Problem Set 4 Zack Garza

① $\underline{S_1 \text{ is solvable}}$: $S_1 \cong \{e\}$.

$\underline{S_2 \text{ is solvable}}$: $S_2 \cong \mathbb{Z}_2$, take the normal series $\{e\} \trianglelefteq S_2$, $S_2/\{e\} \cong \mathbb{Z}_2$, abelian.

$\underline{S_3 \text{ is solvable}}$: Take $\{e\} \trianglelefteq A_3 \trianglelefteq S_3$

$A_3/\{e\} \cong A_3$ $\quad S_3/A_3 \cong \mathbb{Z}_2$, abelian

$\underline{S_4 \text{ is solvable}}$: Take $\{e\} \trianglelefteq \langle (12) \rangle \trianglelefteq \langle (12),(34) \rangle \trianglelefteq A_4 \trianglelefteq S_4$

Quotients: $\cong \mathbb{Z}_2$ $\quad \cong \mathbb{Z}_2$ $\quad \cong \mathbb{Z}_3$ $\quad \cong \mathbb{Z}_2$ all abelian.

$\underline{S_3, S_4 \text{ are not nilpotent}}$: G is nilpotent iff there exists a finite series

$$\{e\} \trianglelefteq Z(G) \trianglelefteq Z_1(G) \trianglelefteq \cdots \trianglelefteq Z_n(G) = G,$$ where $Z_i \trianglelefteq G$ is a subgroup satisfying $Z_i/Z_{i-1} = Z(G/Z_{i-1})$. If $Z(G) = \{e\}$, no such series exists.

$\underline{\text{Claim: } n \geq 3 \Rightarrow Z(S_n) = \{e\}}$:

Let $\sigma \in S_n$ and $\sigma(i) = j$. Choose $\tau = (j\ k)$ for some $k \neq j, i$. Then

$$\tau\sigma\tau^{-1}(i) = \tau\sigma(i) = \tau(j) = k \neq j = \sigma(i),$$

so τ & σ can not commute. So $\sigma \notin Z(S_n)$, thus $Z(S_n) = \{e\}$.

So S_n can not be nilpotent for $n \geq 3$. ■

② Suppose $N \trianglelefteq G$ is simple, and there is a normal series

$$0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_n = G/N \quad \text{s.t. } H_i/H_{i-1} \text{ is } \underline{\text{simple}}.$$

Since each $H_i \trianglelefteq G/N$, we have $H_i = J_i/N$ for some $J_i \trianglelefteq G$ with $N \subseteq J_i$.

So consider

$$0 \trianglelefteq J_1 \trianglelefteq J_2 \trianglelefteq \cdots \trianglelefteq J_n = G$$

and $\frac{J_i}{J_{i-1}} \cong \frac{J_i/N}{J_{i-1}/N} \cong \frac{H_i}{H_{i-1}}$ which is simple, so this is a composition series for G. ∎

③ Suppose $|G| = p^2 q$, then

$$n_p \equiv 1 \bmod p \qquad n_q \equiv 1 \bmod q$$
$$n_p \mid q \qquad n_q \mid p^2$$

Case 1: Suppose $\boxed{q=p}$, so $\# G = p^3$. Then $\# Z(G) = p, p^2$, or p^3.

- $|Z(G)| = p^3 \Rightarrow G$ is abelian, so $[G,G] = \{e\}$ and the derived series terminates, so G is solvable. ✓
- $|Z(G)| = p^2 \Rightarrow$ $$\underset{p^2}{1 \trianglelefteq Z(G)} \underset{p}{\trianglelefteq G}$$] Size of quotients
  But all groups of order p or p^2 are abelian, so G is solvable. ✓
- $|Z(G)| = p \Rightarrow$ $$\underset{p}{1 \trianglelefteq Z(G)} \underset{p^2}{\trianglelefteq G}$$] Size of quotients
  So G is again solvable. ✓

Case 2: Suppose $q<p$. Then since $n_p \equiv 1 \bmod p$, or equivalently $p \mid n_p - 1$, we have either $n_p = 1$ or $p \leq n_p - 1$. Suppose $n_p \neq 1$. Then $n_p \mid q \Rightarrow n_p \leq q$, so

$$p \leq n_p - 1 \leq q - 1 \leq q,$$

contradicting $p>q$. ※

Otherwise, $n_p = 1$, so $Q_p \in Syl(p,G)$ is normal, and

$$\underset{p^2}{1 \trianglelefteq Q_p} \underset{q}{\trianglelefteq G}$$] Size of quotients

But p, q are prime, so G is solvable. ✓

Case 2: $\boxed{q>p.}$ Then $n_q \in \{1, p, p^2\}$ and $n_p \in \{1, q\}$.

- If $n_p = 1$ or $n_q = 1$, G will be solvable, using either Q_p or Q_q in a normal series.

· Otherwise, suppose $n_p = q$ and $n_q \neq 1$.

1) $n_q = p$

Then since $n_q \equiv 1 \mod q$, so $q \leq n_q - 1 = p-1 < p$ and we find that $q < p$. But we assumed $q > p$, a contradiction. ⋇

2) $n_q = p^2$

Then by counting elements, there are $n_q(q-1) = p^2(q-1) = p^2 q - p^2$ elements of order q, and thus p^2 elements of order <u>not</u> q (and not zero). The only other possible orders are p and p^2. But any <u>one</u> sylow-p subgroup contributes (p^2-1) such elements, and if $n_p > 1$, then the remaining distinct sylow-p subgroups contribute at least $(p-1)$ elements, yielding

$$\# \text{elts} = \underbrace{n_q(q-1)}_{n_q \text{ sylow-}q} + \underbrace{1(p^2-1)}_{1 \text{ sylow-}p} + \underbrace{q(p-1)}_{q \text{ other sylow-}p} = p^2(q-1) + (p^2-1) + q(p-1) + 1$$

$$> p^2 q + qp - 1$$

$$> p^2 q = \# G, \text{ a contradiction.}$$

So G is solvable. ■

④

a) $[F:K] = 1$ iff $F = K$.

($\Rightarrow$): F/K is a 1-dimensional vector space, so $F = \langle \vec{e}_1 \rangle$ for some basis element. We always have $K \subseteq F$, so the claim is $F \subseteq K$. Since $1 \in F$, then $1 = k\vec{e}_1$ for some $k \in K$, and so $\vec{e}_1 = k^{-1} \in K$ and thus $\alpha \vec{e} \in K$ $\forall \alpha \in K$. So $F \subseteq K$.

($\Leftarrow$): If $F = K$, then $\langle 1 \rangle$ is a basis for F since $k \in K \Rightarrow k = k \cdot 1$. So $\dim_E(F) = 1$. ■

b) Suppose otherwise that $\exists G$ s.t. F/G and G/k. Then $[F:K] = [F:G][G:K] \Rightarrow p = mn$ for some $m, n \in \mathbb{N}^{\geq 0}$. Since p is prime, either $m=1$ or $n=1$, so by (a), $F = G$ or $G = K$. □

c) If u has degree n over K, then $[K(u):K]=n$. Since $K(u)\subseteq F$, we have

$$[F:K]=[F:K(u)][K(u):K]$$

$$\Rightarrow \quad a \quad = \quad b \quad n \qquad \Rightarrow n \text{ divides } a. \quad \blacksquare$$

(5) Since $K(u^2)\subseteq K(u)$, we have

$$[K(u):K]=[K(u):K(u^2)][K(u^2):K]$$

$$\text{odd} \quad = \quad m \qquad\quad n$$

So both m and n must be odd. Since $f\in K(u^2)[x]$ given by $f(x)=x^2-u^2$ has degree 2 and $f(u)=0$, $m\leq 2$. Since m is odd, $m=1$, so $K(u)=K(u^2)$. $\blacksquare$

(6)

a) We have $x^2-2=(x+\sqrt{2})(x-\sqrt{2})$ irreducible over $\mathbb{Q}$, so

$$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2, \quad \mathbb{Q}(\sqrt{2})=\operatorname{span}_{\mathbb{Q}}(\{1,\sqrt{2}\}).$$

We also have $x^2-3=(x+\sqrt{3})(x-\sqrt{3})$ irreducible over $\mathbb{Q}$, and since if $\sqrt{3}\in\mathbb{Q}(\sqrt{2})$ we would have $\sqrt{3}=a+b\sqrt{2}\Rightarrow 3=a^2+2b^2+2ab\sqrt{2}\Rightarrow \sqrt{2}=(3-a^2-2b^2)/2ab\in\mathbb{Q}$, we find that x^2-3 is irreducible over $\mathbb{Q}(\sqrt{2})$ as well and $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$.

Thus $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=2\cdot 2=4$ and $\mathbb{Q}(\sqrt{2},\sqrt{3})=\operatorname{span}_{\mathbb{Q}}(\{1,\sqrt{2},\sqrt{3},\sqrt{6}\})$. $\blacksquare$

b) We have $\omega_3=\frac{1}{2}(\sqrt{3}+i)\in\mathbb{Q}(i,\sqrt{3})$, so $\mathbb{Q}(i,\sqrt{3},\omega_3)=\mathbb{Q}(i,\sqrt{3})$. Since $\min(\sqrt{3},\mathbb{Q})=x^2-3$ and $\min(i,\mathbb{Q}(\sqrt{3}))=\min(i,\mathbb{Q})=x^2+1$, $[\mathbb{Q}(i,\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(i,\sqrt{3}):\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=2\cdot 2=4$ and $\mathbb{Q}(i,\sqrt{3})=\operatorname{span}_{\mathbb{Q}}(\{1,i,\sqrt{3},i\sqrt{3}\})$.

7) Any two $\mathbb{Q}$-vector spaces of the same dimension are isomorphic, and $\min(i,\mathbb{Q})=x^2+1$, $\min(\sqrt{2},\mathbb{Q})=x^2-2\Rightarrow \dim\mathbb{Q}(i)=\dim\mathbb{Q}(\sqrt{2})=2$.

If $\phi:\mathbb{Q}(\sqrt{2})\to\mathbb{Q}(i)$ is an isomorphism of fields, then $x\in\mathbb{Q}\Rightarrow\phi(x)=x$. If $\phi(\sqrt{2})=\underbrace{a}_{\in\mathbb{Q}}+\underbrace{b}_{\in\mathbb{Q}}i$, then

$$2=(\sqrt{2})^2=f((\sqrt{2})^2)=f(\sqrt{2})^2=(a+bi)^2=a^2-b^2+2abi.$$

So $a^2-b^2=2$ and $2ab=0$, which forces either $a^2=2$ or $b^2=-2$, contradicting $a,b\in\mathbb{Q}$. So ϕ can not exist. $\blacksquare$