orb}(K)| = 6 < \infty$. Thus indeed $\varphi_h \in S_{\mathrm{orb}(K)}$.

Now we show that ψ is nontrivial. It suffices to show that there exists some $h \in H$ such that $\varphi_h \neq \mathrm{id}_{S_{\mathrm{orb}(K)}}$. For this to happen, it suffices to find some h where $hKh^{-1} \neq K$. Now if $hKh^{-1} = K$ for all $h \in H$, K would be a normal subgroup of H. But we assumed that H is simple, so this cannot happen, and such h exists. Therefore the homomorphism ψ is nontrivial, and the kernel of this homomorphism cannot be the entirety of H.

We know that the kernel of a group homomorphism is a normal subgroup of the domain group. Hence, it follows that $\ker \psi$ is a proper normal subgroup of H. Since we assumed H to be simple, the only such group is $\{e\}$, so ψ is in fact injective. Therefore we may view H to be a subgroup of $S_{\mathrm{orb}(K)} \cong S_6$. Not only that, if we consider the composition $H \xrightarrow{\psi} S_{\mathrm{orb}(K)} \xrightarrow{\mathrm{sgn}} \{\pm 1\}$, the kernel of this homomorphism cannot be trivial, since otherwise H injects into $\{\pm 1\}$ which is nonsense ($|H| = 60$...) Therefore, the kernel is a nontrivial normal subgroup of H. Since H is simple, this means that the kernel is H, so in fact every element of $\psi(H)$ has sign $+1$, which implies that $\psi(H) \leq A_6$. Now since $H \cong \psi(H)$, $\psi(H)$ is an order 60 subgroup of A_6, hence of index 6. From the problem above, it follows that $\psi(H) \cong A_5$, i.e. $H \cong A_5$.

As we have shown above, $n_5 = 6$. The remaining numbers are n_2 and n_3. We must have $n_3 \equiv 1 \bmod 3$ and $n_3 | 20$, so $n_3 = 1, 4, 10$. Also A_5 is simple so $n_3 = 1$ cannot happen. The only possibilities are $n_3 = 4, 10$. Note that Sylow 3-subgroups are of order 3, and we know that order 3 elements of A_5 are precisely the 3-cycles. Note that

$$(123), (124), (125), (134), (135), (145), (234), (235), (245), (345)$$

are all 3-cycles that generate distinct subgroups of order 3. Hence $n_3 = 10$. Now, $n_2 \equiv 1 \bmod 2$, and $n_2 | 15$ so $n_2 = 1, 3, 5, 15$, again excluding 1 to get $n_2 = 3, 5, 15$. Suppose $n_2 = 15$. Since Sylow 2-subgroups are of order 4, we conclude that A_5 has 3×15 elements that are of order either 2 or 4. But this cannot happen since $n_3 = 10$, so there are at least 20 elements of A_5 that have order 3. Therefore, either $n_2 = 3$ or 5. However, using the fact that subgroups of order 4 of A_5 must be contained in Sylow 2-subgroups, we find 5 distinct subgroups of A_5 of order 4:

$$\{e, (12)(34), (13)(24), (14)(23)\}$$
$$\{e, (12)(35), (13)(25), (15)(23)\}$$
$$\{e, (12)(45), (14)(25), (15)(24)\}$$
$$\{e, (13)(45), (14)(35), (15)(34)\}$$
$$\{e, (23)(45), (24)(35), (25)(34)\}$$

Therefore these subgroups themselves are the Sylow 2-subgroups, and $n_2 = 5$. □

Problem 5. *Solve the following:*

1. *Compute the subgroup lattice of A_4.*
2. *Show that S_n are solvable for $n \leq 4$.*

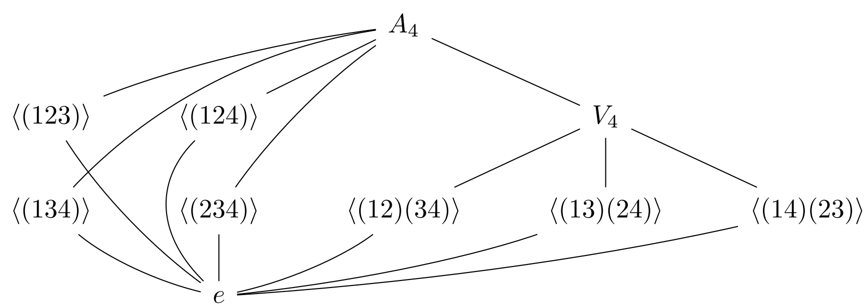
Proof. 1. Elements of A_4:

$$\{e, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$$

The possible orders of subgroups are divisors of 12, namely 1,2,3,4,6. The order 2 subgroups are the ones generated by (12)(34), (13)(24) and (14)(23), since these are the only elements of A_4 of order 2. The order 3 subgroups are the ones generated by (123), (124), (134) and (234), again because nontrivial elements of subgroups of order 3 have order 3, and we know what the order 3 elements of A_4 look like. Also, the only order 4 subgroup of A_4 is $\{e, (12)(34), (13)(24), (14)(23)\}$ since either $n_2 = 1$ or 3, but if $n_2 = 3$ then there must be 9 elements of order either 2 or 4, which is not the case. For simplicity, denote this group as V_4.

Now we find subgroups of order 6. Elements of such subgroup must have order either 2 or 3. Therefore, we check what the group generated by, say $(ab)(cd)$ and (abc) is. Note that $(ab)(cd)(abc) = (bdc)$, $(abc)(ab)(cd) = (acd)$, and $(bdc)(acd) = (abd)$. Therefore, the group generated by $(ab)(cd)$ and (abc) contains all 3-cycles, so it clearly cannot be of order 6. By plugging numbers into a, b, c, d, we may conclude that no subgroup of order 6 of A_4 exists.

Therefore, the subgroup lattice looks like this:[1]



$\square$

Proof. 2. Since A_n are index 2 subgroups of S_n, they are normal, and the quotient is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Thus, it suffices to show that A_n are solvable for $n \leq 4$. Since $A_3 \cong \mathbb{Z}/3\mathbb{Z}$, it is trivially solvable. Hence we prove for A_4. Consider the chain $e \leq \langle(12)(34)\rangle \leq V_4 \leq A_4$ of subgroups of A_4. They are of order 1, 2, 4, 12, respectively, so the quotients are isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$, which are abelian. Thus A_4 is solvable. $\square$

Problem 6.

1. *Show that the permutation action of A_n on J_n is $(n-2)$-transitive for all $n \geq 3$.*
2. *For $n \geq 5$, classify all subgroups of S_n whose permutation action on J_n is $(n-2)$-transitive.*

Proof. 1. Show that the action of A_n on $J_n^{[n-2]}$ is transitive. Here, $J_n^{[n-2]}$ is the set of sequences of $n-2$ elements of $J_n = \{1, 2, \ldots, n\}$, all distinct. Suppose we have an element $(a_1, \ldots, a_{n-2})$ of $J_n^{[n-2]}$. Consider a permutation σ that sends i to $\sigma(i) = a_i$, for $1 \leq i \leq n-2$. There are two such permutations, depending on whether $\sigma(n) = a_n$ or a_{n-1}. Now in one case it is odd, and one case it is even, so there is exactly one such permutation σ in A_n. Therefore any element of $J_n^{[n-2]}$ can be written as $(a_1, \ldots, a_{n-2}) = \sigma(1, 2, \ldots, n-2)$ where $\sigma \in A_n$. $\square$

Proof. 2. We classify subgroups of S_n $(n \geq 5)$ whose permutation action on J_n is $(n-2)$-transitive. First, the order of $J_n^{[n-2]}$ is $\binom{n}{2} \times (n-2)! = n!/2$, so for the action

[1]I know it looks hideous but I had to do it to fit this in the page

to be $(n-2)$-transitive the subgroup must have at least $n!/2$ elements. Above we have shown that A_n acts $(n-2)$-transitively on J_n, so A_n is such a subgroup. We show that the only subgroup of S_n of index 2 is A_n. Suppose $A_n \neq H \leq S_n$ where $[S_n : H] = 2$. Since $A_n \neq H$, H cannot contain all 3-cycles of S_n, say $(abc) \notin H$. (If H contained all 3-cycles, then it would properly contain A_n, which implies $[S_n : H] = 1$.) This implies $(abc)^{-1} = (acb) \notin H$, so $H, (abc)H, (acb)H$ are three distinct cosets of H, contradictory to the assumption that $[S_n : H] = 2$. Thus A_n is the only such subgroup. Trivially, S_n is also an $(n-2)$-transitive subgroup of S_n. $\square$

ALGEBRA I HOMEWORK VI

HOJIN LEE 2021–11045

Problem 1. *Solve the following.*

(1) *Show that every finite domain is a field.*
(2) *Show that if F is a finite field then $|F| = p^n$ for some prime $p > 0$ and $n \in \mathbb{N}_{\geq 1}$.*
(3) *Give an example of a ring A and element $x \in A$ that is left regular but not right regular.*

Proof. (1) Suppose D is a finite domain. Suppose $0, 1 \neq a \in D$. Consider the elements $a, a^2, a^3, \ldots$, and by the pigeonhole principle, we must have $a^i = a^j$ for some $i < j$. Then $a^i - a^j = a^i(1 - a^{j-i}) = 0$, where $a^i \neq 0$ (otherwise, a would be a zerodivisor) so we must have $a^{j-i} = 1$. Since we assumed $a \neq 1$, we have $j - i > 1$, so a has a unique multiplicative inverse. □

Proof. (2) Suppose F is a finite field. Then $\operatorname{char} F = 0$ cannot happen by finiteness of F, and $\operatorname{char} F = p$ for some prime. To show this, suppose $\operatorname{char} F = n = p_1^{n_1} \cdots p_k^{n_k}$ for some composite n. This implies $1 \cdot n = (1 \cdot p_1)^{n_1} \cdots (1 \cdot p_k)^{n_k} = 0$, and since F is a field we must have $1 \cdot p_i = 0$ for some $1 \leq i \leq k$, a contradiction since $p_i < n$. Thus, suppose $\operatorname{char} F = p$ for some prime p. The subfield generated by 1 is isomorphic to $\mathbb{F}_p$, and we may view this as a field extension $F/\mathbb{F}_p$. Thus F is a $\mathbb{F}_p$-vector space, which is finite dimensional since F is finite. Hence it is isomorphic to a finite direct sum $\bigoplus \mathbb{F}_p$, thus of order p^n for some $n \geq 1$. □

Proof. (3) Such ring should be necessarily noncommutative. Consider the ring of endomorphisms of $\mathbb{R}[x]$ as an $\mathbb{R}$-vector space. Let $T : f \mapsto fx$. If $U : 1 \mapsto 1, x^i \mapsto 0$ for $i > 0$, then $U \circ T = 0$ but if $V \neq 0$ then we have $T \circ V \neq 0$. Thus T is not right regular, but is left regular. □

Problem 2. $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ *is a ring generated over* $\mathbb{R}$.

(1) *Show that $\mathbb{H}$ is a division ring.*
(2) *Show that the center of $\mathbb{H}$ is $\mathbb{R}$.*

Proof. (1) Suppose $a = r_1 + r_2 i + r_3 j + r_4 k$ for $r_i \in \mathbb{R}$, $a \neq 0$. We show that there exists a^{-1} such that $aa^{-1} = a^{-1}a = 1$. If we let $b = r_1 - r_2 i - r_3 j - r_4 k$, then we have $ab = r_1^2 + r_2^2 + r_3^2 + r_4^2$, so if we let $a^{-1} = b/(r_1^2 + r_2^2 + r_3^2 + r_4^2)$ then we have $aa^{-1} = 1$. For the other way, we calculate ba. Note that this is just $(r_1 - r_2 i - r_3 j - r_4 k)(r_1 + r_2 i + r_3 j + r_4 k)$, so this will be $r_1^2 + (-r_2)^2 + (-r_3)^2 + (-r_4)^2$, just the same. Thus $a^{-1}a = 1$ too. Hence $\mathbb{H}$ is a division ring. □

Proof. (2) Since $ij = -ji$, i and j are not in the center. Similarly, k is not in the center. Thus the center is contained in $\mathbb{R}$. Every element of $\mathbb{R}$ commutes with other elements of $\mathbb{H}$, so the center is $\mathbb{R}$. □

Date: April 12, 2024.

Problem 3.

Problem 4.

Problem 5. *Let A be a commutative ring. Let I be an ideal of A.*

(1) *Show that $\sqrt{I}$ is an ideal, and that $\sqrt{I}$ contains I.*
(2) *Show that $\sqrt{I} = A$ iff $I = A$.*

Proof. (1) Suppose $x, y \in \sqrt{I}$. Then we have $x^n, y^m \in I$ for some $n, m > 0$. It follows that $(x+y)^{n+m} \in I$, so $x + y \in \sqrt{I}$. Obviously $0 \in \sqrt{I}$ so $\sqrt{I}$ is an additive subgroup of A. Now if we have $x \in \sqrt{I}$, say $x^n \in I$, then $(rx)^n = r^n x^n \in I$, so $rx \in \sqrt{I}$. Hence $\sqrt{I}$ is an ideal. Obviously $\sqrt{I}$ contains I since $i^1 \in I$ for all $i \in I$. $\square$

Proof. (2) $\sqrt{I} = A \Rightarrow 1 \in \sqrt{I} \Rightarrow 1 \in I$. The converse is obvious. $\square$

Problem 6. *Let A a ring. Let M an A-module, and $N, P \leq M$ are A-submodules.*

(1) *Construct the SES*
$$0 \to M/(N \cap P) \to M/N \times M/P \to M/(N+P) \to 0.$$
(2) *For $N + P = M$ conclude we have a natural isomorphism of A-modules*
$$M/(N \cap P) \cong M/N \times M/P.$$

Proof. (1) Note that we have an exact sequence
$$0 \to N \cap P \to N \times P \to N + P \to 0$$
given by $x \mapsto (x, -x)$ and $(a, b) \mapsto a + b$. One may check exactness almost trivially. Now consider the following diagram in Mod_A

$$\begin{tikzcd}
{} \arrow[r, dashed] & \operatorname{coker}\alpha \arrow[r] & \operatorname{coker}\beta \arrow[r] & \operatorname{coker}\gamma \arrow[r] & 0 \\
0 \arrow[r] & M \arrow[r] \arrow[u] & M \times M \arrow[r] \arrow[u] & M \arrow[r] \arrow[u] & 0 \\
0 \arrow[r] & N \cap P \arrow[r] \arrow[u, hook, "\alpha"] & N \times P \arrow[r] \arrow[u, hook, "\beta"] & N + P \arrow[r] \arrow[u, hook, "\gamma"] & 0 \\
 & & & 0 \arrow[u] \arrow[r, dashed, no head] & {}
\end{tikzcd}$$

where β is termwise inclusion, and the maps $M \to M \times M$ and $M \times M \to M$ are given by extending the maps on the bottom row. The diagram commutes, and the desired SES is given by the Snake lemma. $\square$

Proof. (2) Suppose $N + P = M$. Then in the SES above, we have $M/(N \cap P) \cong M/N \times M/P$. $\square$

Problem 7.

ALGEBRA I HOMEWORK VII

HOJIN LEE 2021–11045

Problem 1.

Problem 2.

Problem 3.

Problem 4. *Let A be a domain. Let $S \subset A - \{0\}$ be a multiplicative subset. Show*

(1) *A PID $\Rightarrow A_S$ PID*
(2) *A UFD $\Rightarrow A_S$ UFD*

Proof. (1) Suppose $I \subset A_S$ is an ideal. Then I is generated by elements of the form $a/1$ where $a/s \in I$ for some $s \in S$. This is because $a/s \in I$ iff $a/1 \in I$. Denote this generating set T. Then $T = \ell_S(T')$ where ℓ_S is the canonical localization map and $T' \subset A$. Clearly $0 \in T'$ since $0/1 \in T$. If $a, b \in T'$, then $a + b \in T'$ since $a/1 + b/1 = (a + b)/1 \in T$. Also, if $a \in A$ and $t \in T'$, then $t/1 \in T \subset I$, and $a/1 \cdot t/1 = at/1 \in I$ so $at/1 \in T$. Hence $at \in T'$, so T' is an ideal of A. Since A is a PID, we may write $T' = (t)$, hence $T = \{at/1 \mid a \in A\}$ so $I = (t/1)$. Therefore every ideal of A_S is principal. A_S is a domain since it is a subring of $K(A)$. $\square$

Proof. (2) We use Kaplansky's theorem. Suppose $\mathfrak{p} \subset A_S$ is a nonzero prime ideal. This corresponds to a nonzero prime ideal $\mathfrak{p}'$ of A that does not touch S. Since A is a UFD, $\mathfrak{p}'$ contains a nonzero prime, say p. Then $\mathfrak{p}$ contains $p/1$. Suppose $\frac{p}{1} | \frac{a}{s}\frac{b}{s'}$. Then we have $\frac{p}{1} \times \frac{c}{d} = \frac{ab}{ss'}$ for some $\frac{c}{d}$, i.e. $(pcss' - abd)s'' = 0$ for some $s'' \in S$. Since S does not contain zero and A is a domain, we have $pcss' = abd$, i.e. $p|abd$. Note that $p|d$ cannot happen since if so, then $pd' = d$ where $d \in S$ and $pd' \in \mathfrak{p}$. So either $p|a$ or $p|b$. WLOG $p|a$, so $a = pa'$, then $\frac{a}{s} = \frac{p}{1}\frac{a'}{s}$, so $\frac{p}{1} | \frac{a}{s}$. Hence $p/1$ is a prime element. It follows that A_S is a UFD. $\square$

Problem 5.

Problem 6. *Let $x \in A$.*

(1) *Let $S \subset A$ be multiplicatively closed. Show $\ell_S(x) = 0$ iff $\mathrm{Ann}(x) \cap S \neq \varnothing$.*
(2) *Show TFAE:*
   (a) $x = 0$
   (b) $\ell_{\mathfrak{p}}(x) = 0$ *for all primes.*
   (c) $\ell_{\mathfrak{m}}(x) = 0$ *for all maximal ideals.*

Proof. (1) Suppose $sx = 0$ for some $s \in S$. Then $s \in \mathrm{Ann}(x) \cap S$. Conversely this also implies $x/1 = 0$ since $xs = 0$. $\square$

Proof. (2) (a) $\Rightarrow$ (b) $\Rightarrow$ (c) is obvious. To show (c) $\Rightarrow$ (a), we show the contrapositive. If $x \neq 0$, then $\mathrm{Ann}(x)$ is proper. Hence there exists some maximal ideal $\mathfrak{m}$ containing $\mathrm{Ann}(x)$. Then $\mathrm{Ann}(x) \cap (A - \mathfrak{m}) = \varnothing$, so $\ell_{\mathfrak{m}}(x) \neq 0$. $\square$

Date: May 8, 2024.

Problem 7. *Let $k = \overline{k}$. Show $(x, y) \subset k[x, y]$ is not principal.*

Proof. Suppose $(x, y) = (f)$. Then $x \in (f)$, so $x = fg$ for some $g \in k[x, y]$. Since x is irreducible, either $f = c$ or $f = cx$ for $c \in k$. The first case implies $(x, y) = k[x, y]$, which is not the case since $k[x, y]/(x, y) \cong k \neq 0$. The second case implies $(x, y) = (x)$ which is nonsense. □

Problem 8.

(1) *Show that a Euclidean domain is a PID.*
(2) *Show that $\mathbb{Z}[i]$ is a Euclidean domain.*

Proof. (1) Let A be a Euclidean domain, and $I \subset A$ an ideal. Consider the set $f(I) \subset \mathbb{N}$. This has a minimal element, and denote by b an element of $I - \{0\}$ in $f^{-1}(\min(f(I)))$. If $a \in I - \{0\}$, then $a = bq + r$ for either $r = 0$ or $f(r) < f(b)$. In this case, $r = a - bq \in I$, so by minimality of $f(b)$, the latter cannot happen. Hence $a = bq$ for all $a \in I$, so $I = (b)$. □

Proof. (2) Obviously a domain since it is a subring of $\mathbb{C}$. Define $f : \mathbb{Z}[i] - \{0\} \to \mathbb{N}$ by $f(a + bi) = a^2 + b^2$. WTS if $z, w \in \mathbb{Z}[i]$ with $w \neq 0$, then there exists $q, r \in \mathbb{Z}[i]$ such that $z = wq + r$ where either $r = 0$ or $f(r) < f(b)$. WMA $r \neq 0$. Then $z/w = (z_1 + z_2 i)/(w_1 + w_2 i) = \frac{z_1 w_1 + z_2 w_2 + (z_2 w_1 - z_1 w_2)i}{f(w)}$. By the Euclidean algorithm on $\mathbb{Z}$ (plus some obvious observations), we may write $z_1 w_1 + z_2 w_2 = f(w)q_1 + r_1$ and $z_2 w_1 - z_1 w_2 = f(w)q_2 + r_2$ for $|r_i| \leq \frac{1}{2} f(w)$. Thus, $\frac{z}{w} = \frac{f(w)(q_1 + q_2 i) + r_1 + r_2 i}{f(w)} = q_1 + q_2 i + \frac{r_1 + r_2 i}{f(w)}$. Hence $z = (q_1 + q_2 i)w + \frac{r_1 + r_2 i}{w_1 - w_2 i}$, where $f(\frac{r_1 + r_2 i}{w_1 - w_2 i}) = \frac{r_1^2 + r_2^2}{w_1^2 + w_2^2}$, omitting tedious calculations. (Trust me, I have done all the calculations.) This is just $f(r_1 + r_2 i)/f(w)$, and we want to show this is $< f(w)$, i.e. $f(r_1 + r_2 i) < f(w)^2$. Since $r_1^2 + r_2^2 \leq 2 \times \frac{f(w)^2}{4} = \frac{f(w)^2}{2}$, we have $f(r_1 + r_2 i) \leq \frac{f(w)^2}{2} < f(w)^2$. Take $q = q_1 + q_2 i$ and $r = z - (q_1 + q_2 i)w = \frac{r_1 + r_2 i}{w_1 - w_2 i} \in \mathbb{Z}[i]$. □

Problem 9.

Problem 10.

Problem 11. *Is it irreducible?*

Proof. (1) $x^4 + 1$ does not have a linear factor since it does not have a root in $\mathbb{Q}$ (let alone $\mathbb{R}$). Hence if it did factorize, then each factor would have to be at least of degree 2. Thus the only possible case is $x^4 + 1 = (x^2 + ax + 1)(x^2 + bx + 1)$ for $a, b \in \mathbb{Q}$. By expanding, the conditions become $a + b = 0$ and $ab + 2 = 0$, i.e. $a = -b$ and $a^2 = 2$. This does not have any solution in $\mathbb{Q}$. Hence it is irreducible over $\mathbb{Q}$. □

Proof. (2) Substitute $x \mapsto x + 1$. We get $(x + 1)^6 + (x + 1)^3 + 1 = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3$. Eisenstein's criterion for $p = 3$ is applicable. Hence $x^6 + x^3 + 1$ is irreducible over $\mathbb{Q}$. □

Proof. (3) The polynomial $x^3 - 5x^2 + 1$ has no roots in $\mathbb{F}_2$, hence is irreducible over $\mathbb{F}_2$ since it is of degree 3. Thus it is irreducible over $\mathbb{Q}$. □

Proof. (4) The polynomial $5x^5 - 5x + 1 = 2x^5 + x + 1$ has no roots in $\mathbb{F}_3[x]$. Thus if it did factor in $\mathbb{F}_3[x]$, then it would contain an irreducible factor of degree 2. The degree 2 irreducible polynomials of $\mathbb{F}_3[x]$ are precisely the following:

$$x^2 + 1, \quad x^2 + x + 2, \quad x^2 + 2x + 2, \quad 2x^2 + x + 1, \quad 2x^2 + 2x + 1 \quad 2x^2 + 2.$$

Note that the last 3 polynomials are just -1 times the first three, so it suffices to show that $2x^5 + x + 1$ does not have as factors the first three polynomials.

First, suppose $2x^5 + x + 1 = (x^2 + 1)(2x^3 + ax^2 + bx + 1)$. This cannot happen since the degree 4 coefficient is $a = 0$, but the degree 2 coefficient is $a + 1 \neq 0$.

Next suppose $2x^5 + x + 1 = (x^2 + x + 2)(2x^3 + ax^2 + bx + 1) = 2x^5 + (2 + a)x^4 + (1 + a + b)x^3 + (2a + b + 2)x^2 + (2b + 2)x + 1$. Then $a = b = 1$, but then $2a + b + 2 = 2 \neq 0$.

Suppose $2x^5 + x + 1 = (x^2 + 2x + 2)(2x^3 + ax^2 + bx + 1) = 2x^5 + (1 + a)x^4 + (1 + 2a + b)x^3 + (2a + 2b + 2)x^2 + (2b + 1)x + 1$. Then $a = 2, b = 1$ but $2a + 2b + 2 = 2 \neq 0$.

Therefore it is irreducible over $\mathbb{F}_3$, hence irreducible over $\mathbb{Q}$. $\square$

ALGEBRA I HOMEWORK IX

HOJIN LEE 2021-11045

Problem 1. *Let K be a field of characteristic $p > 0$. Let α be algebraic over K. Show that α is separable over K if and only if $K(\alpha) = K(\alpha^{p^n})$ for all positive integers n.*

Proof. Suppose α is separable over K. Consider the tower of extensions $K(\alpha)/K(\alpha^{p^n})/K$. Since subextensions are also separable, $K(\alpha)/K(\alpha^{p^n})$ is also separable. But since $\mathrm{irr}(\alpha, K(\alpha^{p^n}), X)$ divides $X^{p^n} - \alpha^{p^n} = (X - \alpha)^{p^n}$, the only possible way for the extension to be separable is the minimal polynomial being $X - \alpha$, i.e. $\alpha \in K(\alpha^{p^n})$. This implies $K(\alpha) = K(\alpha^{p^n})$, which holds for all $n > 0$ since n was arbitrary.

Conversely, suppose $K(\alpha) = K(\alpha^{p^n})$ for all $n > 0$. Suppose α is not separable. Then $\mathrm{irr}(\alpha, K, x) = g(x^p)$ for some $g \in K[x]$. Hence $g(\alpha^p) = 0$, which implies that $\mathrm{irr}(\alpha^p, K, x)|g(x)$. But then $[K(\alpha) : K] = [K(\alpha^p) : K] = \deg(\mathrm{irr}(\alpha^p, K, x)) \leq \deg g(x) < \deg g(x^p) = [K(\alpha) : K]$, which is a contradiction. □

Problem 2. *Let K be a field of characteristic $p > 0$. Let $a \in K$. If a has no pth root in K, show that $X^{p^n} - a$ is irreducible in $K[X]$ for all positive integer n.*

Proof. We show the contrapositive. Assume that $f(X) := X^{p^n} - a$ is not irreducible in $K[X]$ for some $n > 0$. Denote by $\alpha \in \overline{K}$ a root of X^{p^n} in the algebraic closure. Then $\alpha^{p^n} = a$, so $X^{p^n} - a = X^{p^n} - \alpha^{p^n} = (X - \alpha)^{p^n}$. Let $g(X) = \mathrm{irr}(\alpha, K, X)$. Then $g(X)|f(X)$, so we may write $f(X) = g(X)^m$. Since $m \deg g = p^n$, the degree and m must both be powers of p, and $m > 1$ since we assumed f to be non irreducible. Suppose $\deg g = p^r$ and $m = p^s$. Then $g(X) = X^{p^r} - \alpha^{p^r} = (X - \alpha)^{p^r} \in K[X]$, so we have $\alpha^{p^r} \in K$. Since $\alpha^{p^{n-1}} = \alpha^{p^r p^{s-1}} = (\alpha^{p^r})^{p^{s-1}}$ where $s - 1 \geq 0$, this element is in K, and is a pth root of a. □

Problem 3. *Let K be a field of characteristic $p > 0$. Let L/K be a finite extension such that $p \nmid [L : K]$. Show that L is separable over K.*

Proof. Let $\alpha \in L$. Let $f(X) = \mathrm{irr}(\alpha, K, X)$, and $d := \deg f$. Then we have $d|[L : K]$, so $p \nmid d$. Hence $f' \neq 0$, so α is separable over K. Since α was arbitrary, L/K is separable. □

Problem 4. *Show that every element of a finite field can be written as a sum of two squares in that field.*

Proof. For characteristic $p = 2$, the Frobenius automorphism will do the trick. Suppose $p \neq 2$ and denote the finite field as $\mathbb{F}$. Consider the assignment $\varphi : \mathbb{F}^\times \to \mathbb{F}^\times$ given by $x \mapsto x^2$. This is a 2-1 map, since if $\varphi(a) = \varphi(b)$, this implies either $a = b$ or $a = -b$ (since $p \neq 2$). Hence there exists $|\mathbb{F}^\times|/2$ square elements in $\mathbb{F}^\times$, in other words there exists $(|\mathbb{F}| + 1)/2$ square elements in $\mathbb{F}$ (counting zero). Let $S := \{s^2 \mid s \in \mathbb{F}\}$ and $T_x := \{x - t^2 \mid t \in \mathbb{F}\}$ for some $x \in \mathbb{F}$. Both

Date: May 24, 2024.

$|S| = |T| = (|\mathbb{F}| + 1)/2$, so $|S| + |T| = |\mathbb{F}| + 1$. This means that $S \cap T \neq \varnothing$, i.e. there exists some $a, b \in \mathbb{F}$ such that $x = a^2 + b^2$. Since x was arbitrary, we win. $\square$

Problem 5. *Let F be a finite field with q elements. Let $n \geq 1$ be an integer. Let $f(X) \in F[X]$ be irreducible. Show that $f(X)|(X^{q^n} - X)$ if and only if $\deg f|n$. Prove that $X^{q^n} - X$ is the product of all monic irreducible polynomials in $F[X]$ with degree dividing n. Counting degrees, conclude that*

$$q^n = \sum_{d|n} d\psi(d)$$

where $\psi(d)$ is the number of monic irreducible polynomials of degree d in $F[X]$.

Proof. Suppose that $f(X)|(X^{q^n} - X)$. Let $\alpha \in \overline{F}$ be a root of f. Consider the extension E/F by adjoining roots of $X^{q^n} - X$, which is of degree n since $X^q = X$ in F. Since f divides $X^{q^n} - X$, it follows that $E/F(\alpha)$, so we have $[E : F] = n = [E : F(\alpha)][F(\alpha) : F]$, so $[F(\alpha) : F] = \deg f|n$. Conversely, suppose $\deg f|n$. The extension $F(\alpha)/F$ is a field with $q^{\deg f}$ elements. Hence we have $\alpha^{q^{\deg f}} = \alpha$. This implies $\alpha^{q^n} = \alpha$ since $\deg f|n$, so α is also a root of $X^{q^n} - X$. Hence $f(X)|(X^{q^n} - X)$.

The polynomial $X^{q^n} - X$ has no repeated zero in $\overline{F}$ since its derivative is nonzero. Then the fact that it is a product of all monic irreducible polynomials in $F[X]$ follows directly from the fact we have proved above. Thus, the degree q^n must be equal to the sum of the degrees of all monic irreducible polynomials in $F[X]$, with degree dividing n. In other words, $q^n = \sum_{d|n} d\psi(d)$. $\square$