210C FINAL EXAM

KIM, SUNGJIN

Problem1.
$\Leftarrow$) We do this in two steps:
(1) If A has a composition series, then A is noetherian and artinian.
(2) A has an A-composition series.

Proof of (1).
Suppose A has a composition series S of length n. If either chain condition fails to hold, one can find submodules

$$A = A_0 \supsetneq A_1 \supsetneq A_2 \supsetneq \cdots \supsetneq A_n \supsetneq A_{n+1},$$

which form a normal series T of length $n+1$. By Shreier's theorem, S and T have refinements that are equivalent. This is a contradiction since S has length n, and refinement of T has length at least $n+1$. Therefore, A satisfies both chain conditions.
Proof of (2).
Using the fact that A is noetherian, any ideal of A contains a finite product of prime ideals. In particular, the ideal (0) contains a finite product $\mathfrak{m}_1 \cdots \mathfrak{m}_n$ of prime ideals $\mathfrak{m}_1, \cdots, \mathfrak{m}_n$ which are also maximal ideals. Thus, we have a filtration

$$0 = \mathfrak{m}_1 \cdots \mathfrak{m}_n \subset \mathfrak{m}_1 \cdots \mathfrak{m}_{n-1} \subset \cdots \subset \mathfrak{m}_1 \subset A.$$

Each quotient $\mathfrak{m}_1 \cdots \mathfrak{m}_i / \mathfrak{m}_1 \cdots \mathfrak{m}_{i+1}$ is a finitely generated module over a field $A/\mathfrak{m}_{i+1}$, and therefore has an A-composition series. It follows that A-module A has an A-composition series, so A is artinian by (1).

$\Rightarrow$) We do this in two steps:
(3) Left artinian DOES imply left noetherian for noncommutative rings too.
(4) If A is an artinian commutative ring, then $\mathrm{Spec}(A) = \mathrm{Max}(A)$.

Proof of (3).
Note that if A is artinian, then $\bar{A} = A/\mathrm{Rad}(A)$ is semisimple, and $\mathrm{Rad}(A)$ is nilpotent.(cf. Homework6 Problem4.) For $J = \mathrm{Rad}(A)$, fix n such that $J^n = 0$. Consider the filtration

$$A \supset J \supset J^2 \supset \cdots \supset J^n = 0.$$

It is enough to show that J^i/J^{i+1} has a composition series. But J^i/J^{i+1} is artinian as module over $\bar{A}$. Since $\bar{A}$ is semisimple, J^i/J^{i+1} is semisimple $\bar{A}$-module, so it is a direct sum of simple $\bar{A}$-modules. The chain condition on J^i/J^{i+1} implies that this direct sum must be finite, so J^i/J^{i+1} does have a composition series as $\bar{A}$-module. Hence, A has a composition series as A-module. By (1), it follows that A is left noetherian.
Proof of (4).
Let $\mathfrak{p} \subset A$ be a prime ideal of A. Then $A/\mathfrak{p}$ is an integral domain. Thus, it is

enough to show that artinian integral domain is a field. Let $a \in A/\mathfrak{p}$ be a nonzero element. Consider a chain of ideals in $A/\mathfrak{p}$,

$$(a) \supset (a^2) \supset \cdots .$$

Since $A/\mathfrak{p}$ is artinian, this chain has to stop, say $(a^n) = (a^{n+1})$. Then $a^n = ba^{n+1}$ for some $b \in A/\mathfrak{p}$. This implies that $a^n(1 - ba) = 0$. Since $a^n \neq 0$, we must have $1 - ba = 0$. Hence $A/\mathfrak{p}$ is a field.

Problem2.
A *fractional ideal* I is a nonzero A-submodule I such that $aI \subset A$ for some nonzero $a \in A$. Let J be a fractional ideal in A. Denote

$$J^{-1} = \{a \in K | aJ \subset A\}.$$

Let P be the unique nonzero prime ideal in A. Since A is local, we have $P = \mathfrak{m}$. It is enough to show that A is a PID. This require the following facts.
(1) Let K be the quotient field of A, for a fractional ideal I in A, then

$$\bar{I} = \{a \in K | aI \subset I\} = A.$$

(2) $A \subsetneq P^{-1}$.
(3) P is invertible.
(4) $\cap_{n \geq 0} P^n = 0$.
(5) P is principal.

We assume (1),$\cdots$, (5), let I be a proper ideal in A. Then $I \subset P$. By (4), we can find N such that $I \subset P^N$, and $I \not\subset P^{N+1}$. By (5), there is $a \in A$ such that $P = (a)$. We see that $I \subset P^N = (a^N)$. Choose $b \in I - P^{N+1}$. Since $b \in P^N$, we can find $u \in A$ such that $b = ua^N$. It follows that u has to be a unit in A, otherwise we would have $u \in P$, and $b \in P^{N+1}$. Thus, $(a^N) = (ua^N) = (b) \subset I$, and we obtain $I = (a^N)$.

Proof of (1).
The inclusion $\supseteq$ is obvious. Since $\bar{I}$ is a fractional ideal, it is isomorphic to some ideal in A. So, $\bar{I}$ is finitely generated A-module, since A is noetherian. This means that every $x \in \bar{I}$ is integral over A. Since A is integrally closed, $x \in A$. Thus, we obtain that $\bar{I} = A$.
Proof of (2).
For any ideal $J \subset A$, we have $A \subset J^{-1}$. Let $\mathcal{F}$ be a family of all ideals J such that $A \subsetneq J^{-1}$. Choose a nonzero $a \in P$, then we know that a is nonunit, and let $J = (a)$. Then $1/a \in J^{-1}$, but $1/a \notin A$. So, the family $\mathcal{F}$ is nonempty. Since A is noetherian, we can find a maximal element M in the family $\mathcal{F}$. We claim that M is a prime ideal. For, assume that $ab \in M$ but $a \notin M$. Choose $c \in M^{-1} - A$, then $cab \in A$, hence $bc(aA + M) \subset A$, giving that $bc \in (aA + M)^{-1}$. By maximality of M, we have $bc \in A$. Thus, $c(bA + M) \subset A$, which implies $c \in (bA + M)^{-1}$. Since $c \notin A$, and again by maximality of M, we have $bA + M = M$. Hence $b \in M$, and M is a prime ideal. By uniqueness, we must have $M = P$. Therefore, $A \subsetneq P^{-1}$.
Proof of (3).
Clearly $P \subset PP^{-1} \subset A$. Since A is local, $PP^{-1} = P$ or A. But if $PP^{-1} = P$ then $A \subsetneq P^{-1} \subset \bar{P} = A$, by (1) and (2). This is a contradiction. Hence $PP^{-1} = A$.
Proof of (4).

This is a consequence of Artin-Rees Lemma, and Nakayama Lemma. (cf. Homework3 Problem1).
Proof of (5).
Choose $a \in P - P^2$(possible by (4)). Then aP^{-1} is a nonzero ideal in A such that $aP^{-1} \nsubseteq P$. Since every proper ideal of A is contained in P, we must have $aP^{-1} = A$. Hence, $(a) = aA = aP^{-1}P = AP = P$ by (3).

Problem3.
($charK = 0$) We start with a fixed subfield F of the complex field K. Let μ be an irreducible character afforded by a simple KG-module M. Let $F(\mu)$ be the field obtained by adjoining all $\mu(g)$ for $g \in G$. Consider those fields S such that $F \subset S \subset K$ for which there exists a SG-module V such that

$$M \simeq K \otimes_S V.$$

For such field S, any S-basis for V becomes a K-basis for M. In this case, we say that M affords a representation realizable in S. In particular, the matrix entries of this representation lie in S. Thus, we see that $\mu(g) \in S$ for all $g \in G$, since each $\mu(g)$ is trace of a matrix in S. Thus, we must have

$$F(\mu) \subset S \subset K.$$

The Schur index is defined by

$$m_F(\mu) = \min(S : F(\mu))$$

where the minimum is taken over all fields S such that M is realizable in S. Then $m_F(\mu) = m_{F(\mu)}(\mu)$. Further, $m_F(\mu) = 1$ if and only if M affords a representation realizable in $F(\mu)$.
Let M be an irreducible KG-module. Let S be any subfield of K. Then M is a direct summand of $V^K = K \otimes_S V$. Thus, every irreducible K-representation of G is realizable in S if and only if S is a splitting field of G. The following holds for Schur index;
Let M be an irreducible KG-module with character μ, and F be a subfield of K. Then for each FG-module W, the multiplicity with which M occurs as a factor of W^K is a multiple of $m_F(\mu)$.

Let $F = \mathbb{Q}(\sqrt[n]{1})$ where n is the exponent of G. Then $\mu(g) \in F$ for all $g \in G$, so $F(\mu) = F$. We claim that F is a splitting field of G. We need only to show that $m_F(\mu) = 1$ for each μ. By Brauer's theorem on induced characters, we may write

$$\mu = \sum a_i w_i^G$$

where $a_i \in \mathbb{Z}$, and w_i are one dimensional characters of elementary subgroups of G. (Elementary subgroup is a product of cyclic group and p-group) Now every one dimensional representation of a subgroup of G is realizable in F. Thus each w_i^G is a character some FG-module, and so the multiplicity of μ in each w_i^G is a multiple of $m_F(\mu)$. However, the multiplicity of μ in each w_i^G is 1. Therefore $m_F(\mu) = 1$. If K contains a primitive n-th root of unity, then by tensoring with K, we obtain that K is a splitting field of G.

Problem4.
The character table for G has to contain the following two more rows

G	$\{1\}$	C_2	C_3	C_4	C_5	C_6	C_7
tr	1	1	1	1	1	1	1
χ_1^2	1	1	1	w	w^2	w	w^2

Since the character table contains a 2-dimensional irreducible representation, it has to contain two more rows (by multiplying with 1-dimensional irreducible representations)

G	$\{1\}$	C_2	C_3	C_4	C_5	C_6	C_7
$\chi_1\chi_2$	2	-2	0	$-w^2$	$-w$	w^2	w
$\chi_1^2\chi_2$	2	-2	0	$-w$	$-w^2$	w	w^2

Thus, we have the following table so far, (0 on the last row comes from orthogonality with the first column.)

G	$\{1\}$	C_2	C_3	C_4	C_5	C_6	C_7
tr	1	1	1	1	1	1	1
χ_1^2	1	1	1	w	w^2	w	w^2
χ_1	1	1	1	w^2	w	w^2	w
χ_2	2	-2	0	-1	-1	1	1
$\chi_1\chi_2$	2	-2	0	$-w^2$	$-w$	w^2	w
$\chi_1^2\chi_2$	2	-2	0	$-w$	$-w^2$	w	w^2
χ_3	e	f	g	0	0	0	0

Let $a = |C_4|$, $b = |C_5|$, $c = |C_6|$, and $d = |C_7|$. Then by orthogonality relations of the first row and the second, third, we have

$$wa + w^2b + wc + w^2d = w^2a + wb + w^2c + wd.$$

This implies $a + c = b + d$. We use orthogonality relations of the first row and the fourth, fifth, we have

$$-a - b + c + d = -w^2a - wb + w^2c + wd.$$

This implies $(-a + c)(1 - w^2) = (-b + d)(w - 1)$. This forces $a = c$, $b = d$, and together with the above equation, we have $a = b = c = d$.
The orthogonality relation of the first column and the third column, we obtain $e|3$. Thus $e = 1$ or $e = 3$. But, $e = 1$ gives $|G| = 16$. Since the character table contains w, G must contain some element having order k with $3|k$. Therefore, we must have $e = 3$. Then by orthogonality of the first column and the second column, we have $f = 3$, $g = -1$. Now, we have that $|G| = 1^2 + 1^2 + 1^2 + 2^2 + 2^2 + 2^2 + 3^2 = 24$.
The orthogonality relation of the first and fourth rows, we obtain $|C_2| = 1$. The orthogonality of the first and last rows give $|C_3| = 6$. Since we have $a = b = c = d$, comparing with the order of G gives $a = b = c = d = 4$. Hence, the character table is

G	$\{1\}$	C_2	C_3	C_4	C_5	C_6	C_7
tr	1	1	1	1	1	1	1
χ_1^2	1	1	1	w	w^2	w	w^2
χ_1	1	1	1	w^2	w	w^2	w
χ_2	2	-2	0	-1	-1	1	1
$\chi_1\chi_2$	2	-2	0	$-w^2$	$-w$	w^2	w
$\chi_1^2\chi_2$	2	-2	0	$-w$	$-w^2$	w	w^2
χ_3	3	3	-1	0	0	0	0

The information on G is so far,
(a) $|G| = 24$.

(b) G has 7 conjugacy classes.
(c) The sizes of conjugacy classes are 1,1,6,4,4,4,4.

To determine the group G, we use the list of all groups of order 24.
(1) $\mathbb{Z}/24\mathbb{Z}$
(2) $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
(3) $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
(4) S_4
(5) $SL_2(\mathbb{Z}/3\mathbb{Z})$
(6) D_{24}
(7) $\mathbb{Z}/2\mathbb{Z} \times A_4$
(8) $\mathbb{Z}/2\mathbb{Z} \times D_{12}$
(9) $\mathbb{Z}/2\mathbb{Z} \times T$ (T is tetrahedron symmetry.)
(10) $\mathbb{Z}/3\mathbb{Z} \times D_8$
(11) $\mathbb{Z}/3\mathbb{Z} \times Q_8$
(12) $\mathbb{Z}/4\mathbb{Z} \times S_3$
(13) $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/8\mathbb{Z}$
(14) $\mathbb{Z}/3\mathbb{Z} \rtimes_\phi D_8$ where $\mathrm{Ker}(\phi) = V$.
(15) $\mathbb{Z}/3\mathbb{Z} \rtimes Q_8$

From (a),(b) above, we know that G is not abelian. So, we exclude (1),(2),(3). Since S_4 has 5 conjugacy classes, we exclude (4). Since D_{24} has a conjugacy class having size 2, we exclude (6). The number of conjugacy classes is 7 which is a prime number. Thus, we must exclude all groups which are direct product of cyclic group and another group. So, (7),$\cdots$, (12) are excluded. Using the multiplicative structure of semidirect product, we obtain that (13),(14),(15) have a conjugacy class of size 2. The only thing remains is (5), $SL_2(\mathbb{Z}/3\mathbb{Z})$.
We have a general result about the conjugacy classes of $SL_2(\mathbb{F}_q)$, where q is odd.

Representative	no.of classes	size of class
$\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$	2	1
$\begin{pmatrix} \pm 1 & 1 \\ 0 & \pm 1 \end{pmatrix}$	2	$\frac{(q-1)(q+1)}{2}$
$\begin{pmatrix} \pm 1 & \epsilon \\ 0 & \pm 1 \end{pmatrix}$,for some fixed $\epsilon \notin \left(\mathbb{F}_q^\times\right)^2$	2	$\frac{(q-1)(q+1)}{2}$
$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ $a \in \mathbb{F}_q^\times - \{\pm 1\}$	$\frac{q-3}{2}$	$q(q+1)$
$\begin{pmatrix} 0 & -1 \\ 1 & \alpha \end{pmatrix}$ $p(t) = t^2 - \alpha t + 1 \in \mathbb{F}_q[t]$ is irreducible.	$\frac{q-1}{2}$	$q(q-1)$

From this, we can verify that $SL_2(\mathbb{Z}/3\mathbb{Z})$ has 7 conjugacy classes having sizes 1,1,6,4,4,4,4. Further, there is only one way to express 24 as the sum of 1 and 6 other squares, namely $1^2 + 1^2 + 1^2 + 2^2 + 2^2 + 2^2 + 3^2$. The Artin-Wedderburn decomposition for $\mathbb{C}SL_2(\mathbb{Z}/3\mathbb{Z})$ is

$$\mathbb{C}SL_2(\mathbb{Z}/3\mathbb{Z}) = \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C}) \times M_2(\mathbb{C}) \times M_2(\mathbb{C}) \times M_3(\mathbb{C}).$$

Hence the group $SL_2(\mathbb{Z}/3\mathbb{Z})$ must have the same 7 by 7 character table as above.

Problem5.

• Solution of Cubic Equations by Radicals:

Consider a cubic polynomial $f(x) = x^3 + ax^2 + bx + c$. By substitution $x = y - a/3$, we have $f(x) = g(y) = y^3 + py + q$, where

$$p = \frac{1}{3}(3b - a^2), \quad q = \frac{1}{27}(2a^3 - 9ab + 27c).$$

Let α, β, γ be all roots of $g(y) = 0$. We want to express roots of $g(y) = 0$ in the form $A + B$ where $-3AB = p$. Using $A^3 + B^3 = (A+B)^3 - 3AB(A+B)$, we obtain

$$A^3 + B^3 = -q.$$

Also, we have $A^3B^3 = -\frac{p^3}{27}$. Thus, A^3, and B^3 are roots of the quadratic

$$t^2 + qt - \frac{p^3}{27} = 0.$$

From the formula for solution of quadratic equations,

$$A^3 = \frac{-q + \sqrt{q^2 + \frac{4}{27}p^3}}{2}$$

$$B^3 = \frac{-q - \sqrt{q^2 + \frac{4}{27}p^3}}{2}.$$

Choosing appropriate cubic roots of RHS which has to satisfy $-3AB = p$, we obtain that

$$\alpha = A + B, \quad \beta = wA + w^2B, \quad \gamma = w^2A + wB.$$

where $w = \exp(2\pi i/3)$.

• Solution of Quartic Equations by Radicals:

Consider a quartic polynomial $f(x) = x^4 + ax^3 + bx^2 + cx + d$. By substitution $x = y - a/4$, we have $f(x) = g(y) = y^4 + py^2 + qy + r$, where

$$p = \frac{1}{8}(-3a^2 + 8b)$$

$$q = \frac{1}{8}(a^3 - 4ab + 8c)$$

$$r = \frac{1}{256}(-3a^4 + 16a^2b - 64ac + 256d).$$

Let $\alpha, \beta, \gamma, \delta$ be all roots of $g(y) = 0$. Add $(ly + m)^2$ to the equation $g(y) = 0$, then we obtain

$$y^4 + py^2 + qy + r + (ly + m)^2 = (ly + m)^2.$$

We use $(y^2 + \lambda)^2 = y^4 + 2\lambda y^2 + \lambda^2$, to complete the square of LHS above, which is

$$y^4 + (p + l^2)y^2 + (q + 2lm)y + r + m^2 = (ly + m)^2.$$

Comparing the coefficient,

$$2\lambda = p + l^2, \quad q + 2lm = 0, \quad r + m^2 = \lambda^2.$$

Then, it follows that

$$(2\lambda - p)(\lambda^2 - r) = \frac{q^2}{4}.$$

Since this is a cubic equation for λ, let λ be a real root for this cubic equation, which can be solved by radicals. Then we have

$$(y^2+\lambda)^2 = (ly+m)^2$$

where $l = \sqrt{2\lambda - p}$, and $m = \sqrt{\lambda^2 - r}$. Now, we reduced the quartic to two quadratics, $y^2 + \lambda = ly + m$, and $y^2 + \lambda = -ly - m$. Hence, the general solution for $g(y) = 0$ is

$$\alpha = \frac{l + \sqrt{l^2 - 4(\lambda - m)}}{2}, \quad \beta = \frac{l - \sqrt{l^2 - 4(\lambda - m)}}{2},$$
$$\gamma = \frac{-l + \sqrt{l^2 - 4(\lambda + m)}}{2}, \quad \delta = \frac{-l - \sqrt{l^2 - 4(\lambda + m)}}{2}.$$