506 Final

Daniel Rui - 6/7,8/21

Problem 1

Let k be an algebraically closed field and A a finitely generated commutative k-algebra (k-module = k-VS that also has ring structure, i.e. multiplication). We want to determine all simple modules over A. Prop. 2.12 from Lec 19 tells us that for a not-necessarily-commutative-ring R with 1, an R-module M is simple if and only if $M \simeq {}^{R}/_{I}$ (module isomomorphism!) for a maximal left ideal $I \lhd R$. In our case, $R = A$ is commutative, so $M \simeq {}^{R}/_{I}$ for a maximal ideal $I \lhd A$ where $K := {}^{R}/_{I}$ is a field (in commutative ring, quotient by maximal ideal is field).

K is a field extension of k because for every element $c \in k$, c is not in I (since k is a field, c would be a unit, so $c \in I$ would imply $I = A$, but I is PROPER maximal ideal). It is also a finitely generated k-algebra, because it is generated by the same elements as A as a k-algebra (and we assumed A was finitely generated k-algebra above). Theorem 1.136 (in Sándor's commutative algebra notes, CA.pdf; see also Problem 7 on the Midterm where this theorem played a starring role) tells us that because K is a field extension of k that is also finitely generated k-algebra, K is a finite algebraic extension of k. But k is algebraically closed, so any finite algebraic extension of it equals itself, i.e. $K = k$ (I used the same trick in Problem 5 of Homework 7). Do note that k is not ACTUALLY a subset of K, just its isomorphic coset copy, so perhaps it is better to write $K \simeq k$.

Thus, every simple module of A is isomorphic to k (when thought of as an A-module).

Problem 2

Let $(A, \mathfrak{m})$ be a commutative local ring. We want to show that A can not be a direct sum of two non-trivial rings R, S. Recall that $A \simeq R \oplus S \iff A = R + S, R \cap S = \{0\}$, where the RHS makes sense if we think of R, S are subrings of A, which we can always do because we can take suitable isomorphic copies of R, S in A via the isomorphism $A \simeq R \oplus S$. So from here on out, let us just suppose R, S denote subrings in A.

I now claim that R, S are proper ideals in A. They are proper because R, S are both non-trivial, and ideals because they are subrings, and given any $a \in A, r \in R$, $ar = r_1 + s_1$ (because $A = R + S$), implying $ar - r_1 = s_1 \in R \cap S \implies ar - r_1 = s_1 = 0 \implies ar = r_1 \in R$ (same argument for S).

Because all ideals are contained in some maximal ideal (Zorn's lemma), but A only has one maximal ideal $\mathfrak{m}$, we have that $R, S \subseteq \mathfrak{m}$. But then because $A = R + S$, we will have that $A \subseteq \mathfrak{m}$, contradicting that $\mathfrak{m}$ is a PROPER maximal ideal.

Problem 3

Let G be a finite group and M a $\mathbb{C}[G]$-module. We want to show that M is both projective and injective as a $\mathbb{C}[G]$-module. Maschke's theorem (Thm 2.40 in Lec 25) says that $\mathbb{C}[G]$ is a semisimple ring, and Prop. 2.25 in Lec 21 tells us that if R is semisimple ring and N is R-module, then N is semisimple R-module, implying that M (our $\mathbb{C}[G]$-module above) is in fact a semisimple $\mathbb{C}[G]$-module. By Prop 2.21(ii) in Lec 20, M is a direct sum of some simple $\mathbb{C}[G]$-modules $M_i \subseteq M$.

Lemma 2.49 in Sándor's homological algebra notes (CT-HA-all.pdf) tells us that $P \oplus Q$ is projective module $\iff$ P, Q projective modules, and $I \oplus J$ injective modules $\iff$ I, J injective modules. Thus, to prove M projective and injective, it suffices to show that all SIMPLE $\mathbb{C}[G]$-modules are projective and injective.

Recall the following definitions of injective and projective modules (resp. Problem 3 and Problem 4 of 506HW2): a module I is injective $\iff$ every $I \hookrightarrow N$ splits (for arbitrary module N); and a module P is projective $\iff$ every $N \twoheadrightarrow P$ splits. So now let I, J be arbitrary simple $\mathbb{C}[G]$-modules.

Observe that an injection $\iota : I \hookrightarrow N$ and surjection $\pi : N \twoheadrightarrow P$ can be extended to the short exact sequences $0 \to I \hookrightarrow N \twoheadrightarrow N/\operatorname{im}(\iota) \to 0$ and $0 \to \ker(\pi) \hookrightarrow N \twoheadrightarrow P \to 0$. Recall now the splitting lemma from homological algebra (see Prop. 25, 26 pg. 383-385 in Dummit & Foote, 3rd Edition), which tells us the following are three equivalent definitions of "splitting" for a short exact sequence of R-modules $0 \to A \overset{\alpha}{\hookrightarrow} B \overset{\beta}{\twoheadrightarrow} C \to 0$: $\textcircled{1}$ $B = \alpha(A) \oplus C'$ (i.e. $B = \alpha(A) + C'$, $\alpha(A) \cap C' = \{0\}$) for some submodule $C' \subseteq B$ s.t. $\beta(C') = C$ (so $B = \alpha(A) \oplus C' \simeq A \oplus C$); $\textcircled{2}$ the injection $\alpha : A \hookrightarrow B$ splits, i.e. there is module homomorphism $s : B \to A$ s.t. $s \circ \alpha = \mathrm{id}_A$; and $\textcircled{3}$ the surjection $\beta : B \twoheadrightarrow C$ splits, i.e. there is module homomorphism $s : C \to B$ s.t. $\beta \circ s = \mathrm{id}_C$.

To complete the proof, I now show that any short exact sequence (s.e.s.) of $\mathbb{C}[G]$-modules $0 \to A \overset{\alpha}{\hookrightarrow} B \overset{\beta}{\twoheadrightarrow} C \to 0$ satisfies condition $\textcircled{1}$, thereby giving us in particular that the short exact sequences above (corresponding to $I \hookrightarrow N$ and $N \twoheadrightarrow P$) split, yielding by $\textcircled{2}$ and $\textcircled{3}$ that $I \hookrightarrow N$ and $N \twoheadrightarrow P$ split for an arbitrary $\mathbb{C}[G]$-module N, implying of course that I, P are respectively injective and projective, as desired (I, P were arbitrarily chosen simple $\mathbb{C}[G]$-modules).

Well, Prop. 2.21(iii) in Lec 20 tells us that for semisimple modules (which again $\mathbb{C}[G]$-modules are, by Maschke (Thm. 2.40 in Lec 25) and Prop. 2.25 in Lec 21), like B in the s.e.s., every submodule of B is a direct summand of B. In particular, we see that $\alpha(A)$ is a submodule of B, so $B = \alpha(A) \oplus L$ for some submodule $L \subseteq M$. Then, $L \simeq B/\alpha(A)$, but by the property of s.e.s. that $\alpha(A) = \operatorname{im}(\alpha) = \ker(\beta)$, we have $L \simeq B/\ker(\beta) \simeq \operatorname{im}(\beta) = C$ by the 1st isomorphism theorem. Thus indeed $\textcircled{1}$ is satisfied by all such s.e.s. of $\mathbb{C}[G]$-modules.

Remarks: we did not need to simplify to the "simple module" case (i.e. we could have deleted that paragraph on projective and injective modules being preserved by direct sums, and made I, P arbitrary $\mathbb{C}[G]$-modules instead of arbitrary SIMPLE $\mathbb{C}[G]$-modules), but it was good review so I kept it in.

Problem 4

We are asked to state Nakayama's lemma, and use it to prove that for any commutative Artinian local ring $(A, \mathfrak{m})$ and a not-necessarily-finitely-generated A-module M and subset $S \subseteq M$ s.t. the image of S in $M/\mathfrak{m}M$ generates $M/\mathfrak{m}M$, it must be that S also generates M.

First things first, **Nakayama's lemma** (Corollary 1.73 in Sándor's commutative algebra notes, CA.pdf) says that for a commutative local ring $(A, \mathfrak{m})$ and finite (-ly generated) A-module M, $M = \mathfrak{m}M \implies M = 0$. A corollary (Corollary 1.74) of this is that for a commutative local ring $(A, \mathfrak{m})$ and A-module M with submodule $N \subseteq M$ s.t. M/N is a finite A-module and $M = N + \mathfrak{m}M$, then it must be that $N = M$ (the proof is that $M = N + \mathfrak{m}M \implies M/N = \mathfrak{m} \cdot M/N$, so Nakayama gives $M/N = 0 \implies M = N$). In particular, if M is a finite A-module and $x_1, \ldots, x_n \in M$ are s.t. their images generate $M/\mathfrak{m}M$, then taking $N = \langle x_1, \ldots, x_n \rangle$, the above corollary yields that $N = M$, i.e. M is generated by $x_1, \ldots, x_n$. Essentially, this problem loosens the restriction that M is a finite A-module, at the cost of further assuming that A is Artinian.

Observe that the requirement that M be a finite A-module in the "corollary to the corollary" is inherited from the statement of **Nakayama's lemma**, which is inherited from the "determinant trick" (Theorem 1.71 in CA.pdf). So, if we manage to prove **Nakayama's lemma** (as stated above) some other way (i.e. using the "extra" assumption that A is Artinian/satisfies the DCC = descending chain condition) that doesn't require M to be finite, then we will be done.

Here's the plan: tinkering with our proof from 506HW3p6 (in which we used the DCC to show that the nilradical is nilpotent), we can show that $\mathfrak{m}$ is in fact nilpotent ($\mathfrak{m}^n = \{0\}$ for some $N \in \mathbb{N}$), which suffices to show that for ANY A-module M with $M = \mathfrak{m}M$ (which implies $\mathfrak{m}^k M = \mathfrak{m}^{k+1}M$ by induction/multiplying by $\mathfrak{m}$ on the left repeatedly), $M = \mathfrak{m}M = \mathfrak{m}^2 M = \ldots = \mathfrak{m}^n M = \{0\}M = 0$. We will have then proven that the statement of Nakayama's lemma holds for general A-modules (in the case of local commutative Artinian rings A), and so the "corollary to the corollary" above about pulling back generating sets of $M/\mathfrak{m}M$ to generating sets of M will hold for general A-modules, thus concluding the problem.

I now copy over my proof from 506HW3p6 and make the appropriate edits: let A be as above (commutative local Artinian, unique maximal ideal $\mathfrak{m}$). We want to prove using the DCC that $\mathfrak{m}$ is nilpotent, i.e. there exists $n \in \mathbb{N}$ s.t. $\mathfrak{m}^n = 0$. We can now construct the following descending chain: $\mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \ldots$, which must by the DCC satisfy $\mathfrak{m}^N = \mathfrak{m}^{N+1} = \ldots$ for some $N \in \mathbb{N}$. Suppose now that $\mathfrak{m}^N \neq 0$ (i.e. the descending chain stabilizes not at 0, so there is no $n \in \mathbb{N}$ s.t. $\mathfrak{m}^n = 0$).

Define $\mathscr{S}$ to be the set of ideals $I \lhd A$ s.t. $I\mathfrak{m}^N \neq 0$ (note that $\mathfrak{m} \in \mathscr{S}$). Because A is Artinian, $\mathscr{S}$ must have a minimal element (reminder: if there's no minimal element, we can get a descending chain that does not plateau), say $\mathfrak{a} \lhd A$. By the condition we placed on $\mathscr{S}$, $\mathfrak{a}\mathfrak{m}^N \neq 0$, so in fact there must exist some $a \in \mathfrak{a}$ s.t. $a\mathfrak{m}^N \neq 0$. Then, the ideal $\langle a \rangle$ must be in $\mathscr{S}$ too, and because $\langle a \rangle \subseteq \mathfrak{a}$, $\langle a \rangle$ must equal $\mathfrak{a}$ by minimality of $\mathfrak{a}$.

Now because $\mathfrak{m}^N = \mathfrak{m}^{N+1}$, we have $\mathfrak{a}\mathfrak{m}^N = \mathfrak{a}\mathfrak{m}^{N+1} \neq 0$. Because A is commutative, $\mathfrak{a}\mathfrak{m}^N = \mathfrak{m}^N\mathfrak{a} = \mathfrak{m}^{N+1}\mathfrak{a}$, so defining L to be the module consisting of elements from $\mathfrak{m}^N\mathfrak{a}$ with A-action defined as multiplication in the ring A, we have that $L = \mathfrak{m}L$. But L is generated by $a \in \langle a\rangle = \mathfrak{a}$ as an A-module, because every element of L (i.e. every element in $\mathfrak{m}^N\mathfrak{a}$) is just some element of A times a! And **Nakayama's lemma** as stated above tells us that since L is a finitely-generated A-module satisfying $L = \mathfrak{m}L$, it must be that $L = 0$. This of course contradicts the earlier statement that $\mathfrak{m}^N\mathfrak{a} \neq 0$. QED.

Problem 5

Let k be a algebraically closed field (not necessarily characteristic 0!), and let H be a finite abelian group of order $n \in \mathbb{N}$ and G be an arbitrary (not necessarily finite!) group with $g \in G$ an element of order $m \in \mathbb{N}$.

(a) Assuming that $\operatorname{char} k \nmid n$, we want to show that H has exactly n (pairwise) inequivalent irreducible representations over k, all of which are linear (i.e. 1-dimensional).

Recall **Theorem 3.2** from Lec 25 on 5/26/21 about complex representations of finite groups, which tells us that (i) $\mathbb{C}[G] \simeq \bigoplus_{i=1}^r M_{n_i}(\mathbb{C})$, and (ii) $\mathbb{C}[G]$ has r distinct isomorphism classes of simple modules $M_1, \ldots, M_r$ with dimensions $n_1, \ldots, n_r$ (when thought of as $\mathbb{C}$ vector spaces), where (iii) $\sum_{i=1}^r n_i^2 = |G|$ and (iv) $r = \dim_{\mathbb{C}} Z(\mathbb{C}[G])$ as well as the number of conjugacy classes in G. Let us do a **rundown of the proof to see that we can generalize** this to the field k (instead of $\mathbb{C}$) and $G = H$, which suffices to prove part (a) because H abelian $\implies$ H has $|H| = n$ conjugacy classes $\implies$ $r = n$ by (iv), but (iii) $\sum_{i=1}^r n_i^2 = |H| \implies n_i = 1$ for each $i \in [r]$, and as irreducible representations are in 1-1 correspondence with the simple modules (up to homomorphism) with dimension of representation = dimension of module (as vector space over k), (ii) gives that there are exactly $r = n$ isomorphism classes of simple modules/irreducible representations with dimension $n_i = 1$ for all $i \in [r]$.

(i) follows from Maschke's theorem/Thm. 2.40 in Lec 25 (which says that $k[H]$ is semisimple IF $\operatorname{char} k \nmid n = |H|$), Artin-Wedderburn/Thm. 2.33 in Lec 23 (which decomposes arbitrary semisimple rings into matrix rings over some division rings), and 506HW7p5 (which says that if an algebraically closed field k contained in the center of a division ring D s.t. D as a vector space is finite dimensional over k, then $D = k$). Everything used in this step is not specific to $\mathbb{C}$, and generalizes to our situation.

(ii) follows from (i) above, Prop. 2.26 in Lec 21 (which says that a simple R-module for a semisimple ring R is isomorphic to a direct summand of R) applied to $R = k[G]$ (again using Maschke as in (i) above), and 506HW7p2 (which says that matrix ring M_n over a division ring D has unique simple module isomorphic to D^n as a vector space). Last part about simple modules corresponding to different summands being non-isomorphic follows from Prop. 2.30 in Lec 22. Everything used in this step is not specific to $\mathbb{C}$, and generalizes to our situation.

(iii) follows from dimension count of (i). Obviously not specific to $\mathbb{C}$ and generalizes.

(iv) we start in the proof of (iv) in Lec 25 with the claim that $Z(M_n(\mathbb{C})) \simeq \mathbb{C}$. This generalizes to any field k, and so indeed $\dim_k Z(k[H]) = r$. The rest of the proof about conjugacy classes $\mathscr{C}_1, \ldots, \mathscr{C}_q$ and $x_i := \sum_{h \in \mathscr{C}_i} h \in k[H]$, $i \in [q]$, forming a basis of $Z(k[H])$ is also not dependent on $\mathbb{C}$ and generalizes to k.

(b) Let $\varrho : G \to \mathrm{GL}_k(V)$ be a finite dimensional representation of G over k and assume that $\operatorname{char} k \nmid m$. We want to prove that there exists a basis of V that consists of eigenvectors of the linear transformation $\varrho(g)$ (for the arbitrary $g \in G$ fixed at the beginning of the problem, where g has order $m \in \mathbb{N}$), WITHOUT using any statements about matrices/Jordan normal forms.

Note that this condition about a basis of eigenvectors is equivalent to $\varrho(g)$ being diagonalizable, and we have already seen a proof that $\varrho(g)$ is diagonalizable in class (Prop. 3.20 in Lec 27) using that the minimal polynomial of $\varrho(g)$ divides $x^m - 1$ (since eigenvalues of $\varrho(g)$ satisfy $x^m - 1$: given eigenvector v s.t. $\varrho(g)v = \lambda v$ for some $\lambda \in k$, $v = I_n v = \varrho(g^m)v = \lambda^m v \implies \lambda^m = 1$), hence has distinct roots, which implies that the Jordan normal form is a diagonal matrix. Basically, this problem is asking us to find an alternate proof that minimal polynomial having distinct roots implies diagonalizable.

Let $\lambda_1, \ldots, \lambda_l$ be the distinct eigenvalues of $\varrho(g)$ (so $l \leq m$, and each λ_i is a root of unity in k). Denote the eigenspace $E_i := \ker(\varrho(g) - \lambda_i I_n)$. Each eigenspace is a k vector space of some dimension d_i, and has some basis $\mathscr{B}_i := \{b_{i,1}, \ldots, b_{i,d_i}\}$. If we show that $V = E_1 + \ldots + E_l$ (i.e. every vector $v \in V$ can be written as sum of some elements of the eigenspaces), then $\tilde{\mathscr{B}} := \bigcup_{i=1}^{l} \mathscr{B}_i$ will form a spanning set of V composed of eigenvectors, and refining $\tilde{\mathscr{B}}$ if necessary to $\mathscr{B}$ by removing linearly dependent vectors, we produce a basis $\mathscr{B}$ of V consisting solely of eigenvectors, thus finishing the problem.

EDIT after due date 11:30 AM 6/8/21: neat proof here. Minimal polynomial $m(x)$ of matrix A is minimal monic polynomial in $k[x]$ s.t. $m(A) = 0$. Fact: minimal polynomial divides any other polynomial that kills A (Thm 4.4 in KConrad article). Cayley-Hamilton tells us in particular characteristic polynomial kills A. Moreover, roots of m and characteristic polynomial are the same, i.e. roots of m are exactly eigenvalues of A (Thm 4.7 in KConrad article). Thus, m not have repeated roots $\implies$ $m = (x - \lambda_1) \cdots (x - \lambda_l)$. Consider $\frac{1}{m(x)}$ and partial fraction decomposition:

$$\frac{1}{m(x)} = \frac{1}{(x - \lambda_1) \cdots (x - \lambda_k)} = \sum_{i=1}^{l} \frac{c_i}{(x - \lambda_i)}$$

for some $c_i \in k$. Define

$$Q_i(x) = \frac{c_i m(x)}{(x - \lambda_i)} = c_i \prod_{j \neq i, j \in [l]} (x - \lambda_j).$$

Then,

$$\textcircled{1} \qquad \sum_{i=1}^{l} Q_i(x) = 1 \implies \sum_{i=1}^{l} Q_i(A) = I_n$$

(because if one can expand out $\sum_{i=1}^{l} Q_i(x)$ and all powers of $x^{1,2,\cdots}$ die leaving $x^0 = 1$, replacing symbol x with symbol A we see all powers of $A^{1,2,\cdots}$ die leaving $A^0 = I_n$) and

$$\textcircled{2} \qquad Q_i(x)(x - \lambda_i) = c_i m(x) \implies Q_i(A)(A - \lambda_i I_n) = (A - \lambda_i I_n) Q_i(A) = c_i m(A)$$

(same reasoning as above, just replacing symbols x, A; we have commutativity because $Q_i(A)$ is just sums of powers of A and powers of A commute). Finally, ① gives that for any $v \in V$, $v = I_n v = [\sum_{i=1}^{l} Q_i(A)]v = \sum_{i=1}^{l}[Q_i(A)v]$, and ② gives $Q_i(A)v \in \ker(A - \lambda_i I_n)$ because $[A - \lambda_i I_n]Q_i(A)v = c_i m(A)v = 0$.

Problem 6

Definition of complex character table: let G be a finite group with r conjugacy classes $\mathscr{C}_1, \ldots, \mathscr{C}_r$ and irreducible complex characters $\chi_1, \ldots, \chi_r$. The complex character table of G is an $r \times r$ matrix of complex numbers where the (i,j)th entry e_{ij} is $\chi_i(x_j)$ where $x_j \in \mathscr{C}_j$ is arbitrary. Suppose we have the following complex character table with some entries missing:

	$\mathscr{C}_1$	$\mathscr{C}_2$	$\mathscr{C}_3$	$\mathscr{C}_4$	$\mathscr{C}_5$
χ_1					
χ_2					-1
χ_3				-1	1
χ_4			-1	1	-1
χ_5		-2	0	0	0

(a) We wish to fill in the rest of the table. Recall the "second orthogonality relation for group characters" (Theorem 3.25 in Lec 28) which says that for any $g, h \in G$, $\sum_{i=1}^{r} \chi_i(g)\overline{\chi_i(h)}$ equals $|C_G(g)| = |G|/|\mathscr{C}_g|$ if g, h are in the same conjugacy class/are conjugate in G, and equals 0 otherwise. In our case, $r = 5$. We know that one of our conjugacy classes $\mathscr{C}_e$ consists of exactly one element, the identity $\{e\}$, so the "2nd ortho relation" gives $\sum_{i=1}^{5} |\chi_i(e)|^2 = |G|$ (Prop. 3.11 in Lec 26 says that since $\mathbb{C}$ is characteristic 0, $\deg \chi_i = \chi_i(e)$, and indeed $\deg \chi_i = n_i$ for the $n_1, \ldots, n_5$ from Thm. 3.2 in Lec 25). **Example:** let us take $g, h \in \mathscr{C}_5$; then $\sum_{i=1}^{5} \chi_i(\mathscr{C}_5)\overline{\chi_i(\mathscr{C}_5)} = |e_{15}|^2 + |-1|^2 + 1^2 + |-1|^2 + 0^2 = 3 + |e_{15}|^2 = |G|/|\mathscr{C}_5|$.

The "1st ortho relation" (Thm. 3.23 in Lec 28) says that defining $\langle \theta, \psi \rangle := \frac{1}{|G|}\sum_{g \in G} \theta(g)\overline{\psi(g)}$, $\langle \chi_i, \chi_j \rangle = \delta_{ij}$ for all $i, j \in [r]$. In particular, we have

$$|G|\langle \chi_i, \chi_j \rangle = \sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} = \sum_{k=1}^{5} |\mathscr{C}_k| \cdot \chi_i(\mathscr{C}_k)\overline{\chi_j(\mathscr{C}_k)} = |G| \cdot \delta_{ij}.$$

Example: taking $i = 5$, we see $\sum_{k=1}^{5} |\mathscr{C}_k| \cdot |\chi_5(\mathscr{C}_k)|^2 = |e_{51}|^2 \cdot |\mathscr{C}_1| + |-2|^2 \cdot |\mathscr{C}_2| + 0 + 0 + 0 = |G|$.

It is now at this time that I realize that I have overlooked something very trivial. Indeed, EVERY group has the trivial complex representation with corresponding character $\chi(g) = 1$ for all $g \in G$. Because χ_i for $i = 2, 3, 4, 5$ in the above table are not 1 for at least one known value, it must be that χ_1 is this trivial character, and so we can fill in the top row $\{e_{11}, \ldots, e_{15}\}$ with just ones. In the $(\mathscr{C}_5, \mathscr{C}_5)$ example above, we now plug in $3+|e_{15}|^2 = 4 = |G|/|\mathscr{C}_5|$. Using "2nd ortho" on these new values we see that $\sum_{i=1}^{5} \chi_i(\mathscr{C}_4)\overline{\chi_i(\mathscr{C}_5)} = 1^2 + e_{24}(-1) + (-1)1 + 1(-1) + 0 = -e_{24} - 1 = 0$, so $e_{24} = -1$. Our table now looks like

	$\mathscr{C}_1$	$\mathscr{C}_2$	$\mathscr{C}_3$	$\mathscr{C}_4$	$\mathscr{C}_5$
χ_1	1	1	1	1	1
χ_2				-1	-1
χ_3				-1	1
χ_4			-1	1	-1
χ_5		-2	0	0	0

Because we know $\chi_i(e) = \chi_i(\mathscr{C}_e)$ equals $\deg \chi_i$, which is a positive integer (again equals n_i from the $n_1, \ldots, n_5$ from Thm. 3.2 in Lec 25), and the columns for $\mathscr{C}_2, \ldots, \mathscr{C}_5$ have negative numbers, it must be that $\mathscr{C}_1 = \{e\}$. Then, $e_{51} \in \mathbb{N}$, and so the above example yields $|e_{51}|^2 \cdot |\mathscr{C}_1| + |-2|^2 \cdot |\mathscr{C}_2| + 0 + 0 + 0 = e_{51}^2 + 4|\mathscr{C}_2| = |G|$. As $|\mathscr{C}_5| = \frac{|G|}{4}$, we see that e_{51} must be divisible by 2, and $|G| \geq 8$.

Aha! Two unknowns in the 3rd column can be solved by forming two equations using "2nd ortho" with 4th and 5th column. "2nd ortho" on $(\mathscr{C}_3, \mathscr{C}_4)$ and $(\mathscr{C}_3, \mathscr{C}_5)$ respectively yields $1 - e_{23} - e_{33} - 1 + 0 = 0$ and $1 - e_{23} + e_{33} + 1 + 0 = 0$; adding the two equations yields $2 - 2e_{23} = 0 \implies e_{23} = 1$, which of course implies $e_{33} = -1$.

We can then find the 3 unknowns in column 2 using 3 equations formed using column 2 and columns 3,4,5. And then of course the final 4 unknowns in column 1 using 4 equations formed using column 1 and columns 2,3,4,5. Doing so (I will not type out these computations) yields

	$\mathscr{C}_1$	$\mathscr{C}_2$	$\mathscr{C}_3$	$\mathscr{C}_4$	$\mathscr{C}_5$
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	-1	1
χ_4	1	1	-1	1	-1
χ_5	2	-2	0	0	0

(b) Now we find the size of the group, center, commutator subgroup, and conjugacy classes. Using "2nd ortho" on all pairs $(\mathscr{C}_i, \mathscr{C}_i)$, we get $1 + 1 + 1 + 1 + 4 = 8 = |G|/|\mathscr{C}_1| = |G|$ (recall from above $\mathscr{C}_1 = \{e\}$); and also $1+1+1+1+4 = 8 = |G|/|\mathscr{C}_2| \implies |\mathscr{C}_2| = 1$. Doing the same thing for $\mathscr{C}_i$ $(i = 3, 4, 5)$, we see $1 + 1 + 1 + 1 = 4 = |G|/|\mathscr{C}_i|$, so $|\mathscr{C}_i| = 2$ (again for $i = 3, 4, 5$). The $n_1, \ldots, n_5$ from Thm 3.2 from Lec 25 (i.e. degrees of χ_i) are just the first column of the table: $1, 1, 1, 1, 2$ (so there are 4 irreducible 1-dimensional complex representations).

An element is in the center if and only if its conjugacy class has 1 element, so $Z(G) = \mathscr{C}_1 \cup \mathscr{C}_2$ has 2 elements.

Corollary 3.4 from Lec 26 says that for any finite group G, the number of inequivalent irreducible complex 1-dimensional representations is $|G/G'| = |G|/|G'|$ for the commutator subgroup $G' = [G, G]$. Thus, $4 = 8/|G'| \implies |G'| = 2$.

EXTRA FOR LATER: recall from 504 that there are 5 groups of order 8: the abelian ones $\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, and the non-abelian ones D_8, Q_8 (dihedral group of order 8 and quaternion group of order 8). Of course G here is non-abelian ($|Z(G)| = 2 < 8 = |G|$), so G must be either D_8 or Q_8.

(c) We are asked to try to write down a composition series for G to determine whether or not G is solvable. In either case $G = D_8, Q_8$, we can form composition series (quotients are order 2 hence normal): $\{1\} \triangleleft \{1, r^2\} \triangleleft \{1, r, r^2, r^3\} \triangleleft D_8$ and $\{1\} \triangleleft \{1, -1\} \triangleleft \{1, i, -1, -i\} \triangleleft Q_8$ (order 4 subgroups are always normal in G because they are index 2).

(d) We are asked to determine the set S of numbers that occur as orders of some elements of the group. By Lagrange, $S \subseteq \{1, 2, 4, 8\}$. Obviously not 8 because that would mean $G \simeq \mathbb{Z}_8$ (in particular abelian), so $S \subseteq \{1, 2, 4\}$. Indeed, this containment is equality because in either case $G = D_8, Q_8$, there are elements of each order ($1, s, r$ and $1, -1, i$ resp.).

(e) In either case $G = D_8, Q_8$, there are 3 order 4 subgroups (see lattice on pg. 99 of Dummit & Foote, 3rd ed.): $\langle r \rangle$, $\{1, r^2, sr, sr^3\}$, $\{1, r^2, s, sr^2\}$ and $\langle i \rangle, \langle j \rangle, \langle k \rangle$.

(f) As already established, G is either D_8 or Q_8 (see end of part (b) above).

(g) If we furthermore know that all subgroups of the group G were normal, could we determine G precisely? Well, $\{1, s\}$ is NOT normal in D_8 because $rsr^{-1} = r^2 s \notin \{1, s\}$, so G given this further assumption must be Q_8.

506 Homework 8

Daniel Rui - 6/5/21

Preliminary definitions: recall from Lec 24 on 5/24/21 (pg. 3 of my green notebook) the following definitions: for a c1-ring A, group G, and M left $A[G]$-module, left multiplication by an element of $A[G]$ gives an A-module endomorphism of M, i.e. $\Phi : A[G] \to \text{End}_A(M)$ given by $\sum a_g g \mapsto [x \mapsto \sum a_g gx]$ is a ring homomorphism, where $[x \mapsto \sum a_g gx]$ is indeed an A-module endomorphism of M (i.e. A-linear map $M \to M$) because $A \subseteq Z(A[G])$. Beware that $[x \mapsto \sum a_g gx]$ is NOT an $A[G]$-linear map (i.e. $A[G]$-module homomorphism) $M \to M$.

Such a Φ restricted to G becomes group homomorphism $\varrho := \Phi|_G : G \to \text{Aut}_A(M)$, where the codomain is the set of automorphisms instead of endomorphisms because elements of g have inverses, and hence $[x \mapsto gx]$ has inverse $[x \mapsto g^{-1}x]$, hence automorphism. This $\varrho : G \to \text{Aut}_A(M)$ is called a "representation of G on M over A". If $A = k$ is a field, then M can be thought of as a vector space V over k (M left $k[G]$-module, so in particular k-module = k vector space), and $\text{Aut}_A(M) = \text{GL}_k(V)$, i.e. the set of invertible linear maps $V \to V$, and in the case that V has dimension d as a vector space over k, since all finite vector spaces of the same dimension are isomorphic (to k^d), $\text{GL}_k(V)$ is the set of $d \times d$ invertible matrices with entries in k.

In fact, we can go the other direction as well: given any group homomorphism $\varrho : G \to \text{Aut}_A(M)$ can be extended linearly to a map $\Phi : A[G] \to \text{End}_A(M)$, i.e. $\Phi = [\sum a_g g \mapsto \sum a_g \varrho(g)]$. So there is a **1-1 correspondence** between such ϱ and Φ.

There is also **1-1 correspondence** between Φ/ϱ ("/" in this paragraph is "or", not "quotient") and left $A[G]$-modules M: the direction $M \rightsquigarrow \Phi/\varrho$ is discussed above ("$\rightsquigarrow$" read "leads to" or "yields"), and for the other direction, it may seem we are forgetting a lot of information about M only considering $\text{End}_A(M)$ or $\text{Aut}_A(M)$ (e.g. in the case $A = k$, $\text{GL}_k(V)$ only is about k-VS (=k-module) structure of V, not (left) $k[G]$-module structure of V), but we recover the module structure of V by defining $\sum a_g g \bullet v = [\Phi(\sum a_g g)](v)$ for $v \in V$ (or equivalently $g \bullet v = [\varrho(g)](v)$ and extending linearly to $k[G]$).

Lastly, we define ϱ is called "faithful" if ϱ is injective; "trivial" if $\varrho(g) = \text{id}_M$ for all $g \in G$; and "irreducible" if M is a simple $A[G]$-module $\iff$ M does not have a G-invariant ($[\varrho(g)](m) \in M$ for all $g \in G, m \in M$) non-trivial (proper) sub-A-module. Two representations are equivalent $\varrho \sim \varrho' \iff$ their corresponding modules M, M' are isomorphic **as $\boldsymbol{A[G]}$-modules**. If A is a field k, then $\varrho \sim \varrho' \iff \varrho = Q^{-1}\varrho' Q$ for some $Q \in \text{GL}_k(V)$ (i.e. there is $Q \in \text{GL}(d, k)$ s.t. for all $g \in G$, the $d \times d$ matrices $\varrho(g)$ and $\varrho'(g)$ are conjugate via Q).

For the below problems, we will mainly be focusing on complex representations, i.e. taking $A = \mathbb{C}$.

Problem 1

Recall Theorem 3.2 from Lec 25 on 5/26/21 about complex representations of finite groups, which tells us that (i) $\mathbb{C}[G] \simeq \bigoplus_{i=1}^r M_{n_i}(\mathbb{C})$, and (ii) $\mathbb{C}[G]$ has r distinct isomorphism classes of simple modules $M_1, \ldots, M_r$ with dimensions $n_1, \ldots, n_r$ (when thought of as $\mathbb{C}$ vector spaces), where (iii) $\sum_{i=1}^r n_i^2 = |G|$ and (iv) $r = \dim_{\mathbb{C}} Z(\mathbb{C}[G])$ as well as the number of conjugacy classes in G. For this problem, $G = S_3$, and we are asked to find all the irreducible complex representations of G.

S_3 has three conjugacy classes: $\{()\}$, $\{(12),(13),(23)\}$, $\{(123),(132)\}$. Thus, by (iv) of the above cited Theorem 3.2, $r = 3$, and as n_i ($i \in [r]$) are positive integers whose squares sum to $|S_3| = 6$ by Thm3.2(iii), they must be $1, 1, 2$ ($3^2 = 9$ is too big, and $2^2 + 2^2 = 4 + 4 = 8$ is too big, leaving just $1^2 + 1^2 + 2^2 = 6$).

Because irreducible (complex) representations are in 1-1 correspondence with the simple modules (up to isomorphism) of $\mathbb{C}[G]$, and Thm3.2(ii) tells us that there are exactly 3 distinct isomorphism classes of simple modules of $\mathbb{C}[G]$, with dimensions $1, 1, 2$ (when thought of as $\mathbb{C}$ vector spaces), we have exactly 3 irreducible complex representations of S_3, two of which are of the form $S_3 \to \mathrm{GL}(1, \mathbb{C}) = \mathbb{C}^\times$, and one of which is of the form $S_3 \to \mathrm{GL}(2, \mathbb{C})$.

We already know (basically off the top of our heads) two group homomorphisms $G \to \mathbb{C}^\times$: the trivial map/representation $g \mapsto 1$ for all $g \in G$ (corresponding to the trivial $\mathbb{C}[G]$-module structure on $V = M_1(\mathbb{C}) = \mathbb{C}^\times$: $g \bullet v = \mathrm{id}_V(v) = v$), and the sign homomorphism $\mathrm{sgn}(\sigma) : S_3 \to \{1, -1\} \subseteq \mathbb{C}^\times$ (from 504HW4/symmetric worksheet, where we used it to define $A_n := \ker(\mathrm{sgn}_n)$). The sign homomorphism correspond to the $\mathbb{C}[G]$-module structure on $\mathbb{C}^\times$: $g \bullet v = \mathrm{sgn}(g) \cdot v$, where "$\cdot$" on the RHS is complex multiplication.

Obviously the two $\mathbb{C}[G]$-module structures are different, so these are indeed the two distinct irreducible 1-dimensional complex representations of S_3 (irreducible because the $\mathbb{C}[G]$ being 1-dimensional $\mathbb{C}$-VS $\implies$ any proper sub-$\mathbb{C}$-module (i.e. sub-$\mathbb{C}$-VS) must be dimension 0, i.e. trivial).

For the sole remaining 2-dimensional irreducible complex representation, **Problem 3** below gives us an irreducible (and faithful! but not necessary here) 2-dimensional complex representation of D_n for $n \geq 3$, but $D_3 = S_3$, generated by

$$r = (123) \mapsto \begin{bmatrix} \cos(\frac{2\pi}{3}) & -\sin(\frac{2\pi}{3}) \\ \sin(\frac{2\pi}{3}) & \cos(\frac{2\pi}{3}) \end{bmatrix}, \quad s = (12) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

and so we have found explicitly the three (two 1-dim, one 2-dim) irreducible complex representations of S_3.

Problem 2

For this problem, $G = Q$ the quaternion group (with 8 elements), and we are asked to find all the irreducible complex representations of G. Q has five conjugacy classes: $\{1\}$, $\{-1\}$, $\{i,-i\}$, $\{j,-j\}$, $\{k,-k\}$. Thus, by (iv) of the above cited Theorem 3.2 (see Problem 1 above), $r = 5$, and as n_i $(i \in [r])$ are positive integers whose squares sum to $|Q| = 8$ by Thm3.2(iii), they must be $1, 1, 1, 1, 2$ ($3^2 = 9$ is too big, and $1^2 + 1^2 + 1^2 + 2^2 + 2^2 = 3 + 4 + 4 = 11$ is too big, leaving just $1^2 + 1^2 + 1^2 + 1^2 + 2^2 = 8$).

Because irreducible (complex) representations are in 1-1 correspondence with the simple modules (up to isomorphism) of $\mathbb{C}[G]$, and Thm3.2(ii) tells us that there are exactly 5 distinct isomorphism classes of simple modules of $\mathbb{C}[G]$, with dimensions $1, 1, 1, 1, 2$ (when thought of as $\mathbb{C}$ vector spaces), we have exactly 5 irreducible complex representations of Q, four of which are of the form $Q \to \mathrm{GL}(1, \mathbb{C}) = \mathbb{C}^\times$, and one of which is of the form $Q \to \mathrm{GL}(2, \mathbb{C})$.

As before in Problem 1, we tackle the 1-dimensional representations first. Suppose we have a group homomorphism $\varrho : Q \to \mathbb{C}^\times$ (thinking of Q as $\{\pm 1, \pm i, \pm j, \pm k\}$ with $i^2 = j^2 = k^2 = ijk = -1$, where cancellation gives $ijk = k^2 \implies ij = k$, $ijk = i^2 \implies jk = i \implies jki = -1 = j^2 \implies ki = j$, and $ji = (-1)(jk)(ki) = -ij$, etc.). Because group homomorphisms preserve the identity, we must have that $\varrho(1) = 1$, implying $\varrho(-1)^2 = \varrho(1) = 1 \implies \varrho(-1) = \pm 1$. But recall $ij = -ji$, and because $\mathbb{C}^\times$ is commutative, it must be that $\varrho(-1) = 1$. Then, $\varrho(i)^2 = \varrho(j)^2 = \varrho(-1) = 1 \implies \varrho(i), \varrho(j) \in \{\pm 1\}$. As $k = ij \implies \varrho(k) = \varrho(i)\varrho(j)$ and $\varrho(-g) = \varrho(-1)\varrho(g) = \varrho(g)$ for any $g \in G = Q$, determining ϱ for i, j fixes everything, so we have ≤ 4 possibilities for a 1-dimension representation $Q \to \mathbb{C}^\times$: $\varrho(i) = \pm i, \varrho(i) = \pm 1$. We know from the previous paragraph that there are EXACTLY FOUR 1-dimensional (hence irreducible) representations $Q \to \mathbb{C}^\times$, so indeed these 4 possibilities are realized/are actually well-defined group homomorphisms.

Now to the sole remaining 2-dimensional irreducible representation $\varrho : Q \to \mathrm{GL}(2, \mathbb{C})$. To make ϱ a group homomorphism, we obviously must have $\varrho(1) = I_2$, but also denoting by A, B, C the images via ϱ of i, j, k respectively, the matrices A, B, C must satisfy the same identities as i, j, k (such as $i^2 = j^2 = k^2 = ijk = -1$). The most natural first idea would be to try $\varrho(-1) = -I_2$ and see where that takes us. The following matrices do satisfy $A^2 = B^2 = C^2 = ABC = -I_2$, as can be checked by straightforward, if tedious calculation by hand, or by WolframAlpha:

$$\varrho(i) = A := \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad \varrho(j) = B := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \varrho(k) = C := \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

This is indeed a valid 2-dimensional representation $\varrho : Q \to \mathrm{GL}(2, \mathbb{C}) = \mathrm{GL}_{\mathbb{C}}(V)$ where as a vector space $V = \mathbb{C}^2$, but we have yet to prove that it is irreducible. Recall (from Lec 24, or see the first page of this HW) that ϱ is irreducible exactly when V has no non-trivial proper sub-$\mathbb{C}$-VS W that is G-invariant, i.e. $[\varrho(g)](w) \in W$ for all $g \in G, w \in W$. Because W is a non-trivial proper $\mathbb{C}$ vector subspace of $V = \mathbb{C}^2$, it must have dimension $= 1$, given it contains $w \neq 0$, it must be $W = \mathbb{C}w$. To satisfy G-invariance, it must satisfy $Aw, Bw, Cw \in W = \mathbb{C}w$ for our above A, B, C. In other words, w must be an eigenvector of A, B, and C.

We can therefore check that the above ϱ is indeed irreducible very easily, by finding the eigenvectors of in particular A and B and seeing that they are not equal. The eigenvectors of A are $\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$, while the eigenvectors of B are $\left[\begin{smallmatrix}-i\\1\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix}i\\1\end{smallmatrix}\right]$, and so A and B do not have any eigenvectors in common, and so there does NOT exist any such W, meaning ϱ is irreducible as desired.

Problem 3

We find an explicit faithful irreducible complex 2-dimensional representation $\varrho : G \to \mathrm{GL}(2,\mathbb{C})$ of the dihedral group $G = D_n$ (which has $2n$ elements $\{1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$ for a rotation r and flip s, which satisfy $r^k s = sr^{-k}$ (can be proven by induction from just $rs = sr^{-1}$), $r^n = s^2 = 1$) for $n \geq 3$. Like at the end of Problem 2, we try to find matrices $R, S \in \mathrm{GL}(2,\mathbb{C})$ that satisfy the relations that $r, s \in D_n$ satisfy. Defining

$$\varrho(r) = R := \begin{bmatrix} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{bmatrix}, \quad \varrho(s) = S := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

One (or WolframAlpha) can then check that (obviously) $R^n = S^2 = \mathrm{Id}_2$, and (less obviously):

$$R^k = \begin{bmatrix} \cos(\frac{2\pi k}{n}) & -\sin(\frac{2\pi k}{n}) \\ \sin(\frac{2\pi k}{n}) & \cos(\frac{2\pi k}{n}) \end{bmatrix}, \quad RSR = \begin{bmatrix} \cos(\frac{2\pi k}{n}) & \sin(\frac{2\pi k}{n}) \\ \sin(\frac{2\pi k}{n}) & -\cos(\frac{2\pi k}{n}) \end{bmatrix} R = S.$$

Note that R, S satisfy all the relations $r, s \in D_n$ do (hence ϱ is group homomorphism), and moreover R^k are distinct from each other for $k \in \{0, \ldots, n-1\}$ (with determinant 1), implying that all the SR^k are distinct from each other for $k \in \{0, \ldots, n-1\}$ (with determinant $\det(S) \cdot \det(R)^k = -1$) since if not we can just multiply on the left by $S^{-1} = S$ and get a contradiction $R^{k_1} = R^{k_2}$ for non-equal $k_1, k_2 \in \{0, \ldots, n-1\}$. That is to say, $\{R^0, \ldots, R^{n-1}, SR^0, \ldots, SR^{n-1}\}$ are $2n$ distinct matrices, so ϱ is in fact an INJECTIVE group homomorphism, which is exactly what it means for ϱ to be a faithful representation.

Finally, we show that ϱ is irreducible. As we saw at the end of Problem 2 above, if R, S do not share any eigenvectors, then there can not be any non-trivial proper G-invariant subspaces W of $V = \mathbb{C}^2$, implying that ϱ is irreducible. Thus, it suffices to find the eigenvectors of R, S and see that they do not share any eigenvectors. Well, the eigenvectors of R are $\left[\begin{smallmatrix}-i\\1\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix}i\\1\end{smallmatrix}\right]$, and the eigenvectors of S are $\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$, so indeed R and S do not share any eigenvectors and hence ϱ is indeed a faithful irreducible complex 2-dimensional representation of D_n.

Problem 4

Let G be a finite group with $\varrho : G \to \mathrm{GL}(V)$ a finite dimensional complex representation (say $\mathrm{GL}(V) = \mathrm{GL}(d,\mathbb{C})$ where d is one of the $n_1, \ldots, n_r$ from Thm. 3.2, which I copied in Problem 1 above), and $g \in G$ be arbitrary. We want to prove that $\mathrm{tr}\, \varrho(g)$ (the trace of an $d \times d$ matrix) is a sum of roots of unity.

Def. 3.6 in Lec 26 says that for a representation $\varrho : G \to \mathrm{GL}_k(V)$, we can define the character $\chi := \operatorname{tr} \varrho : G \to k$. This problem asks us to prove that $\chi(g)$ (the trace of the matrix $\varrho(g)$) is a sum of roots of unity. Do note that we proved this in class, in Prop. 3.20(ii) in Lec 27 on 6/4/21. However, I provide an alternate (albeit quite similar) proof.

Recall from linear algebra that the trace of a matrix equals the sum of its eigenvalues: the eigenvalues are exactly the zeroes of the characteristic polynomial $p(t) \det(A - tI) = (-1)^n t^n \pm (\operatorname{tr} A)t^{n-1} \pm \ldots \pm \det A$, where the coefficient of t^{n-1} is $\pm \operatorname{tr} A$ because any t^{n-1} term must come from $(a_{11} - t) \cdots (a_{nn} - t)$ (since each term of the determinant is a product of n numbers, one from each row/column, and any $n - 1$ size collection of t leaves the only available spot on the diagonal) yielding the coefficient is $\pm(a_{11} + \ldots + a_{nn}) = \pm \operatorname{tr} A$, and where I write "$\pm$" to indicate it's either plus or minus, but I just don't want to figure out how many power of (-1) there are flying around; but also $p(t) = (-1)^n (t - \lambda_1) \cdots (t - \lambda_n)$ where λ_i, $i \in [n]$, are the eigenvalues of A, and of course the coefficient of the t^{n-1} term in this expression is the sum of the eigenvalues.

So suppose λ is an eigenvalue of $\varrho(g)$, where $g^m = 1$ (there is such an $m \in \mathbb{N}$ because G is finite group). Then, for the corresponding eigenvector v, $\varrho(g^m)v = \varrho(1)v = \mathrm{Id}(v) = v$, but $\varrho(g^m)v = \varrho(g)^m v = \lambda^m v$, implying that $\lambda^m v = v \implies \lambda^m = 1 \implies \lambda$ is a root of unity. Thus, all eigenvalues of $\varrho(g)$ are roots of unity, so $\operatorname{tr} \varrho(g)$ being the sum of eigenvalues $\implies \operatorname{tr} \varrho(g)$ is a sum of roots of unity.

Problem 5 (sketch)

Let G be a finite group that admits a faithful irreducible complex representation $\varrho : G \to \mathrm{GL}(n, \mathbb{C})$. We want to show that $Z(G)$ is cyclic. Schur's lemma (Theorem 2.10 in Lec 19) in context of vector space of algebraically closed field give that only module homomorphisms $V \to V$ (thinking of V as $\mathbb{C}[G]$-module) are scalar multiplication. Of course, this include $v \mapsto \varrho(z)v$ for any $z \in Z(G)$, so all $\varrho(z)$ are scalar multiplication matrices. So $\varrho : G \to \mathbb{C}^\times$ induces image of $Z(G)$ via ϱ in $\mathbb{C}^\times$, but G finite $\implies Z(G)$ finite and finite subgroups of the multiplicative group of a field are cyclic, so $\operatorname{im} Z(G)$ is cyclic. But ϱ faithful $\implies$ injective, so by 1st iso thm $Z(G) \simeq \operatorname{im} Z(G)$ so $Z(G)$ is also cyclic.

Problem 6

Let G be a finite group generated by two elements $x, y \in G$ and the relations $x^3 = y^2 = (xy)^2 = 1$. First note that given just the relations $x^3 = y^2 = 1$, we would have words $x^{0,1,2}y^1x^{1,2}y^1 \cdots x^{1,2}y^1x^{0,1,2}$. With the added condition $(xy)^2 = xyxy = 1 \implies xyx = y \implies xy = yx^2$, we can move any x's on the left all the way to the right, yielding words of the form $y^{0,1}x^{0,1,2}$. Thus, we have ≤ 6 distinct words given these relations. Then, because D_3 satisfies these relations (take $x \in G$ to be $r \in D_3$ and $y \in G$ to be $s \in D_3$), this shows that these relations do not FORCE any of the 6 possibly distinct words to be equal, and so $\varphi : D_3 \to G$ defined by $r \mapsto x, s \mapsto y$ is an injective and surjective homomorphism, so $G \simeq D_3 \simeq S_3$. Thus, all the irreducible complex representations of G are just those of S_3, which we found above in Problem 1.

506 Homework 7

Daniel Rui - 5/28/21

In the following problems, R will denote a not-necessarily commutative ring with unity.

Problem 1

Suppose that R is a simple ring (i.e. it does not have non-trivial two-sided ideals; this is NOT saying that R is a simple module!). We want to show that $M_n(R)$ is as well. Furthermore if D is a division ring, we want to prove that $M_n(D)$ is a simple ring (NOT simple module!) which is both Artinian and Noetherian (as a left module over itself).

Recall **Problem 6** of Homework 6, which claimed that for any two-sided ideal $I \lhd M_n(R)$, there must exist a unique (two-sided) ideal $J \lhd R$ s.t. $I = M_n(J)$. Thus, if $M_n(R)$ were not a simple ring, then it would have a non-trivial two-sided ideal I, meaning by the cited HW6p6, there is a non-trivial two-sided ideal $J \lhd R$, which can not happen.

Now for the second part. First note that if D is a division ring, then it must be simple, because if $I \lhd D$ is a non-trivial two-sided ideal and non-zero $x \in I \subseteq D$, then because D is a division ring there is $y \in D$ s.t. $yx = 1$, meaning that because I is closed under (left or right in this case, since two-sided) multiplication by elements of D, $1 = yx \in I \implies I = D$. Thus, D is indeed simple. As for being both Artinian and Noetherian, we know from Theorem 2.19 in Lec 19 that an R-module M admits a composition series (i.e. Def. 2.14 in Lec 19: sequence of submodules $0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_r = M$ s.t. all quotients M_i/M_{i-1} are simple modules) if and only if M is both Artinian and Noetherian, and from Prop. 2.24 in Lec 21 that for a semisimple module M, M has a composition series if and only if it is a finite direct sum of simple modules. Well, Problem 2 below tells us that $M_n(D)$ is indeed a semisimple ring that is the finite direct sum of simple modules, and so we are done.

Problem 2 - SKETCH, NO NEED TO GRADE

Let D be a division ring and $M_n(D)$ be the ring of $n \times n$ matrices with entries in D. We want to determine all the left ideals, in particular the MINIMAL left ideals, of $M_n(D)$, and use this to prove that $M_n(D) \simeq V_1 \oplus \ldots \oplus V_n$ (where V_i is a minimal left ideal of $M_n(D)$ for $i \in [n]$, and $V_i \simeq V_j$ as left $M_n(D)$-modules for all $i, j \in [n]$). With this result, we conclude that $M_n(D)$ is a semisimple ring, and that there exists a UNIQUE simple $M_n(D)$-module (V, isomorphic to the V_i, i.e. isomorphic to the set of "vectors"/n-tuples D^n) — in fact $M_n(D)$ is V-isotypic of order n.

For Problem 1 above, we only need to show that $M_n(D) \simeq V_1 \oplus \ldots \oplus V_n$ for simple V_i, $i \in [n]$. Define V_i to consist of matrices with arbitrary ith column and zeroes in all other columns. Can check that each V_i is a left ideal of $M_n(D)$ by quick computation using matrix multiplication, and obviously $V_i \simeq D^n$. Obviously $M_n(D) = V_1 + \ldots + V_n$, and they are all independent/trivial overlap between any disjoint collections, i.e. $\sum_{i \in I} V_i \cap \sum_{j \in J} V_j = \{0\}$ when $I \cap J = \varnothing$, implying indeed that $M_n(D) \simeq V_1 \oplus \ldots \oplus V_n$.

Lastly, each V_i is simple $M_n(D)$-module because $V_i := M_n(D)e_i$ where e_i is the vector with 1 in ith component and zeroes elsewhere, and Prop. 2.12 in Lec 19 tells us that M is simple R-module $\iff$ $M = Rx$ for any $0 \neq x \in M$ (for any $0 \neq x \in V_i$, there is matrix in $A \in M_n(D)$ s.t. $Ax = e_i$; namely if $x = [d_1 \ \dots \ d_n]^\top$, and $d_j \neq 0$, let A be matrix all zeroes except d_j^{-1} in (i, j)th spot).

Problem 3

Let D be a division ring and $M_n(D)$ again be the ring of $n \times n$ matrices with entries in D, and let V denote the unique simple $M_n(D)$-module found in Problem 2 above. We want to prove that $\mathrm{End}_{M_n(D)}(V) \simeq D^{\mathrm{op}}$ as rings. Define a map $\Phi : D^{\mathrm{op}} \to \mathrm{End}_{M_n(D)}(V)$ by $d^{\mathrm{op}} \mapsto \varphi_d$ where φ_d (a module homomorphism $V \to V$, thinking of V as a $M_n(D)$-module) is defined by $x \mapsto xd$ (from Problem 2, we know that we can think of V as a left ideal of $M_n(D)$, and any element of $M_n(D)$ has valid left and right multiplication by elements of D). Recall from class or my MSE question that Sándor answered that defining φ_d by right multiplication is necessary to make it an endomorphism $V \to V$, and that Φ is a ring homomorphism.

Note first that Φ is injective, because $d_1 x = d_2 x \implies (d_1 - d_2)x = 0$, but thinking of $x \in V \subseteq M_n(D)$ (again from Problem 2, a left ideal of $M_n(D)$), we see that $(d_1 - d_2)x = 0 \implies x = 0_{M_n(D)}$ or $d_1 = d_2$; the first possibility is not the case because $\varphi_{d_1} = \varphi_{d_2} \iff d_1 x = d_2 x$ for all $x \in V$, so indeed we are left with $d_1 = d_2$ (perhaps it'd be simpler if I had just said "think of V as D^n" at the beginning, but oh well). We move onto surjectivity.

Let $\varphi \in \mathrm{End}_{M_n(D)} V$ be arbitrary, where we are thinking of V as the set of vectors/n-tuples D^n, which can obviously be acted upon by $M_n(D)$ from the left so that V is a left $M_n(D)$-module. Let e_i denote the vector with ith component 1 and all other components 0; it is clear that $\{e_i\}_{i=1}^n$ is a linearly independent spanning set of $V = D^n$. Any element $x \in V$ can be written as $x = Ae_1$, for some matrix $A \in M_n(D)$ (e.g. take the matrix $A \in M_n(D)$ with first column equal to the vector $x \in V = D^n$ and all other columns 0), and so $\varphi(x) = \varphi(Ae_1) = A\varphi(e_1)$. Say $\varphi(e_1)$ is some vector with first component equal to $d_1 \in D$; then because A only has first column non-zero, $A\varphi(e_1)$ is a vector equal to d_1 times the first column of A, i.e. $d_1 x = x d_1$. We conclude that $\varphi(x) = x d_1$ for all $x \in V$, i.e. $\varphi = \varphi_{d_1}$, so indeed Φ is surjective.

Remarks: we use the notation $E_{ij} \in M_n(D)$ to denote the $n \times n$ matrix with the (i, j)th entry 1 and all the other entries 0 (we've actually used this notation before, in 504HW6p3). We could have written the above prove in a shorter and perhaps clearer way as follows: $\varphi(x) = \varphi(Ae_1) = \varphi(AE_{11}e_1) = AE_{11}\varphi(e_1) = AE_{11}[d_1 \ \dots \ d_n]^\top = A[d_1 \ 0 \ \dots \ 0]^\top = d_1(Ae_1) = xd_1$ (with this proof, we don't even need to specify A, we just need the property that $x = Ae_1$).

Problem 4

Let N be a simple R-module and $M = \bigoplus_{\lambda \in \Lambda} N$ and $M' = \bigoplus_{\lambda' \in \Lambda'} N$ be two N-isotypic semisimple modules, with at least one of Λ, Λ' is finite. We want to show that $M \simeq M'$ if and only if $|\Lambda| = |\Lambda'|$.

($\Longleftarrow$): supposing $|\Lambda| = n < \infty$, we have that $|\Lambda'| = n$ as well. Then, $M = \bigoplus_{\lambda \in \Lambda} N \simeq \bigoplus_{i=1}^n N$ and $M' = \bigoplus_{\lambda' \in \Lambda'} N \simeq \bigoplus_{i=1}^n N$, where the RHS of both expressions are clearly equal.

($\Longrightarrow$): supposing $|\Lambda| = n < \infty$, we have $M = \bigoplus_{\lambda \in \Lambda} N \simeq \bigoplus_{i=1}^n N$. Denote $\varphi : M \to M'$ to be some R-module isomorphism between M and $M' = \bigoplus_{\lambda' \in \Lambda'} N$. I claim that Λ' can not possibly be infinite in cardinality. We proceed by contradiction — suppose Λ' was infinite in cardinality. Supposing have a linearly independent spanning set $\{x_1, \ldots, x_n\}$ in M (e.g. x_i is the tuple with 1 in the ith coordinate and 0 elsewhere), the set $\{\varphi(x_1), \ldots, \varphi(x_n)\}$ is a spanning set of M' (by the surjectivity of φ: $y \in M'$ equals $\varphi(x)$ for some $x \in M$, which equals $\sum_{i=1}^n a_i x_i$, and so by R-linearity of φ, $\sum_{i=1}^n a_i \varphi(x_i) = \varphi(x) = y$), and is linearly independent (by the injectivity of φ: $\sum_{i=1}^n a_i \varphi(x_i) = 0 \iff \varphi(\sum_{i=1}^n a_i x_i) = 0 \iff \sum_{i=1}^n a_i x_i = 0 \iff a_i = 0$ for all $i \in [n]$). But because $\varphi(x_i) \in M'$ is a tuple with all but finitely many elements 0 (say all coordinates $\geq \#_i \in \mathbb{N}$ are 0, where we are assuming a well-ordering of Λ' by the Axiom of Choice), then taking $\#$ to be $\max_{i \in [n]}\{\#_i\}$, any linear combinations of the $\{\varphi(x_i)\}_{i=1}^n$ must have all coordinates $\geq \#$ 0, meaning that $\{\varphi(x_i)\}_{i=1}^n$ can not possibly span M'.

Now that we know that both Λ, Λ' have finite cardinality (denoted n and m respectively), we show that $M \simeq \bigoplus_{i=1}^n N \not\simeq \bigoplus_{i=1}^m N$ for $m \neq n$. We know from Proposition 2.24 that a semisimple module has a composition series if and only if it is a finite direct sum of simple modules; if it is the direct sum of r simple modules, then we say that the length of M is r, and it admits a composition series $0 = N_0 \subseteq N_1 \subseteq \ldots \subseteq N_{r-1} \subseteq N_r = M$. Jordan-Hölder (i.e. Homework 2.15 in Lec 19) tells us that any two composition series have the same length. Thus, going back to our problem, we see that if $n \neq m$, then because $M' \simeq \bigoplus_{i=1}^n N$ and $M' \simeq \bigoplus_{i=1}^m N$, we can form two composition series of length n and m, contradicting that all composition series have the same length.

Problem 5

Let k be an algebraically closed field, contained in the center of a division ring D. Suppose further that as a vector space, D is finite dimensional over k (say dimension n). We want to show that $D = k$. Well, let x be some arbitrary element of D. Because D is a ring with $k \subseteq D$ and $x \in D$, $k[x]$ (which recall has elements $\{a_n x^n + \ldots + a_0 : a_i \in k\}$) is a subring of D, and because k is contained in the center of D (i.e. for any $d \in D$ and $c \in k$, $cd = dc$, or equivalently, in any product, one may move the elements of k around willy-nilly), $k[x]$ is moreover commutative. Because D as a vector space has dimension $n \in \mathbb{N}$ over k, it must be that $\{x, x^2, x^3, \ldots, x^{n+1}\}$ (all elements of D) can not form a linearly independent set (because for vector spaces, size of LI set $\leq$ size of LI and spanning set $=$ size of basis $=$ dimension), meaning that $x^{n+1} = a_n x^n + \ldots + a_0$ for some $a_i \in k$.

Moreover note that if $a_0 = 0$, then we can move everything to the LHS and factor out however many x's we need until we get some power of x's times some polynomial with non-zero constant term, and because division rings do not have zero divisors, we either have that x is the root of a polynomial with non-zero constant term, or $x = 0$. In other words, we now see that either $x = 0$, or x is the root of a polynomial with non-zero constant term, say $x^{n+1} - a_n x^n - \ldots - a_0 = 0$ for $a_0 \neq 0$.

Thus, supposing that $x \neq 0$, the inverse of x (which we know exists in D because D is a division ring) is in $k[x]$ because $x \cdot \frac{1}{a_0}(x^n - a_n x^{n-1} - \ldots - a_1) = 1$. Thus, $k[x]$ is a commutative subring of D where every non-zero element is a unit, meaning that $k[x]$ is a field. But then we have that $k[x]$ is a finite (hence algebraic) field extension of the algebraically closed k, and therefore $k[x]$ must equal k, implying that $x \in k$. But $x \in D$ was chosen arbitrarily, so indeed $D = k$.

Problem 6

Let M be an R-module and $N \subseteq M$ a submodule. We want to prove that there exists a submodule $N' \subseteq M$ s.t. $M = N \oplus N'$ if and only if there exists a (module) homomorphism $\pi : M \to N$ s.t. $\pi|_N = \mathrm{id}_N$.

($\implies$): define $\varphi : M \to N$ by $n + n' \mapsto n$. It is well defined because $M = N \oplus N' \iff M = N + N'$ and $N \cap N' = \{0\}$ means that every $m \in M$ can be uniquely written as $n + n'$ for some $n \in N, n' \in N'$ (unique because if not, we would get $n_1 + n_1' = n_2 + n_2'$ and writing n's on one side and n''s on the other side we get a non-zero element in $N \cap N'$). It is also a module homomorphism because $\varphi(m_1 + m_2) = n_1 + n_2 = \varphi(m_1) + \varphi(m_2)$ and $\varphi(rm) = \varphi(r(n + n')) = \varphi(rn + rn') = rn = r\varphi(m)$, and obviously for all $n \in N$, $\varphi(n) = n$.

($\impliedby$): so there exists $\pi : M \to N$, a module homomorphism. I claim that taking $N' := \ker \pi$, we have that $M = N + N'$ and $N \cap N'$ (which again as I stated in the ($\implies$) direction above is $\iff M = N \oplus N'$). Recall that since π is surjective, the 1st isomorphism theorem gives that $M/\ker \pi \simeq N$, i.e. all $m \in M$ are in some coset $n + \ker \pi$, i.e. there is some $n \in N$, $n' \in N' = \ker \pi$ s.t. $m = n + n'$, implying that $M = N + N'$. To show that the intersection is trivial, suppose we had $x \in N \cap \ker \pi$. Then, we know that $x \in \ker \pi \implies \pi(x) = 0$, but also $x \in N \implies \pi(x) = x$. Therefore, $x = 0$, and so indeed the only element of $\ker \pi \cap N$ is 0. ■

506 Homework 6

Daniel Rui - 5/19/21

In the following problems, R will denote a not-necessarily commutative ring with unity.

Problem 1

(a) Let $x \in R$ be left-invertible, i.e. there is $y \in R$ s.t. $yx = 1$ (but not necessarily $xy = 1$!). We want to show that if y is also left-invertible, then x, y are units. This allows us to conclude that if R is s.t. every non-zero element is left-invertible, then R is a division ring (we just proved that all left-invertible elements with their left inverse also left-invertible are units, but from the assumption on R that every non-zero element is left-invertible, we see that all non-zero elements are units).

Ok, so we have $yx = 1$ and also because y is left-invertible, $zy = 1$ for some $z \in R$ (note that all x, y, z are non-zero because 0 times anything is 0, not 1). Then, $x = 1 \cdot x = zyx = z \cdot 1 = z$. Thus, x, y are each other's multiplicative (both left and right) identities, and hence are units.

(b) Assuming that $1 - ab \in R$ is left-invertible, we want to prove that $1 - ba$ is also left-invertible by constructing an explicit inverse of $1 - ba$ using the (left-)inverse of $1 - ab$, which we'll call c (i.e. $c(1 - ab) = c - cab = 1$). I'll give away the answer now and talk a bit about where such a "miraculous" computation comes from. Let us verify that $(1 + bca)$ is the left-inverse of $1 - ba$:

$$\begin{aligned}(1 + bca)(1 - ba) &= 1 + bca - ba - bcaba \\ &= 1 + bca - ba - b(c - 1)a \\ &= 1 + bca - ba - bca + ba = 1.\end{aligned}$$

As for where this number comes from, note that the above formula $c - cab = 1 \iff c = 1 + cab$ can be substituted into itself over and over again, yielding $c = 1 + (1 + cab)ab = 1 + ab + c(ab)^2$, and $c = 1 + ab + (ab)^2 + c(ab)^3$, and so on. This is reminiscent of the "geometric series" formula from analysis regarding the inverse $\frac{1}{1-x} = 1 + x + x^2 + \ldots$ of $1 - x$ for $x \in B(0, 1)$ (in both $\mathbb{R}$ or $\mathbb{C}$). Thus, if one throws rigor to the wind and writes $c = 1 + ab + (ab)^2 + \ldots$ (and similarly $(1 - ba)^{-1} = 1 + ba + (ba)^2 + \ldots$), then $bca = ba + baba + (ba)^3 + \ldots$, yielding $(1 - ba)^{-1} = 1 + ba + (ba)^2 + \ldots = 1 + bca$. Then of course one has to check that indeed this is the left-inverse, which we already did above.

Later remarks: turns out this is a well known puzzle, see this Math Overflow thread. In it, user Victor Protsak describes a way to make this "power series" technique rigorous: consider the ring $R((\lambda))$ of formal Laurent series in the variable λ (i.e. formal series $\sum_{n=-\infty}^{\infty} a_n \lambda^n$). Then, (where $\cdot^{-1}$ denotes left-inverse, and also λ commutes with all elements) we have $(\lambda - ba)^{-1} = \sum_{n=0}^{\infty} \lambda^{-(n+1)}(ba)^n$ because formally $(\sum_{n=0}^{\infty} \lambda^{-(n+1)}(ba)^n)(\lambda - ba) = \sum_{n=0}^{\infty} \lambda^{-n}(ba)^n -$

$\sum_{n=0}^{\infty} \lambda^{-(n+1)}(ba)^{n+1} = \lambda^{-0}(ba)^0 = 1$, but also

$$\begin{aligned}(\lambda - ba)^{-1} &= \sum_{n=0}^{\infty} \lambda^{-(n+1)}(ba)^n = \lambda^{-1} + \sum_{n=1}^{\infty} \lambda^{-(n+1)} b(ab)^{n-1}a \\ &= \lambda^{-1}\left(1 + b\left(\sum_{n=1}^{\infty} \lambda^{-n}(ab)^{n-1}\right)a\right) = \lambda^{-1}(1 + b(\lambda - ab)^{-1}a).\end{aligned}$$

This is true in $R((\lambda))$, so defining $\varphi : R((\lambda)) \to R$ by $r \mapsto r$, and $\lambda, \lambda^{-1} \mapsto 1$, we get that $(1-ba)^{-1} = \varphi(\lambda - ba)^{-1} = \varphi((\lambda - ba)^{-1}) = \varphi(\lambda^{-1}(1 + b(\lambda - ab)^{-1}a)) = 1 \cdot (1 + b(1-ab)^{-1}a)$, where the 2nd equality comes from the fact that for any ring homomorphism $\phi : R \to S$ that sends $1_R \mapsto 1_S$, we have $r'r = 1 \implies \phi(r')\phi(r) = 1$, i.e. the left inverse of r gets sent to the left inverse of $\phi(r)$.

Problem 2

We define the *Jacobson radical* $J(R)$ of R to be the intersection of all maximal left ideals of R.

(a) We want to prove that for each $x \in R, x \in J(R) \iff 1 - yx$ is left-invertible for EACH $y \in R$.

($\Longleftarrow$): suppose $x \in R$ s.t. for all $y \in R$, $1 - yx$ is left-invertible. To show $x \in J(R)$, we want to show that $x \in \mathfrak{m}$ for all left ideals $\mathfrak{m} \triangleleft R$. Well, suppose that $x \notin \mathfrak{m}$ for some left ideal $\mathfrak{m} \triangleleft R$. Then, $(x) + \mathfrak{m}$ is an ideal that strictly contains $\mathfrak{m}$, and so by maximality of $\mathfrak{m}$, it must be that $(x) + \mathfrak{m} = R$. But then there is $y \in R, m \in \mathfrak{m}$ s.t. $y \cdot x + m = 1 \iff 1 - yx = m \in \mathfrak{m}$, but this is impossible because if it were, we could multiply by the left-inverse to get that $1 \in \mathfrak{m}$.

($\Longrightarrow$): if $x \in J(R)$ and there is $y \in R$ s.t. $1 - yx$ is not left-invertible, then obviously $1 - yx$ is not a unit of R, and hence there is a maximal left ideal $\mathfrak{m}$ containing it. But because $J(R) \subseteq \mathfrak{m}$, the element x is also in $\mathfrak{m}$, so $1 = (1 - yx) + y \cdot x \in \mathfrak{m}$; contradiction (note that here is where we need the order to be exactly "yx", since $y \in R$ and $\mathfrak{m}$ is a left ideal — if instead we were considering right ideals, the statement would be true if we considered left-invertible elements $(1 - xy)$ for $y \in R$ instead).

(b) We want to show that $J(R)$ is equal to the intersection of all maximal RIGHT ideals of R. Looking at the above argument (in fact in the last statement in the parentheses that I wrote in part (a)) it is clear that $x \in R$ is in the intersection of all RIGHT ideals if and only if $1 - xy$ is left-invertible for all $y \in R$. Well, we know from Problem 1(b) that $1 - xy$ left-invertible $\iff 1 - yx$ left-invertible, so indeed x in the intersection of maximal right ideals $\iff 1 - xy$ left-invertible for all $y \in R \iff 1 - yx$ left-invertible for all $y \in R \iff x$ in the intersection of maximal left ideals.

(c) And finally we want to prove that $J(R)$ is a two-sided ideal. Because $J(R)$ is the intersection of maximal LEFT ideals, it is left ideal, and because $J(R)$ is the intersection of maximal RIGHT ideals, it is also right ideal.

Problem 3

We want to prove that R that the following are equivalent:

(i) R has a unique maximal left ideal

(ii) R has a unique maximal right ideal

(iii) $R/J(R)$ is a division ring

Furthermore, if one (equiv. all) of these conditions is satisfied, we call R a *local ring* (recall we only defined local ring for commutative rings with unity), then the unique maximal left ideal equals the unique maximal right ideal (equals $J(R)$!).

Suppose (i) holds. Then, since $J(R)$ (see Problem 2) is the intersection of all maximal left ideals of R, the unique maximal left ideal must be exactly $J(R)$. We now prove that $J(R)$ is a maximal right ideal (implying it must be the unique maximal right ideal, because we know $J(R)$ is the intersection of all right ideals, and a maximal ideal containing another maximal ideal must in fact be an equality). We already know from Problem 2(c) that $J(R)$ is a right ideal, so we just need to prove maximality. Well suppose we have a larger right ideal $\mathfrak{m} \supsetneq J(R)$. By Problem 2(a), there is $x \in \mathfrak{m}$ s.t. there is some $y \in R$ s.t. $1-yx$ is not left-invertible; $1-xy$ is also not left-invertible by Problem 1(b). Let us now define $I := \{r(1-xy) : r \in R\}$. Then, I is clearly a proper left ideal of R, and because $J(R)$ is the unique maximal left ideal, $I \subseteq J(R)$, and so again by Problem 2(a), we have that $1_R(1-xy) \in I \subseteq J(R) \subsetneq \mathfrak{m}$. Because $x \in \mathfrak{m}$ and $\mathfrak{m}$ is a right ideal, $xy \in \mathfrak{m}$, and so $1 = (1-xy) + xy \in \mathfrak{m}$, meaning $\mathfrak{m} = R$, proving that indeed $J(R)$ is a maximal right ideal.

The above shows (i) $\implies$ (ii). The implication (ii) $\implies$ (i) follows practically by symmetry; just swap "left" and "right" (though "left-invertible" remains "left-invertible"), and use $(1-yx)$ instead of $(1-xy)$ to define I. We now show that $\mathfrak{m} \triangleleft R$ is a maximal left ideal if and only if $R/\mathfrak{m}$ is a division ring. ($\implies$): we want to prove that every non-zero element $x + \mathfrak{m} \in R/\mathfrak{m}$ has a (double sided) inverse, but recall from Problem 1(a) that it suffices to show that every non-zero element $x + \mathfrak{m}$ has a left-inverse. Well, $x + \mathfrak{m} \neq 0_{R/\mathfrak{m}} \iff x \notin \mathfrak{m}$, meaning that we can define the left ideal $\mathfrak{m} + Rx$ which strictly contains $\mathfrak{m}$. By the maximality of $\mathfrak{m}$, it must be that $\mathfrak{m} + Rx = R$, i.e. there is $m \in \mathfrak{m}, r \in R$ s.t. $m + rx = 1_R$, implying $rx + \mathfrak{m} = 1_R + \mathfrak{m} = 1_{R/\mathfrak{m}}$, i.e. $(r + \mathfrak{m})(x + \mathfrak{m}) = 1_{R/\mathfrak{m}}$. We have thus shown the existence of a left-inverse for every non-zero element $x + \mathfrak{m} \in R/\mathfrak{m}$, and we are done with this direction.

($\impliedby$): if $\mathfrak{m} \triangleleft R$ is s.t. $R/\mathfrak{m}$, to show that $\mathfrak{m}$ is maximal left ideal, it suffices to show that for any $x \in R \setminus \mathfrak{m}$, the left ideal $\mathfrak{m} + Rx = R$. Well, we know that for any $x \in R \setminus \mathfrak{m}$, $x + \mathfrak{m} \neq 0_{R/\mathfrak{m}}$, and so because $R/\mathfrak{m}$ is a division ring, there is a left inverse $r + \mathfrak{m}$ s.t. $rx + \mathfrak{m} = 1_R + \mathfrak{m} \implies rx + m = 1_R$ for some $m \in \mathfrak{m}$, implying that indeed $1_R \in \mathfrak{m} + Rx \implies \mathfrak{m} + Rx = R$, as desired.

This proposition shows that (i) $\implies$ (iii) because assuming (i), we have that $J(R)$ is the unique maximal left ideal, so $R/J(R)$ must a division ring; conversely assuming (iii) we have that $J(R)$ must be a maximal left ideal (implying it must be unique, because we know $J(R)$ is the intersection of all left ideals, and a maximal ideal containing another maximal ideal must in fact be an equality).

Lastly, we prove that in a local ring R, any element that has a left-inverse must be a unit. Suppose we have $x \in R$ s.t. $yx = 1$ for some $y \in R$. We want to show that $xy = 1$ as well. Well, $yx = 1 \implies yxy = y$, i.e. $y(1 - xy) = 0$. Let us define $I := \{r \in R : r(1 - xy) = 0\}$. It is clear that I is a left ideal of R. If it were a proper left ideal of R, then because $J(R)$ is the unique maximal left ideal, $I \subseteq J(R)$, but this is not possible because we know $y \in I$, and $y \notin J(R)$ because if it were, then because $J(R)$ is also a right ideal, $1 = yx \in J(R)$, which it is not. Thus, I must not be a proper left ideal of R, i.e. it must be R itself. But then $1_R \in I$, so $1_R(1 - xy) = 0 \iff 1 = xy$, as desired.

Problem 4

Let M be an R-module (more specifically a left R-module) and define its annihilator to be $\mathrm{Ann}(M) := \{x \in R : xM = 0\} \subseteq R$. We want to prove that $\mathrm{Ann}(M)$ is a two-sided ideal of R. That is, we want to show that $a, b \in \mathrm{Ann}(M) \implies a - b \in \mathrm{Ann}(M)$, and for any $r \in R, a \in \mathrm{Ann}(M)$, $ra \in \mathrm{Ann}(M)$ (left ideal) and $ar \in \mathrm{Ann}(M)$ (right ideal):

- "$-$" condition: by definition, we have for any $m \in M$ that $am = bm = 0$, so $(a - b)m = 0$ for all $m \in M$, meaning $a - b \in \mathrm{Ann}(M)$.
- left multiplication condition: well $(ra)m = r(am) = r \cdot 0_M = 0_M$ for all $m \in M$, so indeed $ra \in \mathrm{Ann}(M)$.
- right multiplication condition: for any $m \in M$ and $r \in R$, rm is just some element of M (by module properties), so $(ar)m = a(rm) \in aM = \{0_M\}$, so indeed $ar \in \mathrm{Ann}(M)$.

Problem 5

Let M be a semisimple R-module. We want to show that M Noetherian $\iff$ M Artinian. Recall from Definition 2.22/Proposition 2.21 from Lec 20 that M being a semisimple R-module means that $M = \bigoplus_{i \in I} S_i$ for a set of simple submodules $S_i \subseteq M$, $i \in I$ for some index set. Moreover, Theorem 2.19 of Lec 19 gives that an R-module M admits a composition series (i.e. Definition 2.14 in Lec 19: a sequence of submodules $0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_r = M$ s.t. all quotients M_i/M_{i-1} are simple modules) if and only if M is both Artinian and Noetherian. Proposition 2.24 of Lec 21 gives that a semisimple R-module M admits a composition series if and only if it is a finite direct sum of simple modules. Thus, to prove the claim of this problem, it suffices to show that $M = \bigoplus_{i \in I} S_i$ has I finite in the cases that M is Artinian or Noetherian.

We prove this by contradiction/contrapositive. If I was infinite (let us use the Axiom of Choice to give it a well-ordering), then $S_1 \subsetneq S_1 \oplus S_2 \subsetneq S_1 \oplus S_2 \oplus S_3 \subsetneq \ldots$ is an infinite non-plateauing ascending chain of submodules, and so M can not possibly be Noetherian. Similarly, defining N_1 to be the submodule of M s.t. the 1st coordinate is always 0, and N_2 to be the submodule of M s.t. the 1st and 2nd coordinates are always 0, and similarly N_n to be the submodule of M s.t. the first n coordinates are always 0, $M \supsetneq N_1 \supsetneq N_2 \supsetneq \ldots$ forms an infinite non-plateauing descending chain of submodules, implying that M can not possibly be Artinian.

Problem 6

Consider the ring of $n \times n$-matrices $M_n(R)$ with entries in R for $n > 0$. Let $I \triangleleft M_n(R)$ be a two-sided ideal. We want to prove that there is a unique ideal $J \triangleleft R$ s.t. $I = M_n(J)$. https://math.stackexchange.com/questions/2368440/prove-that-every-ideal-of-m-nr-is-of-the-form-m-ni-where-i-is-an-idea

506 Midterm

Daniel Rui - 5/11/21

Sándor it seems allowed collaboration (though hesitantly, I guess?) and seemed to think it was a good idea to list collaborators. So, acknowledgments to Bashir Fattel-Abdah and Rahul Chandra.

In the following problems, k denotes a field, and A denotes a c1-ring (commutative with identity).

Problem 1

Let A be an integral domain and assume that A is injective as an A-module. We want to show that A must in fact be a field. Recall from Homework 2 that injective modules I are those that satisfy the "triangle diagram"

$$\begin{tikzcd}
B \arrow[r, hook, "f"] \arrow[d] & C \arrow[dl, dashed, "\exists"] \\
I &
\end{tikzcd}$$

for any A-modules B, C and injective map $f : B \hookrightarrow C$. An alternative definition is that for any module M, every injection $I \hookrightarrow M$ splits, i.e. for all $f : I \hookrightarrow M$ and modules M, there is $s : M \to I$ s.t. $s \circ f = \mathrm{id}_I$ (where f, s are A-module homomorphisms). I proved in Problem 3 of Homework 2 that these are equivalent, but I will provide a proof of the direction I need here, for sake of completeness (copied from Problem 2 of my Homework 2).

Claim: if I is injective, then any injection $f : I \hookrightarrow M$ splits. *Proof:* since I is injective, we can use the triangle diagram to see that $\mathrm{id}_I : I \to I$ extends to some map $s : M \to I$ s.t. $s \circ \iota = \mathrm{id}_I$.

Now for the actual problem. To show A is a field, it is sufficient (and necessary) to show that for any non-zero $a \in A$, there is an inverse of a in A. Let us fix some arbitrary non-zero element $a \in A$. Consider $f : A \to A$ defined by $x \mapsto ax$. This map is injective because $ax = 0 \implies x = 0$ because A is an integral domain, and we specified that $a \neq 0$ above. Then, by the **claim** above, there is a splitting $s : A \to A$ s.t. $s \circ f = \mathrm{id}_I$, so in particular $s(f(1)) = s(a) = 1$. Because s is an A-module homomorphism, $s(a) = s(a \cdot 1) = as(1)$, and so we see that $as(1) = 1$, and so $s(1)$ is the desired inverse of a. ■

Problem 2

We are asked to think about the word `Hauptidealsatz`, and name the first mathematician we think of upon seeing this word. Well, we can split the word up as follows: `Haupt` (main; cf. Hauptgerichte/Hauptspeisen, "main dishes"), `ideal` (ideal of ring), and `satz` (theorem). Main leads me to think either "maximal" or "principal", and only principal seems to fit ("main dishes" matches "principal dishes" more closely than "maximal dishes"). So this is some "theorem about principal ideals". And as the only other "satz" I know is Hilbert's Nullstellensatz, I'll go with Hilbert.

Problem 3

Let A be a Noetherian ring with unique maximal ideal $\mathfrak{m}$ (i.e. A is a Noetherian local ring), and M be a finite A-module with $x \in \mathfrak{m}$ be s.t. it is neither zero-divisor on A nor on M. We want to show that M/xM being a free A/xA-module implies that M is a free A-module. M/xM being a free A/xA-module means there is some basis $\tilde{B} := \{b_1 + xM, \ldots, b_n + xM\}$ that generates M/xM as an A/xA-module (i.e. for any element $\epsilon + xM$ of M/xM, there are elements $a_1 + xA, \ldots, a_n + xA$ s.t. that element can be written as $\epsilon + xM = \sum_{i=1}^n (a_i + xA)(b_i + xM) = \sum_{i=1}^n a_i b_i + xM$), and is moreover linearly independent over A/xA (i.e. $\sum_{i=1}^n a_i b_i + xM = 0 + xM \implies a_i + xA = 0$ for all $i \in [n]$).

If we had that $xM = \mathfrak{m}M$, then by Nakayama's lemma (Corollary 2.39 in Lec 9), $B := \{b_1, \ldots, b_n\}$ would generate M as an A-module. In the case that $xM \subsetneq \mathfrak{m}M$ (the only other case, as $x \in \mathfrak{m}$), we would have to show that $\tilde{B}$ generates $M/\mathfrak{m}M$ in order to use Nakayama again. That is, we would have to show that for any element $\epsilon + \mathfrak{m}M$ of $M/\mathfrak{m}M$, there are elements $a_1 + xA, \ldots, a_n + xA$ s.t. that element can be written as $\epsilon + \mathfrak{m}M = \sum_{i=1}^n (a_i + xA)(b_i + \mathfrak{m}M) = \sum_{i=1}^n a_i b_i + \mathfrak{m}M$. Well, because $xM \subsetneq \mathfrak{m}M$, the map $\phi = \epsilon + xM \mapsto \epsilon + \mathfrak{m}M : M/xM \to M/\mathfrak{m}M$ is well-defined and surjective. Thus, for any $\epsilon + \mathfrak{m}M \in M/\mathfrak{m}M$, we have that $\epsilon + xM = \sum_{i=1}^n (a_i + xA)(b_i + xM) = \sum_{i=1}^n a_i b_i + xM \implies \epsilon + \mathfrak{m}M = \sum_{i=1}^n (a_i + xA)(b_i + \mathfrak{m}M) = \sum_{i=1}^n a_i b_i + \mathfrak{m}M$, and so indeed $\{b_1 + \mathfrak{m}M, \ldots, b_n + \mathfrak{m}M\}$ generates $M/\mathfrak{m}M$, and we can again use Nakayama to see that $B := \{b_1, \ldots, b_n\}$ generates M as an A-module.

Problem 4

Let A be a Noetherian integral domain and let $t \in A$ be a non-unit. We want to show that $\bigcap_{n \in \mathbb{N}} (t^n) = 0$. If $t = 0$, the claim is trivial so suppose $t \neq 0$ (integral domain-ness gives that $t^n \neq 0$ for all $n \in \mathbb{N}$). Well, suppose for sake of contradiction that this intersection is not 0; then there is some (non-zero) $x \in A$ s.t. $x \in (t^n)$ for all $n \in \mathbb{N}$. This means that there are (non-zero) $a_n \in A$ (for each $n \in \mathbb{N}$) s.t. $x = a_1 t^1 = a_2 t^2 = \ldots = a_n t^n = a_{n+1} t^{n+1} = \ldots$ and so on. Because A is an integral domain, we can cancel non-zero elements, and so we get that $a_n = a_{n+1} t$ for all $n \in \mathbb{N}$.

That means that defining the ideals $I_n = (a_n)$ for all $n \in \mathbb{N}$, we have that $I_1 \subseteq I_2 \subseteq \ldots$ and so on is an ascending chain of ideals ($a_n = a_{n+1} t \in (a_{n+1}) = I_{n+1} \implies I_n = (a_n) \subseteq I_{n+1}$). These inclusions moreover have the be strict, because $I_{n+1} \subseteq I_n \iff a_{n+1} \in (a_n) \implies a_{n+1} = a_n a$ for some $a \in A \implies a_{n+1} = a_{n+1} t a \implies$ (again by cancellation) $1 = ta$, contradicting t being a non-unit (as specified above). Of course, such a chain of ideals contradicts A being Noetherian, and so our initial assumption must have been false; there must not exist non-zero $x \in (t^n)$ for all $n \in \mathbb{N}$. ■

Problem 5

Let k be a field and let $A = {}^{k[x_1, \ldots, x_n]}/_{I}$ for $I := (x_1^2 + \ldots + x_n^2)$. We are asked to find an explicit demonstration of Noether normalization, i.e. to find a set of algebraically independent elements that generate a k-subalgebra of A over which A is integral, and then to use this to determine $\dim A$. It will be good to reference Theorem 2.96 (Noether normalization) and Definition 2.95 (algebraic independence) from Lec 16, which uses Corollary 2.82 (integral extension preserve dimension) from Lec 14 for the statement about the dimension.

I claim that the elements $x_1 + I, \dots, x_{n-1} + I$ are algebraically independent s.t. $x_n + I$ (and hence A) is integral over $A' := k[x_1 + I, \dots, x_{n-1} + I]$ (i.e. the k-subalgebra of A generated by $x_1 + I, \dots, x_{n-1} + I$). First, we have $x_n + I$ integral over A', because $x_n + I$ is the root of the monic polynomial $t^2 + (x_1 + I)^2 + \dots + (x_{n-1} + I)^2 = x_1^2 + \dots + x_{n-1}^2 + t^2 + I \in A'[t]$, because $x_1^2 + \dots + x_{n-1}^2 + x_n^2 + I = 0 + I = 0_A$.

These elements are algebraically independent (see Definition 2.95 in Lec 16) because if we have some polynomial f in the polynomial ring in $n-1$ variables over k s.t. $f(x_1 + I, \dots, x_{n-1} + I) = f(x_1, \dots, x_{n-1}) + I = 0 \iff f(x_1, \dots, x_{n-1}) \in I \iff f(x_1, \dots, x_{n-1}) = p \cdot (x_1^2 + \dots + x_n^2)$ for some $p \in k[x_1, \dots, x_n]$, then because we have an identical equality we can set all the $x_1, \dots, x_{n-1}$ to 1, yielding a constant on the LHS and a polynomial in x_n on the RHS, a contradiction unless $p = 0$, in which case f is identically 0.

Thus we have A is integral over $k[x_1 + I, \dots, x_{n-1} + I]$, which by algebraic independence (again see Def. 2.95 in Lec 16) is isomorphic to the polynomial ring in $n-1$ variables over k, which has dimension $n-1$, by Theorem 2.87 in Lec 15. By Corollary 2.82 from Lec 14, which says that an integral extension B of A has the same dimension as A, we see that A must also have dimension $n-1$. ■

Problem 6

Let $I := (x^2 - yz, xy - zt) \triangleleft k[x, y, z, t]$. We want to show that I is not prime. The immediate thought is to find some polynomials $p, q \in k[x, y, z, t]$ s.t. $pq \in I$ but one of p, q are not in I, and the first thing to try would just be to plug in these relations into one another, and in fact (surprisingly, perhaps?) this admittedly stupid/juvenile method works.

I first tried plugging $x^2 = yz$ into $z(xy - zt)$, getting that $xy - zt \in I \implies xyz - z^2t \in I \implies x^3 - z^2t \in I$ (where we can do this substitution because any monomial with yz, say $yz \cdot$(blah) differs from $x^2 \cdot$(blah) by $(x^2 - yz) \cdot$(blah) $\in I$) — this unfortunately was not particularly insightful. The second thing I tried was plugging $x^2 = yz$ into $x(xy - zt)$, getting that $x^2y - xzt \in I \implies (yz)y - xzt = z(y^2 - xt) \in I$. Aha! Now we have a product in I; let us try now to show that one of z or $y^2 - xt$ are not in I.

It is clear that $I \subseteq (x, z)$ (elements of I are $p \cdot (x^2 - yz) + q \cdot (xy - zt) +$ constants $= x(p \cdot x + q \cdot y) + z(p \cdot (-y) + q \cdot (-t)) +$ constants, where p, q are polynomials in $k[x, y, z, t]$). It is also clear that $y^2 - xt \notin (x, z)$, because if it were, then because $xt \in (x, z)$, $y^2 = y^2 - xt + xt \in (x, z)$, which it is not as y^2 is neither constant nor an element of the form $p \cdot x + q \cdot z$ for polynomials $p, q \in k[x, y, z, t]$. Thus, I is not prime, as desired.

Problem 7

Let $\mathfrak{m}$ be a maximal ideal of $A := \mathbb{Z}[x_1, \ldots, x_n]$ (polynomial ring over n variables). We want to show that ${}^{A}/_{\mathfrak{m}}$ is a finite field. We know (from as early as Math 504) that in fact for any (c1-)ring A and ideal $I \triangleleft A$, I is maximal if and only if ${}^{A}/_{I}$ is a field, so indeed ${}^{A}/_{\mathfrak{m}}$ is a field. The hard part of the problem is proving that it is finite. We split into two cases.

We first review Theorem 1.136 from Lec 17, which says that for a field extension K of a field k s.t. K is finitely generated k-algebra, we then have that K is algebraic over k and moreover is a finite extension of k, i.e. $[K : k] < \infty$. The proof is as follows: from Theorem 2.96 (Noether normalization) from Lec 16, we have that K finitely generated k-algebra $\implies$ K is finite/integral over $k[z_1, \ldots, z_r]$ for algebraically independent $z_1, \ldots, z_r \in K$, where r actually must equal 0 because Prop. 2.75 of Lec 14 says that for an integral extension B of A, A field $\iff$ B field, and $k[z_1, \ldots, z_r]$ which is isomorphic to the polynomial ring in r variables over k is not a field unless $r = 0$.

Case 1: non-zero integer in $\mathfrak{m}$. The smallest positive integer contained in $\mathfrak{m}$ must in fact be prime (maximal ideals are prime, and composite number in $\mathfrak{m}$ implies smaller factor in $\mathfrak{m}$), say p, and in fact $\mathbb{Z} \cap \mathfrak{m} = (p)$. Then, we have that $\mathbb{F}_p$ (finite field with p elements) embeds in ${}^{A}/_{\mathfrak{m}}$, i.e. ${}^{A}/_{\mathfrak{m}}$ is a field extension of $\mathbb{F}_p$. Because ${}^{A}/_{\mathfrak{m}}$ is a finitely generated $\mathbb{Z}$-algebra (has valid multiplication because it's a ring and $\mathbb{Z}$-module, i.e. an abelian group w.r.t. addition that has valid scalar multiplication with scalars in $\mathbb{Z}$, generated as a $\mathbb{Z}$-algebra by the elements $x_1 + \mathfrak{m}, \ldots, x_n + \mathfrak{m}$), it is also a finitely generated $\mathbb{F}_p$-algebra (all the scalars in $\mathbb{Z}$ are now taken modulo p because we are quotienting by $\mathfrak{m}$ which contains p), and so by Theorem 1.136 (described above), we must have that ${}^{A}/_{\mathfrak{m}}$ is a finite algebraic extension of $\mathbb{F}_p$. A finite field extension of a finite field remains a finite field, so in this case, we have successfully that ${}^{A}/_{\mathfrak{m}}$ is finite.

Case 2: no non-zero integer in $\mathfrak{m}$. In this case, we have that all of $\mathbb{Z}$ embeds in ${}^{A}/_{\mathfrak{m}}$ (via the map $z \mapsto z + \mathfrak{m}$, which is injective because $z_1 + \mathfrak{m} = z_2 + \mathfrak{m} \iff z_1 - z_2 \in \mathfrak{m} \implies z_1 - z_2 = 0$). We know that the fraction field of an integral domain is the smallest field containing that ring, so in fact we must also have an embedding $\mathbb{Q} \hookrightarrow {}^{A}/_{\mathfrak{m}}$ (for any integral domain R embedded in a field K, for any fraction $\frac{r}{s} \in \operatorname{Frac} R$, define φ to map it to rs^{-1} where s^{-1} is the inverse of s in K; this is a field homomorphism because $\varphi(\frac{r_1}{s_1} + \frac{r_2}{s_2}) = \varphi(\frac{r_1 s_2 + r_2 s_1}{s_1 s_2}) = (r_1 s_2 + r_2 s_1) s_1^{-1} s_2^{-1} = r_1 s_1^{-1} + r_2 s_2^{-1} = \varphi(\frac{r_1}{s_1}) + \varphi(\frac{r_2}{s_2})$, and similar for multiplication, and injective because $rs^{-1} = 0 \implies r = 0 \implies \frac{r}{s} = 0_{\operatorname{Frac} R}$).

Thus, ${}^{A}/_{\mathfrak{m}}$ is a field extension of $\mathbb{Q}$, and because it is also a finitely generated $\mathbb{Q}$-algebra (field extension of k is special case of k-algebra, and finitely generated as a $\mathbb{Q}$-algebra because it is finitely generated as a $\mathbb{Z}$-algebra; more explicitly we have that every element of ${}^{A}/_{\mathfrak{m}}$ can be written as polynomial $p(x_1 + \mathfrak{m}, \ldots, x_n + \mathfrak{m})$ where p is a polynomial in n variables over $\mathbb{Z} \subseteq \mathbb{Q}$), Theorem 1.136 gives that ${}^{A}/_{\mathfrak{m}}$ is a finite algebraic extension of $\mathbb{Q}$.

Thus, letting $y_i := x_i + \mathfrak{m}$, we have that all the y_i ($i \in [n]$) are roots of monic polynomials in $\mathbb{Q}[t]$, say $p_1, \ldots, p_n$. Letting $d_1, \ldots, d_s$ be the denominators of the fractions in the coefficients of $p_1, \ldots, p_n$, we have that $p_1, \ldots, p_r \in \mathbb{Z}[\frac{1}{d_1}, \ldots, \frac{1}{d_s}]$, and so in fact $y_1, \ldots, y_n$ are integral over $\mathbb{Z}[\frac{1}{d_1}, \ldots, \frac{1}{d_s}]$, implying that ${}^{A}\!/_{\mathfrak{m}} = \mathbb{Z}[x_1 + \mathfrak{m}, \ldots, x_n + \mathfrak{m}] = \mathbb{Z}[y_1, \ldots, y_n] \subseteq \mathbb{Z}[\frac{1}{d_1}, \ldots, \frac{1}{d_s}][y_1, \ldots, y_n]$ is finite/integral over $\mathbb{Z}[\frac{1}{d_1}, \ldots, \frac{1}{d_s}]$ (see Prop. 2.70(ii) in Lec 13). But because $\mathbb{Q}$ is embedded in ${}^{A}\!/_{\mathfrak{m}}$, we get also that $\mathbb{Q}$ is integral over $\mathbb{Z}[\frac{1}{d_1}, \ldots, \frac{1}{d_s}]$.

Letting q be a prime that is not in the factorization of d_i for $i \in [s]$, I claim that $\frac{1}{q}$ can not possibly be integral over $\mathbb{Z}[\frac{1}{d_1}, \ldots, \frac{1}{d_s}]$, because if we had that $(\frac{1}{q})^d + c_{n-1}(\frac{1}{q})^{d-1} + \ldots + c_0 \iff (\frac{1}{q})^d = -c_{n-1}(\frac{1}{q})^{d-1} - \ldots - c_0$ for coefficients $c_i \in \mathbb{Z}[\frac{1}{d_1}, \ldots, \frac{1}{d_s}]$, then clearing denominators (say multiply by $q^d \cdot \prod_{i=1}^{s} d_i$) yields that the LHS is not a multiple of q while the RHS is, of course a contradiction. Thus in fact Case 2 can not happen, and we already showed that Case 1 results in ${}^{A}\!/_{\mathfrak{m}}$ being a finite field. ■

Problem 8

For variables α, β, we want to show that $A := k[\alpha^4, \alpha^3\beta, \alpha\beta^3, \beta^4] \subseteq k[\alpha, \beta]$ is not integrally closed, and then find its integral closure. To show that it is not integrally closed, it suffices to find some element in $\operatorname{Frac}(A) \setminus A$ that is the root of some monic polynomial in $A[x]$.

Let us first determine some elements of $\operatorname{Frac} A$; we have $\frac{\alpha}{\beta} = \frac{\alpha^4}{\alpha^3\beta} \in \operatorname{Frac} A$ (similarly $\frac{\beta}{\alpha}$ by symmetry), and $\alpha^2\beta^2 = \frac{(\alpha^3\beta)^2}{\alpha^4} \in \operatorname{Frac} A$ (in fact these are the only interesting ones I found). Note that $\alpha^2\beta^2 \notin A$ because any non-constant monomial term of a polynomial in A has the exponent of $\alpha \geq 3$ or the exponent of $\beta \geq 3$, and of course the exponents of $\alpha^2\beta$ are both $2 < 3$; moreover, it is obvious that $\alpha^2\beta^2 \in \operatorname{Frac}(A) \setminus A$ is the root of $x^2 - \alpha^4\beta^4 \in A[x]$, and so indeed we have shown that A is not integrally closed.

To find the integral closure of A, note that we have the following chain of inclusions: $A \subseteq$ [integral closure of A in $\operatorname{Frac} A$] $\subseteq$ [integral closure of A in $\operatorname{Frac}(k[\alpha, \beta]) = k(\alpha, \beta)$] $\subseteq$ [integral closure of $k[\alpha, \beta]$ over $k(\alpha, \beta)$]. Because $k[\alpha, \beta]$ is a UFD, it is integrally closed, as I proved in Problem 2 of 506 Homework 5. I provide a copy of the proof at the end of the problem.

Thus, we have the chain of inclusions is $\subseteq k[\alpha, \beta]$. The integral closure of A over $k(\alpha, \beta)$ is in fact equal to $k[\alpha, \beta]$; it suffices to show that $\alpha, \beta \in k[\alpha, \beta]$ are integral over A, which they are because obviously α, β are roots $x^4 - \alpha^4, x^4 - \beta^4$ respectively. Finally, we see that the integral closure over A in $\operatorname{Frac} A$ are exactly the elements of $k[\alpha, \beta]$ integral over A that are ALSO in $\operatorname{Frac} A$, i.e. we have that the integral closure over A (in its fraction field $\operatorname{Frac} A$) is exactly $\operatorname{Frac} A \cap k[\alpha, \beta]$.

I claim that $\operatorname{Frac} A \cap k[\alpha, \beta] = k[\alpha^4, \alpha^3\beta, \alpha^2\beta^2, \alpha\beta^3, \beta^4] =: A'$. The $(\supseteq)$ direction is obvious, as we already established $\alpha^2\beta^2 \in \operatorname{Frac} A$. Now for $(\subseteq)$. Suppose we have an element in the intersection; then we have that $\frac{a}{b} = p \iff a = bp$ for polynomials $a, b \in A$ and $p \in k[\alpha, \beta]$. We want to prove that this $p \in A'$. As $a, b \in A = k[\alpha^4, \alpha^3\beta, \alpha\beta^3, \beta^4]$, we know that all their monomials have degree multiple of 4 (i.e. each monomial $\alpha^i\beta^j$ has 4 dividing $\deg(\alpha^i\beta^j) := i + j$).

We can split p into p_1+p_2, where p_1 consists of all monomials with degree multiple of 4 and p_2 consists of all monomials with degree $\neq$ multiple of 4. Let's moreover put all the constants terms of p in p_1 as well. Then, we have that $a - bp_1 = bp_2$, where the LHS has all monomials degree multiple of 4, and the RHS has all monomials degree $\neq$ multiple of 4 (the product of a degree mult. of 4 monomial with a degree $\neq$ mult. of 4 monomial yields a degree $\neq$ mult. of 4 monomial). This implies that $bp_2 = a - bp_1$ must be constants. The only way for bp_2 to be constant is if $p_2 = 0$ (because we put all the constant terms of p in p_1), in which case $p = p_1$, i.e. p consists of monomials with degree multiple of 4, implying $p \in A'$ as desired.

Appendix: UFDs are integrally closed

Let us now prove that UFDs are integrally closed (Homework 2.73 in Lec 13), which will prove that $k[\alpha, \beta]$ is integrally closed because we proved polynomial rings with finitely many variables are UFDs in Homework 1 from Math 505). Let A be a UFD and let $K = \operatorname{Frac} A$. It suffices to prove that any monic polynomial $f \in A[x]$ is such that $\alpha \in K$ is a root, then α is in fact in A, because $\tilde{A}$ is the set of all $\alpha \in K$ s.t. there is monic $f \in A[x]$ s.t. $f(\alpha) = 0$, and this claim gives that $\tilde{A} \subseteq A$, and of course $A \subseteq \tilde{A}$.

Ok, suppose $\alpha = \frac{a}{b} \in K$ is the root of some polynomial $x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in A[x]$. Moreover because A is a UFD, we can suppose that a and b have no (non-unit) factors in common (if they did, we can just cancel them). Then, we get that $a^n = -(a_{n-1}a^{n-1}b + \ldots + a_0 b^n)$, i.e. a^n is a multiple of b. But this is impossible, since a, b not having (non-unit) factors in common in their unique (!) factorization means that a^n, b can not have (non-unit) factors in common in their unique factorization. Thus, b must be a unit, and $\alpha = \frac{a}{b} \in A$.

506 Homework 5

Daniel Rui - 5/4-7/21

For all these problems, k denotes an algebraically closed field. Furthermore, recall from Lec 12 on 4/23/21 that an A-algebra B is integral over A (a c1-ring) if every element $y \in B$ is integral over A; i.e. every $y \in B$ is the root of some MONIC (!!!) polynomial $f \in A[x]$. Analogue to “algebraic over”.

Problem 1

Consider the injective ring homomorphism $k[x,y] \hookrightarrow k[x,z]$ given by $x \mapsto x, y \mapsto xz$. We want to prove that this is NOT an integral extension. If we want to think about things as a strict (inclusion) extension, we can say that we want to prove that $k[x,xz] \subseteq k[x,z]$ is not an integral extension. It suffices (and I think necessary?) to prove that z is not integral over $A := k[x,xz]$, i.e. there is no monic $f(t) \in A[t]$ s.t. $f(z) = 0$. Indeed, suppose there was such an $f = t^n + a_{n-1}t^{n-1} + \ldots + a_0 \in A[t]$.

In order to make $f(z) = 0$, it must be that there is some term in $a_{n-1}z^{n-1} + \ldots + a_0$ that cancels with z^n. But because $a \in A$ are of the form $xp(x,xz) + xzq(x,xz) + c$ for $p(x,xz), q(x,xz) \in k[x,xz]$ and $c \in k$, either a_i for $i \in \{0,\ldots,n-1\}$ is a multiple of x, in which case it couldn't possibly cancel with z^n (if $f(z)$ is identically 0, we could set $x = 0$ and still get 0), or a constant $c \in k$, in which case cz^i also couldn't possibly cancel with z^n (since $i < n$).

Problem 2

Let $A = {}^{k[x,y]}/_{I}$ for $I := \langle x^3 + x^2 - y^2 \rangle$. We want to determine the integral closure of A. It will be instructive to look at Lec 13 on 4/26/21, especially Definition 2.71, and Examples 2.72, 2.74. Recall the following definitions: if B is an A-algebra, then $\tilde{A} := \{y \in B : y \text{ integral over } A\}$ (which is a subring of B, and satisfies $\tilde{\tilde{A}} = \tilde{A}$) is the integral closure of A in B. The integral closure of A is its integral closure in $B := \operatorname{Frac} A$. Lastly, A integrally closed in B means that $A \cdot 1_B = \tilde{A}$, and A integrally closed means that A is integrally closed in $B := \operatorname{Frac} A$.

First, recall from Problem 6 of Homework 4 (last week) that $A \simeq k[t^2-1, t(t^2-1)] \subseteq k[t]$. Then, $\operatorname{Frac} A \simeq \operatorname{Frac}(k[t^2-1, t(t^2-1)]) = k(t)$ (the $(\subseteq)$ direction is obvious, and $t = \frac{t(t^2-1)}{t^2-1}$ gives the $(\supseteq)$ direction). Because $A \subseteq A' \implies \tilde{A} \subseteq \tilde{A}'$ (because $y \in B$ integral over A implies it is obviously integral over A'), we have that the integral closure of A over $B := k(t)$ is contained in the integral closure of $k[t]$ over $k(t)$.

Let us now prove that UFDs are integrally closed (Homework 2.73 in Lec 13), which will prove that $k[t]$ is integrally closed because we proved polynomial rings with finitely many variables are UFDs in Homework 1 from Math 505). Let A be a UFD and let $K = \operatorname{Frac} A$. It suffices to prove that any monic polynomial $f \in A[x]$ is such that $\alpha \in K$ is a root, then α is in fact in A, because $\tilde{A}$ is the set of all $\alpha \in K$ s.t. there is monic $f \in A[x]$ s.t. $f(\alpha) = 0$, and this claim gives that $\tilde{A} \subseteq A$, and of course $A \subseteq \tilde{A}$.

Ok, suppose $\alpha = \frac{a}{b} \in K$ is the root of some polynomial $x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in A[x]$. Moreover because A is a UFD, we can suppose that a and b have no (non-unit) factors in common (if they did, we can just cancel them). Then, we get that $a^n = -(a_{n-1}a^{n-1}b + \ldots + a_0 b^n)$, i.e. a^n is a multiple of b. But this is impossible, since a, b not having (non-unit) factors in common in their unique (!) factorization means that a^n, b can not have (non-unit) factors in common in their unique factorization. Thus, b must be a unit, and $\alpha = \frac{a}{b} \in A$.

Going two paragraphs up, recall that we said that the integral closure $\tilde{A}$ of $A = {}^{k[x,y]}/_{I} \simeq k[t^2 - 1, t(t^2-1)]$ over $\operatorname{Frac} A \simeq k(t)$ is contained in the integral closure of $k[t]$ over $k(t)$, which we just proved is $k[t]$ itself. Thus, $\tilde{A} \subseteq k[t]$. This is actually an equality, and to prove this, it suffices to show that $t \in \tilde{A}$. Observe that t is a root of the polynomial $x^3 - x^2 + t(t^2-1) \in A[x]$ (when thinking of A as $k[t^2 - 1, t(t^2-1)]$). Thus, we have found that the integral closure of A over $\operatorname{Frac} A$ is isomorphic to $k[t]$.

Problem 3

Assume that the characteristic of $k \neq 2$ and let $f \in A := k[x_1, \ldots, x_n]$ be a square-free non-constant polynomial (i.e. f is not divisible by the square of a non-constant polynomial). Define $B = {}^{A[z]}/_{I}$ for $I := \langle z^2 - f \rangle$ and let $K = \operatorname{Frac} A$ and $L = \operatorname{Frac} B$. Note that elements of L are $\frac{p(z)+I}{q(z)+I}$. Let $\alpha = g + hz \in L$ where $g, h \in K$, where we think of $\alpha = \frac{a}{b} + \frac{cz}{d} = \frac{ad+bcz}{bd}$ as the corresponding element $\frac{ad+bcz+I}{bd+I} \in L$. We want to determine the minimal polynomial of α over K and prove that α is integral over A if and only if $g, h \in A$.

Recall from Homework 4 (last week) Problem 1 that L is a degree-2 algebraic extension of K, so we know all minimal polynomials have degree ≤ 2. In the case that $h = 0$, we clearly have that $\operatorname{Irr}(\alpha, K) = t - g \in K[t]$, and in fact $\alpha = g \in K$. In the case that $h \neq 0$, $\alpha \notin K$ (because if it was, $z = \frac{\alpha - g}{h} \in K$; contradiction), and so $\operatorname{Irr}(\alpha, K)$ must have degree 2. With this information it is not hard to find $\operatorname{Irr}(\alpha, K) = (t-g)^2 - h^2 f = t^2 - 2gt + g^2 - h^2 f \in K[t]$, which indeed satisfies $(\alpha - g)^2 - h^2 f = h^2(z^2 - f) = 0_L$.

Because A is a UFD (see Problem 2 above) and $\alpha \in K = \operatorname{Frac} A$, Corollary 2.67 from Lec 12 on 4/23/21 tells us that α is integral over A if and only if the coefficients of its monic minimal polynomial over $K = \operatorname{Frac} A$ are in A. Thus, for ($\Longleftarrow$), we see that $g, h \in A \implies$ the coefficients of both possible minimal polynomials $t - g$ and $(t-g)^2 - h^2 f$ are in $A \implies \alpha$ integral over A.

For ($\implies$), α integral over A implies (in the case that $h = 0$) that $g \in A, h = 0 \in A$, or (in the case that $h \neq 0$) that $-2g, g^2 - h^2 f \in A$. Then, $g \in A$ (because $-\frac{1}{2} \in k \subseteq A$, using that char $k \neq 2$) and $g^2 - (\frac{c}{d})^2 f = q$ where $q \in A$ and we can assume c, d do not share factors (A being UFD is important for these "share factors" arguments). Clearing the denominators yields $g^2 d^2 - c^2 f = q d^2 \implies f = \frac{d^2(q - g^2)}{-c^2} \in A$. But c^2 does not share factors with d^2, meaning $c^2 \mid (q - g^2)$, and so $d^2 \mid f$, implying that d^2 must be constant (and hence d also) because f is square free, and so $h \in A$.

Finally, observe that this proves that B is integrally closed, because the elements $\alpha = g+hz$ for $g, h \in A$ correspond (in the sense above in the 1st paragraph) exactly with the elements of B considered as elements of L, i.e. elements $\frac{p(z)+I}{1+I}$. This is because clearly $\alpha = \frac{g+hz+I}{1+I}$ is such an element of $B \subseteq L$ (my notation for the copy of B in L), and for other direction of inclusion, for any $p(z)+I$, any degree 2 or higher term in $p(z)$ can just be replaced by a degree 0 or 1 term, since $z^{2n+0,1} + I = f^n z^{0,1} + I$. Thus, we have that the elements of $B \subseteq L$ are exactly those that are integral over A, i.e. B is the integral closure of A in L. We'll denote the operation "integral closure of ... in L" by the tilde. Recall from Prop. 2.70(iv) of Lec 13 on 4/26/21 that $\tilde{A} = \tilde{\tilde{A}}$. Then, $B = \tilde{A} = \tilde{\tilde{A}} = \tilde{B}$, and indeed B is integrally closed (over its fraction field L).

Problem 4

Let A be an integrally closed integral domain and $K = \operatorname{Frac} A$.

Problem 5

Let A be a Noetherian integral domain. We want to prove the following, where we think of everything as elements of $K = \operatorname{Frac} A$ (A being integral domain is important for K to exist):

$$A = \bigcap_{\mathfrak{p} \lhd_{\text{pr}} A} A_{\mathfrak{p}} = \bigcap_{\mathfrak{m} \lhd_{\max} A} A_{\mathfrak{m}} \qquad \text{(thinking of everything as} \subseteq K).$$

By A above we mean the localization $\{1\}^{-1}A$. Note that it was important that A is an integral domain for us to think of all these localizations $S^{-1}A$ as subsets of K, because the identity map $\phi_S : S^{-1}A \to K$ defined by $\frac{a}{s} \mapsto \frac{a}{s}$ induces a surjection $A \twoheadrightarrow \operatorname{im} \phi_S = \{\frac{a}{s} \in K : a \in A, s \in S\}$, that is also injective because if there is $b \in A \setminus \{0\}$ s.t. $\frac{a}{s} = \frac{0}{b}$, then $ab = 0$, and by integral domain-ness and $b \neq 0$, we must have $a = 0$.

We will prove this chain of equalities by proving that $A \subseteq \bigcap_{\mathfrak{p} \lhd_{\text{pr}} A} A_{\mathfrak{p}} \subseteq \bigcap_{\mathfrak{m} \lhd_{\max} A} A_{\mathfrak{m}} \subseteq A$. For the first ($\subseteq$), we have already proven in the above paragraph that all the localizations can be thought of as subsets of K, and indeed A (thought of as a subset of K), i.e. $\{\frac{a}{1} \in K : a \in A\}$, is a subset of $A_{\mathfrak{p}}$ (thought of as a subset of K), i.e. $\{\frac{a}{s} \in K : a \in A, s \in S := A \setminus \mathfrak{p}\}$, because $1 \in S := A \setminus \mathfrak{p}$. The second ($\subseteq$) is trivial because maximals ideals are prime, and taking the intersection over a bigger set of things will be smaller (or equal to) the intersection over any subset of that bigger set.

Now for the third ($\subseteq$). Suppose we have some $x := \frac{a}{b} \in K$ s.t. $x = \frac{a}{b} \in A_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m} \lhd A$, and assume for sake of contradiction that $x \notin A$. Let us now define the ideal $I := \{a \in A : ax \in A\}$ (ideal because $i \in I, a \in A \implies ax \in A \implies iax \in A \implies ia \in A$ and $i_1, i_2 \in I \implies i_1 x, i_2 x \in A \implies (i_1 - i_2)x \in A \implies i_1 - i_2 \in I$) and note that $x \notin A \implies 1 \notin I \implies I$ is a proper ideal of A. Because I is proper, we can then find a maximal ideal $\mathfrak{m}$ containing it (just Zorn's lemma); now I claim that x can not possibly be in $A_{\mathfrak{m}}$ (which will be a contradiction).

If $x \in A_{\mathfrak{m}}$ (thought of as a subset of K), then there will be $s \in S := A \setminus \mathfrak{m}$ and $a \in A$ s.t. $x = \frac{a}{s} \implies sx = a \in A$ (or if we're being pedantic, $sx = \frac{a}{1} \in \{1\}^{-1}A$, i.e. the copy of A in K talked about in the first paragraph), implying that $s \in I \subseteq \mathfrak{m}$. This of course contradicts that $s \in S := A \setminus \mathfrak{m}$, and so our initial assumption that $x \notin A$ was false. QED.

Problem 6

We want to use the notation and statement of Problem 5 to prove that the following are equivalent:

(i) A is integrally closed

(ii) $A_{\mathfrak{p}}$ is integrally closed for all prime ideals $\mathfrak{p} \triangleleft A$.

(iii) $A_{\mathfrak{m}}$ is integrally closed for all maximal ideals $\mathfrak{m} \triangleleft A$.

We prove these equivalences by showing (i) $\implies$ (ii) $\implies$ (iii) $\implies$ (i). First note that the fraction field of any of these localizations $S^{-1}A$ is just K again, because note that $\frac{a/s}{b/t} = \frac{at/1}{bs/1} \in \mathrm{Frac}(S^{-1}A)$ since $\frac{a}{s}\frac{bs}{1} = \frac{abs}{s} = \frac{ab}{1} = \frac{abt}{t} = \frac{b}{t}\frac{at}{1}$; then $\phi : \mathrm{Frac}(S^{-1}A) \to K$ defined by mapping $\frac{a/1}{b/1} \mapsto \frac{a}{b}$ is well defined and injective ($\frac{a/1}{b/1} = \frac{c/1}{d/1} \iff ad = bc \iff \frac{a}{b} = \frac{c}{d}$) and surjective.

Let us begin by tackling (i) $\implies$ (ii). Suppose we have $\alpha \in K$ integral over $A_{\mathfrak{p}}$ for some prime ideal $\mathfrak{p} \triangleleft A$. Then, we have that α is the root of some monic polynomial in $A_{\mathfrak{p}}[x]$, say $x^n + \frac{a_{n-1}}{s_{n-1}}x^{n-1} + \ldots + \frac{a_0}{s_0} \in A_{\mathfrak{p}}[x]$, i.e. we have that $\alpha^n + \frac{a_{n-1}}{s_{n-1}}\alpha^{n-1} + \ldots + \frac{a_0}{s_0} = 0$ for $a_i \in A$ and $s_i \in S := A \setminus \mathfrak{p}$. Defining $s := \prod_{i=0}^{n-1} s_i$ and multiplying by s^n, we see that the coefficients become elements of A, where the first term is $(s\alpha)^n$ and all subsequent terms have coefficients containing s^{n-1}. In other words, by multiplying by s^n, we have found that $s\alpha \in K$ is the root of a monic polynomial in $A[x]$. Because A is integrally closed, $s\alpha$ must be an element of A, and so then $\alpha = \frac{s\alpha}{s} \in A_{\mathfrak{p}}$. Thus, we have shown that all elements of K that are integral over $A_{\mathfrak{p}}$ are actually elements of $A_{\mathfrak{p}}$, and hence $A_{\mathfrak{p}}$ is integrally closed (over its fraction field $\mathrm{Frac}(A_{\mathfrak{p}}) \simeq K$).

For (ii) $\implies$ (iii), it is just like I said above in Problem 5: maximals ideals are prime, so proving something for all prime ideals proves that thing for all maximal ideals too.

For (iii) $\implies$ (i), suppose we have $\alpha \in K$ integral over A. Then, we have that α is the root of some monic polynomial $f(x) := x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in A[x]$, where in fact we think of the elements of A as elements of K. But recall from Problem 5 that we proved that $A \subseteq A_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m} \triangleleft A$. That means that $f(x) \in A_{\mathfrak{m}}[x]$ for every $\mathfrak{m} \triangleleft_{\max} A$, and because we assume that all the $A_{\mathfrak{m}}$ are integrally closed, α root of $f(x) \in A_{\mathfrak{m}}[x] \implies \alpha$ integrally closed over $A_{\mathfrak{m}} \implies \alpha \in A_{\mathfrak{m}}$. But this is for any $\mathfrak{m} \triangleleft_{\max} A$, and so indeed we have shown that $\alpha \in \bigcap_{\mathfrak{m} \triangleleft_{\max} A} A_{\mathfrak{m}}$, which recall from Problem 5 is equal to A. Thus, all $\alpha \in K$ integral over A are actually elements of A, and so A is integrally closed, as desired.

506 Homework 4

Daniel Rui - 4/30/21

Problem 1

Let k be a field of characteristic $\neq 2$, and let $f \in A = k[x_1, \ldots, x_n]$ be a square-free non-constant polynomial (i.e. f is non-constant and it is not the square of any element of A). Let $B = A[z] \big/ \langle z^2 - f \rangle$ and define the fraction fields $K = \operatorname{Frac}(A)$ and $L = \operatorname{Frac}(B)$. We want to prove that L is a Galois extension of K with Galois group $\mathbb{Z}/2\mathbb{Z}$ generated by $z \mapsto -z$.

First note that for any fields (not characteristic 2!) K, L, if L is a degree two extension of K, then L is a Galois extension of K. This is because if $\alpha \in L \setminus K$, then $\operatorname{Irr}(\alpha, K)$ has degree 2 (can't be degree one since $\alpha \notin K$, and can't be degree > 2 because then $[L : K]$, i.e. the dimension of L when thought of as a vector space over K would have more than 2 linearly independent elements, contradiction $[L : K] = 2$). Then, $\operatorname{Irr}(\alpha, K)$ splits over L since we can write it as $(x - \alpha)g(x)$, where $\deg g + \deg(x - \alpha) = \deg \operatorname{Irr}(\alpha, K) = 2 \implies \deg g = 1$ implying that $\operatorname{Irr}(\alpha, K)$ has both roots in L. Separability is where it's important that we are in characteristic $\neq 2$, since in this scenario, the (formal) derivative of $\operatorname{Irr}(\alpha, K)$ would have a $2x \neq 0$ term, and we know that derivative of irreducible polynomial $\neq 0 \iff$ separable.

Now, note that $z^2 - f \in A[z]$ is an irreducible polynomial, because if it were reducible, then we would have a degree 1 factor, i.e. a root $\alpha \in A$ s.t. $\alpha^2 - f = 0$, but this is forbidden because f was said to be square-free. Gauss's lemma then tells us that $z^2 - f$ is irreducible over $K[z]$, since $A = k[x_1, \ldots, x_n]$ is a UFD (both Gauss's lemma and A being UFD was proven in Homework 1 from Math 505). Therefore, letting α be a root of $z^2 - f$, we have that $K[z] \big/ \langle z^2 - f \rangle \simeq K(\alpha)$, which is a degree 2 extension of K because $\alpha^2 = f \in A \subseteq K$.

Now we prove that $L \simeq K[z] \big/ \langle z^2 - f \rangle$. Consider the map $\varphi : \operatorname{Frac}\Big(A[z] \big/ \langle z^2 - f \rangle\Big) \to K[z] \big/ \langle z^2 - f \rangle$ defined by

$$\frac{p(z) + \langle z^2 - f \rangle}{q(z) + \langle z^2 - f \rangle} \mapsto \frac{p(z)}{q(z)} + \langle z^2 - f \rangle.$$

This map is well-defined and injective because

$$\begin{aligned} \tfrac{p(z)+\langle z^2-f\rangle}{q(z)+\langle z^2-f\rangle} = \tfrac{p'(z)+\langle z^2-f\rangle}{q'(z)+\langle z^2-f\rangle} &\iff p(z)q'(z) + \langle z^2 - f \rangle = p'(z)q(z) + \langle z^2 - f \rangle \\ &\iff p(z)q'(z) - p'(z)q(z) \in \langle z^2 - f \rangle \\ &\iff \tfrac{p(z)}{q(z)} = \tfrac{p'(z)}{q'(z)} \text{ modulo } \langle z^2 - f \rangle, \end{aligned}$$

and obviously surjective. Thus, indeed $L \simeq K(\alpha)$, and so it is a degree 2, hence Galois extension of K. The Galois group has order $[L : K] = 2$, and the only group of order two is $\mathbb{Z}/2\mathbb{Z}$, so this is the Galois group. $\operatorname{Gal}_K(K(\alpha))$ is obviously generated by $\alpha \mapsto -\alpha$, and because α corresponds to the coset $\overline{z} := z + \langle z^2 - f \rangle \in K[z] \big/ \langle z^2 - f \rangle$, one can think of $\operatorname{Gal}_K(L)$ as generated by $\overline{z} \mapsto -\overline{z}$.

Problem 2

Let $J = (x^2 - yz, xz - x) \lhd A := k[x, y, z]$. We want to prove that $J = \sqrt{J}$, i.e. J is a radical ideal that is furthermore the intersection of three prime ideals. Recall that the radical $\sqrt{I}$ of an ideal $I \lhd A$ is defined to be $\{a \in A : a^n \in I \text{ for some } n \in \mathbb{N}\}$. Let us now prove that any intersection of prime ideals is a radical ideal.

Let $N = \bigcap_{i \in I} \mathfrak{p}_i$ for some prime ideals $\mathfrak{p}_i$ and index set I. It is true that for any ideal $I \subseteq \sqrt{I}$ (for $x \in I, x^1 \in \sqrt{I}$), so we just want to prove that $\sqrt{N} \subseteq N$. Well, if $x \in \sqrt{N}$, then $x^n \in N$ for some $n \in \mathbb{N}$, so $x^n \in \mathfrak{p}_i$ for all $i \in I$, and so by primality $x \in \mathfrak{p}_i$ for all $i \in I$, implying that $x \in N$. It is interesting to compare this to Corollary 2.32 from Lec 8 on 4/14/21 which says that for $I \lhd A$, $\sqrt{I}$ is the intersection of all prime ideals $\mathfrak{p} \supseteq I$.

Thus, it suffices to prove that J in our problem is the intersection of 3 prime ideals. It may help to give some geometric intuition; this problem corresponds to the fact that the zero set $\{(x, y, z) \in \mathbb{R}^3 : x^2 - yz = 0, xz - x = 0\}$ is the union of three curves, namely the y-axis, z-axis, and the parabola $\{(x, y, z) \in \mathbb{R}^3 : y = x^2, z = 1\}$ (one can verify this by graphing on say Geogebra). We set out to prove rigorously that $J = (x, z) \cap (x, y) \cap (x^2 - y, z - 1)$ where all three of these ideals are prime. Let's call them $\mathfrak{y}, \mathfrak{z}, \mathfrak{p}$ for y-axis, z-axis, and parabola respectively.

We prove these ideals are prime by showing that quotienting by them yields an integral domain. It is clear that $A\big/(x, z) = A\big/(x, y)$ (math does not care which symbols we use). I claim that they are both isomorphic to $k[t]$; for the first one consider the map $\phi : A \to k[t]$ defined by $y \mapsto t, x, z \mapsto 0$ (clearly surjective, and kernel is (x, z) because any $f(x, y, z) + (x, z) \in A\big/(x, z)$ can be written as $g(y) + (x, z)$, so being in the kernel yields $g(t) = 0$).

Lastly, we have that $A/\mathfrak{p}$ is also isomorphic to $k[x]$ by the map $\phi : A \to k[t]$ defined by $z \mapsto 1, y \mapsto t^2, x \mapsto t$ (any polynomial $f(x, y, z) + \mathfrak{p} \in A/\mathfrak{p}$ can be written $yg(x) + h(x) + \mathfrak{p}$, so being in the kernel yields $t^2 g(t) = -h(t)$ giving us $yg(x) + h(x) = yg(x) - x^2 g(x) = (y - x^2)g(x)$). As $k[t]$ is an integral domain, these three ideals are prime.

From Sándor himself: One small trick is that the last ideal is the same as $(z - 1, yz - x^2)$ (the difference of the two generators replacing each other is $y(z - 1)$). And then notice that $yz - x^2$ is in the intersection of the other two ideals (x, y) and (x, z), so what you need to prove is that $(x, y) \cap (x, z) \cap (z - 1) = J$. Using that polynomial rings are UFDs it is (again) relatively easy to prove that $(x, y) \cap (x, z) = (x, yz)$, and that $(x, yz) \cap (z - 1) = (x(z - 1), yz(z - 1))$. What's left to prove is that $(x(z - 1), yz(z - 1)) = J$. One of their generators are actually equal, and for the other, $yz(z - 1) = x^2(z - 1) - (z - 1)(x^2 - yz)$ shows that $yz(z - 1) \in J$. I am not sure if this is what you meant by a messy symbol-pushing/manipulation. I don't think there is a considerably easier way to do it. :)

Problem 3

Let $A = k[t]$ and $B = {k[x,y]}\Big/{\langle 1-xy\rangle}$. We want to prove that $A \not\cong B$ (as rings). Suppose that $\varphi : B \to A$ is a homomorphism. Because of homomorphism properties, it must satisfy $\varphi(1-xy) = 0$ because $1 - xy = 0_B$ (all elements here will actually denote the coset containing that element). Then, $\varphi(x)\varphi(y) = 1$, and so $\varphi(x), \varphi(y)$ are units and inverse of each other. But $\varphi(x), \varphi(y) \in k[t]$, and a degree argument gives that $0 = \deg(1) = \deg(\varphi(x)) + \deg(\varphi(y))$, which implies that both $\varphi(x), \varphi(y)$ are constants (since $\deg \geq 0$ and $\deg 0 \implies$ constant). Thus, we see that φ maps x, y to constants, and so φ maps all elements of $k[x,y]$ to constants, and so φ can not be surjective (e.g. it can never reach $t \in k[t]$ which is not a constant).

Problem 4

Let $\phi : k[z_{00}, z_{01}, z_{10}, z_{11}] \to k[x_0, x_1, y_0, y_1]$ be the k-algebra homomorphism given by $z_{ij} \mapsto x_i y_j$ for $i, j = 0, 1$. We want to show that $\ker\phi = \langle z_{00}z_{11} - z_{01}z_{10}\rangle$. Obviously, we have the $(\supseteq)$ direction, because $\phi(z_{00}z_{11} - z_{01}z_{10}) = x_0y_0x_1y_1 - x_0y_1x_1y_0 = 0$. We first prove a key lemma.

Kernel lemma: for any A-modules M, N and S, T submodules of M s.t. $S + T = M$ (where $S + T = \{s + t : s \in S, t \in T\}$), and a module homomorphism (A-linear) $\phi : M \to N$ s.t. $T \subseteq \ker\phi$ and $\phi|_S$ is injective, it is then true that $\ker\phi = T$.
Proof: deceptively easy for such a powerful lemma. Let $x \in \ker\phi$. Then, because $S + T = M$, there is $s \in S, t \in T$ s.t. $x = s + t$. Then, we have $0 = \phi(x) = \phi(s) + \phi(t)$. But $\phi(t) = 0$ because $t \in T \subseteq \ker\phi$, so $\phi(s) = 0$. By injectivity of $\phi|_S$, $s = 0$ and so $x = t \in T$, proving that $\ker\phi \subseteq T$.

We now apply this lemma. Let $T := \langle z_{00}z_{11} - z_{01}z_{10}\rangle$. We would like to find a submodule $S \subseteq M$ s.t. $S + T = M$ and $\phi|_S = M := k[z_{00}, z_{01}, z_{10}, z_{11}]$. Now why is ϕ not injective on M? Well, we see that $\phi(z_{00}z_{11}) = x_0y_0x_1y_1 = x_0y_1x_1y_0 = \phi(z_{01}z_{10})$. Basically, we may have different orderings of the indices of the z's which result in the same output product.

Thus, if we restrict ourselves to monomials $\prod_{i=1}^k z_{a_ib_i}$ ($a_i, b_i \in \{0,1\}$) such that the indices are increasing (weakly), like $a_1 \leq a_2 \leq \ldots \leq a_k$ and $b_1 \leq b_2 \leq \ldots \leq b_k$, then ϕ will be injective because given any $\prod_{i=1}^k x_{a_i}y_{b_i}$, we just reorder the indices so everything is increasing, and recover the unique monomial $\prod_{i=1}^k z_{a_i'b_i'}$ (where again I put a_i' instead of a_i because we reordered the a_i to be increasing, and same with the b_i). Thus, let us define S to be the submodule generated by all such "increasing" monomials; since the elements of S are then sums of these "increasing" monomials, injectivity for the monomials that we just proved holds through to these sums.

Finally we want to show that $S + T = M$. So suppose are given a monomial $\prod_{i=1}^k z_{a_ib_i}$. Then, we can suppose that the a_i are already weakly increasing since we can reorder them if they aren't. Note that we can't reorder BOTH a_i and b_i at the same time. Well, we would now like to prove that $\prod_{i=1}^k z_{a_ib_i}$ and $\prod_{i=1}^k z_{a_ib_{\sigma(i)}}$ differ by an element of T for any permutation $\sigma \in S_k$ (the symmetric group on k elements). In other words, we want to show that $\prod_{i=1}^k z_{a_ib_i} = \prod_{i=1}^k z_{a_ib_{\sigma(i)}}$ modulo T for any $\sigma \in S_k$.

Because S_k is generated by transpositions of the form $(1j)$ for $j \in \{2, \ldots, k\}$, it suffices to prove the claim for such transpositions. So let $\sigma = (1j)$; then,

$$\prod_{i=1}^{k} z_{a_i b_i} - \prod_{i=1}^{k} z_{a_i b_{\sigma(i)}} = \left(\prod_{i \in [k], i \neq 1, j} z_{a_i b_i} \right) \left(z_{a_1 b_1} z_{a_j b_j} - z_{a_1 b_j} z_{a_j b_1} \right).$$

There are several possibilities for the indices: if $a_1 = b_1 = 0, a_j b_j = 1$ or $a_1 = b_j = 0, a_j = b_1 = 1$, then indeed the RHS is an element of $T = \langle z_{00} z_{11} - z_{01} z_{10} \rangle$. The only other cases are that $a_1 = a_j$ or $b_1 = b_j$, in which case the RHS is 0. Thus in all cases, we have that these two products differ by an element of T, and so indeed $S + T = M$ (general elements are just sums of monomials, and we've shown that all monomials can be decomposed into a sum of two elements from S, T). Thus, by the **kernel lemma**, $\ker \phi = T = \langle z_{00} z_{11} - z_{01} z_{10} \rangle$.

Problem 5

Problem 6

Let $A = k[t]$, $B = k[x,y] \big/ \langle y^2 - x^2(x+1) \rangle$ and $C = k[x,y] \big/ \langle y^2 - x^3 \rangle$. Let these two ideals in the "denominators" respectively be I_B and I_C. We want to show that B and C can be embedded into A as k-algebras. Our method will be to define k-algebra homomorphisms $\varphi_B, \varphi_C : k[x,y] \to k[t]$ with respective kernels I_B, I_C so that the first isomorphism theorem gives that $B \xrightarrow{\sim} \operatorname{im}(\varphi_B) \subseteq A$ and similarly $C \xrightarrow{\sim} \operatorname{im}(\varphi_C) \subseteq A$.

Let us define φ_B by $x \mapsto t^2 - 1$ and $y \mapsto t(t^2 - 1)$, so then any $p(x,y) \in k[x,y]$ gets mapped to $p(t^2 - 1, t(t^2 - 1)) \in k[t]$; in essence we are trying to parameterize the curve $y^2 - x^2(x+1)$ (that's how to come up with the values to which we map x, y). Writing the map this way makes it trivial to check that $\varphi(f + g) = \varphi(f) + \varphi(g)$, $\varphi(fg) = \varphi(f)\varphi(g)$, and $\varphi(\lambda f) = \lambda \varphi(f)$ for any $f, g \in k[x,y]$ and $\lambda \in k$. Obviously, we have $I_B \subseteq \ker \varphi_B$ because $\varphi_B(y^2 - x^2(x+1)) = t^2(t^2-1)^2 - (t^2-1)^2(t^2 - 1 + 1) = 0$. For the other direction of inclusion, note that $y^2 = x^3 + x^2$ in B, so everything with $y^2, y^3, \ldots$ can be replaced with x's, and so any $p(x,y) + I_B \in B$ can be written as $yg(x) + h(x) + I_B$. Now suppose that this is in $\ker \varphi_B$. Then,

$$t(t^2 - 1) g(t^2 - 1) + h(t^2 - 1) = 0,$$

where the degree of the left term is $2a + 3$ for some $a \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ if $g \neq 0$ and the degree of the right term is $2b$ for some $b \in \mathbb{N}_0$ if $h \neq 0$. One is odd and one is even, and hence can not add up to 0, meaning that $g = h = 0$, proving that there is nothing in the kernel outside of I_B, i.e. $\ker \varphi_B \subseteq I_B$. Again, as advertised, the first isomorphism theorem gives that $B \simeq k[t^2 - 1, t(t^2 - 1)] \subseteq k[t]$.

The scenario with C follows in much the same way. Let us define φ_C by $x \mapsto t^2$ and $y \mapsto t^3$, so then any $p(x,y) \in k[x,y]$ gets mapped to $p(t^2, t^3) \in k[t]$. Writing the map this way makes it trivial to check that $\varphi(f + g) = \varphi(f) + \varphi(g)$, $\varphi(fg) = \varphi(f)\varphi(g)$, and $\varphi(\lambda f) = \lambda \varphi(f)$ for any $f, g \in k[x,y]$ and $\lambda \in k$. Obviously, we have $I_C \subseteq \ker \varphi_C$ because $\varphi_B(y^2 - x^3) = t^6 - t^6 = 0$. For the other direction of inclusion, note that $y^2 = x^3$ in C, so everything with $y^2, y^3, \ldots$ can be replaced with x's, and so any

$p(x, y) + I_C \in C$ can be written as $yg(x) + h(x) + I_C$. Now suppose that this is in $\ker \varphi_C$. Then,

$$t^3 g(t^2) + h(t^2) = 0,$$

where the degree of the left term is $2a + 3$ for some $a \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ if $g \neq 0$ and the degree of the right term is $2b$ for some $b \in \mathbb{N}_0$ if $h \neq 0$. One is odd and one is even, and hence can not add up to 0, meaning that $g = h = 0$, proving that there is nothing in the kernel outside of I_C, i.e. $\ker \varphi_C \subseteq I_C$. Again, as advertised, the first isomorphism theorem gives that $C \simeq k[t^2, t^3] \subseteq k[t]$.

506 Homework 3

Daniel Rui - 4/20/21

Problem 1

Chinese remainder theorem: let $I_1, \ldots, I_r \trianglelefteq A$ be a set of ideals in a commutative ring A. We define $\chi : A \to A/I_1 \times \ldots \times A/I_r$ to be the combination of natural morphisms to each of the quotient rings A/I_i.

(a) We want to show that $\ker \chi = I_1 \cap \ldots \cap I_r$. Well, we have that $\chi = (\chi_1, \ldots, \chi_r)$ where $\chi_i : A \to A/I_i$ is the map $a \mapsto a + I_i$. Thus, $\chi(a) = 0 \iff \chi_i(a) = 0$ for all $i \in [r] \iff a + I_i$ for all $i \in [r] \iff a \in I_i$ for all $i \in [r] \iff a \in I_1 \cap \ldots \cap I_r$, and we are done.

(b) For the remainder of this problem, we assume that $I_i + I_j := \langle I, J \rangle := \{a_1 i_1 + a_2 i_2 : a_1, a_2 \in A$ $i_1 \in I_i, i_2 \in I_j\} = A$ for all $i \neq j$ (i.e. they are all *comaximal*). We want to prove that $I_1 \cap \ldots \cap I_r = I_1 \cdots I_r := \{\sum x_1 \cdots x_r : x_i \in I_i\}$. The ($\supseteq$) direction is given by the fact that any product $x_1 \cdots x_r$, $x_i \in I_i$ is in the intersection $I_1 \cap \ldots I_r$ (since each I_i is an ideal, if $x_i \in I_i$ and $a \in A$ arbitrary, $ax_i \in I_i$ too), and because the intersection is an ideal and hence is closed under taking sums. For the ($\subseteq$) direction, it suffices to prove the claim for two ideals, say I_1, I_2 (can extend to r ideals by induction). So we want to prove that $I_1 \cap I_2 \subseteq I_1 I_2 := \{\sum x_1 x_2 : x_i \in I_i\}$. By comaximality, there is $x_1 \in I_1$ and $x_2 \in I_2$ s.t. $x_1 + x_2 = 1$, so for any $x \in I_1 \cap I_2$, $x = x_1 x + x x_2$ is of the form $\sum x_1 x_2$ and hence in $I_1 I_2$.

Last remarks: comaximality holds in the induction because if I_1, I_2, I_3 are all pairwise comaximal, then $I_1 \cap I_2 = I_1 I_2$ and I_3 are comaximal because we know there exist $x_i \in I_i$ s.t. $x_1 + x_3 = x_2 + x_3' = x_1' + x_2' = 1 \implies (x_1 x_2' + x_2 x_1') + (x_3 x_2' + x_3' x_1') = 1$, i.e. we've found an element of $I_1 I_2$ and I_3 that sum to 1. Can use this one result to prove if $I_1, \ldots, I_k$ are all pairwise comaximal, then $I_1 \cdots I_{k-1}$ and I_k are comaximal (i.e. $I_1, \ldots, I_k$ all comax $\implies I_1 I_2, I_3, \ldots, I_k$ all comax (just consider all triples (I_1, I_2, I_i)) $\implies I_1 I_2 I_3, I_4, \ldots, I_k$ all comax (consider triples $(I_1 I_2, I_3, I_i)$), etc.).

(c) We want to prove that χ is surjective. We proceed by induction on r. The base case $r = 1$ is trivial. Now suppose we have that $\chi_{r-1} : A \to A/I_1 \times \ldots \times A/I_{r-1}$ is surjective. We know from part (a) that the kernel of this is $I_1 \cap \ldots \cap I_{r-1} = I_1 \cdots I_{r-1}$. Now suppose we have χ_r and an element $\Lambda_r := (a_1 + I_1, \ldots, a_r + I_r) \in A/I_1 \times \ldots \times A/I_r$. By the previous sentences, we know that $\chi_r^{-1}(\Lambda_r) \subseteq \chi_{r-1}^{-1}(\Lambda_{r-1}) = b + I_1 \cdots I_{r-1}$ for some $b \in A$ and where $\Lambda_{r-1} := (a_1 + I_1, \ldots, a_{r-1} + I_{r-1})$. Now we just need to prove that there is some element $a \in b + I_1 \cdots I_{r-1}$ s.t. $a + I_r = a_r + I_r \iff a_r - a \in I_r$. We know by comaximality of $I_1 \cdots I_{r-1}$ and I_r (see part (b) *Last remarks*) that there is some $\Sigma \in I_1 \cdots I_{r-1}$ and $x_r \in I_r$ s.t. $\Sigma + x_r = a_r - b \iff a_r - (b + \Sigma) = x_r \in I_r$. Thus, $\chi_r(b + \Sigma) = \Lambda_r$, and χ_r is indeed surjective.

(d) Finally, the 1st isomorphism theorem for rings gives us that ${}^{A}\!/_{I_1 \cdots I_r} = {}^{A}\!/_{I_1 \cap \ldots \cap I_r} = {}^{A}\!/_{\ker \chi} \simeq A/I_1 \times \ldots \times A/I_r$.

Problem 2

Let A be a commutative ring. We say that A satisfies the *ascending chain condition* (ACC) if for any ascending sequence of ideals $I_1 \subseteq I_2 \subseteq \ldots \subseteq A$ there exists an $n \in \mathbb{N}$ s.t. $I_n = I_{n+1} = \ldots$; we also use the word *Noetherian* to describe a commutative ring satisfying the ACC. One can think of the ACC as a "finiteness condition", perhaps in a similar philosophy to "compactness" in topology. We want to show that A is Noetherian if and only if every ideal in A is finitely generated.

($\implies$): suppose not; i.e. suppose that there is some ideal I of A that is not finitely generated. Then, let S be a generating set of I, so $I = \langle S \rangle$. We know S must in particular be infinite, so say $S = \{a_1, a_2, \ldots\}$. Then, consider the ascending sequence of ideals $\langle a_1 \rangle \subseteq \langle a_1, a_2 \rangle \subseteq \ldots \subseteq I$. But the ACC says that there exists an $N \in \mathbb{N}$ s.t. $\langle a_1, \ldots, a_N \rangle = \langle a_1, \ldots, a_{N+1} \rangle = \ldots$, or in other words, for $n \geq N$, $a_n \in \langle a_1, \ldots, a_N \rangle$. But then $I = \langle S \rangle$ must be contained in $\langle a_1, \ldots, a_N \rangle$, and taking into account the fact that obviously $\langle a_1, \ldots, a_N \rangle \subseteq \langle S \rangle = I$, we must have that $I = \langle a_1, \ldots, a_N \rangle$, contradicting that I is not finitely generated.

($\impliedby$): suppose we have an ascending sequence of ideals $I_1 \subseteq I_2 \subseteq \ldots \subseteq A$. Define I to be the ideal $\bigcup_{n=1}^{\infty} I_n$. Because we are assuming that all ideals of A are finitely generated, I is generated by say $\{a_1, \ldots, a_k\}$. By the definition of I as an infinite union, we know that for each a_i, there must be some $n_i \in \mathbb{N}$ s.t. $a_i \in I_{n_i}$ (and hence in all subsequent I_n's). Take $N := \max_{i \in [k]} n_i$; then for all $n \geq N$, I_n contains $a_1, \ldots, a_k$, and hence $n \geq N \implies I_n = \langle a_1, \ldots, a_k \rangle$ (since we already know $I_n \subseteq \bigcup_{n=1}^{\infty} I_n = \langle a_1, \ldots, a_k \rangle$), and so the ACC holds.

Problem 3

We want to give an example of a non-Noetherian commutative ring A s.t. $A_{\mathfrak{p}}$ is Noetherian for every prime ideal $\mathfrak{p} \lhd A$. Recall (from Lec 5 of 4/7/21) that $A_{\mathfrak{p}}$ is defined as the localization $S^{-1}A$ for the multiplicative set $S = A \setminus \mathfrak{p}$, and furthermore that $A_{\mathfrak{p}}$ is a local ring with unique maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$, because $A_{\mathfrak{p}}$ consists of all fractions $\frac{a}{b}$ for $a \in A$ and $b \in S = A \setminus \mathfrak{p}$ and if I is an ideal of $A_{\mathfrak{p}}$ s.t. $I \not\subseteq \mathfrak{p}A_{\mathfrak{p}}$, then there is some fraction $\frac{a}{b} \in I$ s.t. $a, b \in A \setminus \mathfrak{p}$, meaning that $\frac{b}{a}$ is also a valid fraction in $A_{\mathfrak{p}}$, but $\frac{a}{b} \cdot \frac{b}{a} = 1$, meaning that I contains a unit, meaning that $I = A_{\mathfrak{p}}$; this shows that the only proper ideals of $A_{\mathfrak{p}}$ are contained in $\mathfrak{p}A_{\mathfrak{p}}$, thus proving both uniqueness and maximality.

We will prove the following facts: $\textcircled{1}$ if A is a boolean ring (i.e. every element $a \in A$ satisfies $a^2 = a$), then for any prime ideal $\mathfrak{p} \lhd A$, $A_{\mathfrak{p}}$ is also a boolean ring; $\textcircled{2}$ a boolean ring is local if and only if it is isomorphic to (the ring/field) $\mathbb{Z}/2\mathbb{Z}$.

$\textcircled{1}$ is obvious, since we defined multiplication on the localization as $(\frac{a}{b})^2 = \frac{a}{b} \cdot \frac{a}{b} = \frac{a^2}{b^2} = \frac{a}{b}$. Before we prove $\textcircled{2}$, let us state and provide the proof of **Corollary 2.30** from Lec 8 on 4/14/21 (just for my own reference): the nilradical of a (c1-)ring A (the set of all nilpotent elements) is the intersection of all prime ideals of A. ($\subseteq$): if a is nilpotent, then we have that $a^n = 0$ for some $n \in \mathbb{N}$, so for any prime ideal $\mathfrak{p} \lhd A$, $(a^{n-1})a = 0 \in \mathfrak{p} \implies a \in \mathfrak{p}$ or $a^{n-1} \in \mathfrak{p}$; by induction, we have that $a \in \mathfrak{p}$.

($\supseteq$): suppose $a \in A$ is not nilpotent. Then, consider the multiplicative set $S = \{a^n : n \in \mathbb{N}_0 = \{0, 1, \ldots, \}\}$. Let $\mathscr{S}$ be the set of ideals $I \lhd A$ s.t. $I \cap S = \varnothing$. This set is non-empty because $(0) \in \mathscr{S}$. If we have an ascending chain $I_1 \subseteq I_2 \ldots$ of ideals in $\mathscr{S}$, then $\bigcup_{i=1}^{\infty} I_i$ will also be in $\mathscr{S}$, so by Zorn's lemma, there is a maximal element $\mathfrak{p}$. As the name suggests, $\mathfrak{p}$ is prime, as follows (proof from Prop. 2.21 in Lec 7 on 4/12/21): if $x_1, x_2 \in A \setminus \mathfrak{p}$, the ideals $J_i = \mathfrak{p} + \langle x_i \rangle$, $i = 1, 2$, strictly contain $\mathfrak{p}$, so by maximality of $\mathfrak{p}$, it must be that $J_i \cap S \neq \varnothing$, meaning that $p_i + a_i x_i \in J_i \cap S$ for some $p_1, p_2 \in \mathfrak{p}$ and $a_1, a_2 \in A$; but then because S is multiplicative, $\prod_{i=1,2}(p_i + a_i x_i) \in S$, but $\prod_{i=1,2}(p_i + a_i x_i) = (p_1 p_2 + p_1 a_2 x_2 + p_2 a_1 x_1) + a_1 a_2 x_1 x_2$, where the stuff in the parentheses is in $\mathfrak{p}$, implying that $x_1 x_2$ can not possibly be in $\mathfrak{p}$, as desired.

One more **baby lemma**: if a boolean ring A is an integral domain, it must be isomorphic to $\mathbb{Z}/2\mathbb{Z}$, because $a^2 = a \implies a(a-1) = 0 \implies a = 0$ or $a = 1$, meaning every element in A is either 0 or 1, so A must be $\simeq \mathbb{Z}/2\mathbb{Z}$. This yields a **baby corollary**: every prime ideal in a Boolean ring is also a maximal ideal, because A boolean $\implies A/\mathfrak{p}$ boolean, but $\mathfrak{p}$ prime $\implies A/\mathfrak{p}$ integral domain, so the baby lemma tells us that $A/\mathfrak{p} \simeq \mathbb{Z}/2\mathbb{Z}$, but $\mathbb{Z}/2\mathbb{Z}$ is also a field, so $\mathfrak{p}$ must be maximal.

Now to prove $\textcircled{2}$. ($\implies$): if A is boolean and local, it has a unique maximal ideal $\mathfrak{m}$. From the baby corollary, it must be that $\mathfrak{m}$ is the unique prime ideal of A. Above we proved that the nilradical equals the intersection of all prime ideals, so in fact $\mathfrak{m}$ in this case must equal the nilradical. But in a boolean ring, we have by induction that $a^2 = a \implies a^n = a$ for all $n \in \mathbb{N}$, so in fact the nilradical is exactly 0! Thus, $A \simeq A/\mathfrak{m}$ is a field hence integral domain, and so $A \simeq \mathbb{Z}/2\mathbb{Z}$ by the baby lemma. ($\impliedby$): $\mathbb{Z}/2\mathbb{Z}$ has exactly one proper ideal, (0).

With $\textcircled{2}$ proven, we just need to find some boolean ring A that is not Noetherian, since for any prime ideal $\mathfrak{p} \lhd A$, $A_{\mathfrak{p}} \simeq \mathbb{Z}/2\mathbb{Z}$ which is finite hence Noetherian. Consider $A := \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$. This is clearly a commutative unital boolean ring, so we just need to find an ascending chain of ideals that does not plateau. Easy; take:

$$\langle (1, 0, 0, \ldots) \rangle \subseteq \langle (1, 0, 0, \ldots), (0, 1, 0, \ldots) \rangle \subseteq \ldots$$

where at stage n we add $(0, \ldots, 0, 1, 0, \ldots)$ where the 1 is in the nth spot.

Problem 4

Let A be a commutative ring. We say that A satisfies the *descending chain condition* (DCC) if for any descending sequence of ideals $A \supseteq I_1 \supseteq I_2 \supseteq \ldots$ there exists an $n \in \mathbb{N}$ s.t. $I_n = I_{n+1} = \ldots$; we also use the word *Artinian* to describe a commutative ring satisfying the DCC. We want to prove that an Artinian integral domain is a field. Note that if A is Noetherian/Artinian, then for any ideal $\mathfrak{a} \trianglelefteq A$, $A/\mathfrak{a}$ is also Noetherian/Artinian since any ascending/descending sequence $I_1 + \mathfrak{a}, I_2 + \mathfrak{a}, \ldots$ of $A/\mathfrak{a}$ pulls back to an ascending/descending sequence $I_1, I_2, \ldots$ of A; thus for any Artinian ring A and prime ideal $\mathfrak{p} \lhd A$, $A/\mathfrak{p}$ is an Artinian integral domain hence field, implying that $\mathfrak{p}$ is also maximal, i.e. all prime ideals are maximal.

This in particular gives that the Krull dimension of an Artinian ring is 0, because there is no chain of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$ of length $n > 0$ since all prime ideals are maximal.

Alright, so suppose we have an Artinian integral domain A. To show that A is a field, we just need to find an inverse to every non-zero element $a \in A$. Consider the descending chain of ideals $\langle a \rangle \supseteq \langle a^2 \rangle \supseteq \langle a^3 \rangle \supseteq \ldots$; the DCC tells us that there is some $n \in \mathbb{N}$ s.t. $\langle a^n \rangle = \langle a^{n+1} \rangle = \ldots$, or said another way $a^n \in \langle a^{n+1} \rangle \iff$ there is $b \in A$ s.t. $a^n = ba^{n+1}$. Because a is non-zero and A is an integral domain, we can use the cancellation property to see that $1 = ba$, i.e. b is the inverse to a (in a commutative setting left and right do not matter).

Problem 5

We want to prove that an Artinian ring only has a finite number of prime ideals. Consider the set $\mathscr{S}$ of ideals that are the intersections of finitely many prime ideals. There must be minimal elements of this set, because if not, then for any $I_n \in \mathscr{S}$, we can find $I_{n+1} \in \mathscr{S}$ s.t. $I_n \supsetneq I_{n+1}$, implying that we have a non-plateauing descending chain $I_1 \supsetneq I_2 \supsetneq \ldots$ contradicting the DCC.

Moreover, there must only be one minimal element because if I and I' are minimal in $\mathscr{S}$, then $I \cap I'$ is also a finite intersection of prime ideals which is a subset of I and I', implying that $I \cap I' = I$ and $I \cap I' = I'$, i.e. $I = I'$. So let $\mathfrak{n}$ be *the* minimal element of $\mathscr{S}$ ($\mathfrak{n}$ for mi$\underline{\text{n}}$imal), say $\mathfrak{n} = \bigcap_{i=1}^n \mathfrak{p}_i$ for some prime ideals $\mathfrak{p}_i$.

Now suppose that $\mathfrak{p}$ is some prime ideal in A. Clearly, $\mathfrak{p} \in \mathscr{S}$, so $\mathfrak{p} \supseteq \mathfrak{n} = \bigcap_{i=1}^n \mathfrak{p}_i$. It turns out that if this intersection is in $\mathfrak{p}$, then there is some $\mathfrak{p}_i$ for $i \in [n]$ s.t. $\mathfrak{p} \supseteq \mathfrak{p}_i$. By induction, it suffices to show that if $I_1 \cap I_2 \subseteq \mathfrak{p}$ for some arbitrary ideals I_1, I_2 and prime ideal $\mathfrak{p}$, then $I_1 \subseteq \mathfrak{p}$ or $I_2 \subseteq \mathfrak{p}$. This is actually super easy: if $I_1 \subseteq \mathfrak{p}$, we're done, so assume that there is some $x \in I_1 \setminus \mathfrak{p}$; then for any $y \in I_2$, $xy \in I_1 \cap I_2 \subseteq \mathfrak{p} \implies x \in \mathfrak{p}$ or $y \in \mathfrak{p}$, but since we specified $x \notin \mathfrak{p}$, it must be that $y \in \mathfrak{p}$, and because $y \in I_2$ was arbitrary, we have that $I_2 \subseteq \mathfrak{p}$.

But recall from Problem 4 that all prime ideals of an Artinian ring are maximal, so $\mathfrak{p} \supseteq \mathfrak{p}_i \implies \mathfrak{p} = \mathfrak{p}_i$, so indeed all prime ideals of A are one of $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, which is a finite set as desired.

Problem 6

Let A be an Artinian ring. We want to prove using the DCC that the nilradical of A is nilpotent, i.e. there exists $n \in \mathbb{N}$ s.t. $(\sqrt{0})^n = 0$. Let $\mathfrak{n}$ denote the nilradical $\sqrt{0}$ (yes, it is the same $\mathfrak{n}$ as in Problem 5, since we proved in Problem 3 that the nilradical is the intersection of all prime ideals!). We can now construct the following descending chain: $\mathfrak{n} \supseteq \mathfrak{n}^2 \supseteq \mathfrak{n}^3 \supseteq \ldots$, which must by the DCC satisfy $\mathfrak{n}^N = \mathfrak{n}^{N+1} = \ldots$ for some $N \in \mathbb{N}$. Suppose now that $\mathfrak{n}^N \neq 0$ (i.e. the descending chain stabilizes not at 0, so there is no $n \in \mathbb{N}$ s.t. $\mathfrak{n}^n = 0$).

Define $\mathscr{S}$ to be the set of ideals $I \lhd A$ s.t. $I\mathfrak{n}^N \neq 0$ (note that $\mathfrak{n} \in \mathscr{S}$). By the same argument from Problem 5, $\mathscr{S}$ must have a minimal element (reminder: if there's no minimal element, we can get a descending chain that does not plateau), say $\mathfrak{a} \lhd A$. By the condition we placed on $\mathscr{S}$, $\mathfrak{a}\mathfrak{n}^N \neq 0$, so in fact there must exist some $a \in \mathfrak{a}$ s.t. $a\mathfrak{n}^N \neq 0$. Then, the ideal $\langle a \rangle$ must be in $\mathscr{S}$ too, and because $\langle a \rangle \subseteq \mathfrak{a}$, $\langle a \rangle$ must equal $\mathfrak{a}$ by minimality of $\mathfrak{a}$.

Now because $\mathfrak{n}^N = \mathfrak{n}^{N+1}$, we have that $a\mathfrak{n}^{N+1} \neq 0$ as well, meaning that there is some $x \in \mathfrak{n}$ s.t. $ax\mathfrak{n}^N \neq 0$, or equivalently $\langle ax \rangle \mathfrak{n}^N \neq 0$. But $\langle ax \rangle \subseteq \langle a \rangle = \mathfrak{a}$, so again by minimality, we must have $\langle ax \rangle = \langle a \rangle$. This means that there is some $b \in A$ s.t. $axb = a$, and so by induction $a = a(xb)^n$ for all $n \in \mathbb{N}$. But recall that $x \in \mathfrak{n}$, so $bx \in \mathfrak{n}$, implying that there is some $n \in \mathbb{N}$ s.t. $(bx)^n = 0$! That is to say, a must be 0! However, this contradicts what we specified earlier, about $a\mathfrak{n}^N \neq 0$, and so in fact it can not be that $n^N \neq 0$. QED.

506 Homework 2

Daniel Rui - 4/13/21 (actually 4/16/21)

Let M be a module over a ring. An *essential extension* of M is a module N that contains M as a submodule s.t. for any non-zero submodule $L \subseteq N$ it's true that $M \cap L \neq 0$. Obviously, we have that $M \subseteq M$ is an essential extension; this is called the *trivial essential extension*.

The *projective dimension* of a module is defined as the shortest length of a projective resolution.

Also, recall that A-module I being injective means that the functor $\operatorname{Hom}_A(-, I)$ is exact. Remember that $\operatorname{Hom}_A(-, M)$ is a contravariant left exact functor (i.e. sends exact sequences $B \xrightarrow{f} C \xrightarrow{g} D \to 0$ to $0 \to \operatorname{Hom}(D, M) \xrightarrow{-\circ g} \operatorname{Hom}(C, M) \xrightarrow{-\circ f} \operatorname{Hom}(B, M)$), so indeed $\operatorname{Hom}_A(-, I)$ being exact is equivalent to $[f : B \to C$ injective $\implies - \circ f$ is a surjective map $\operatorname{Hom}(C, I) \to \operatorname{Hom}(B, I)]$, or in other words we have what **I will refer to as the "triangle diagram"**:

$$\begin{tikzcd}
B \arrow[r, hook, "f"] \arrow[d] & C \arrow[dl, dashed, "\exists"] \\
I &
\end{tikzcd}.$$

Problem 0, Extra Credit Problem 1 (PROVEN AT END!)

We want to prove the following major theorem: for any A-module M, there is an injective A-module I s.t. $M \hookrightarrow I$. Admitted.

Take a look at the following: https://www3.nd.edu/~sevens/injectives.pdf, which offers a worksheet-like walkthrough; https://sites.math.washington.edu/~mitchell/Algh/chung.pdf, which is quite thorough; and http://www.math.leidenuniv.nl/~edix/tag_2009/michiel_2.pdf, which I think covers the same ground as Chung (but of course two presentations always better than one!). One thing I got caught up on was that R-modules are automatically $\mathbb{Z}$-modules (pg. 2 of http://www.math.ucsd.edu/~jmckerna/Teaching/15-16/Winter/100B/l_11.pdf).

Problem 1

We want to show that a module has no non-trivial essential extensions if and only if it is an injective module.

($\Longleftarrow$): suppose we have an injective module M and essential extension N of M. That means we have an injective map $\iota : M \hookrightarrow N$. Since M is injective, we can use the triangle diagram (see intro section) to see that $\mathrm{id}_M : M \to M$ extends to some map $s : N \to M$ s.t. $s \circ \iota = \mathrm{id}_M$. This is exactly what it means for ι to split, so indeed we have just proved that for an injective module I, every injective homomorphism $I \hookrightarrow M$ into some arbitrary module M splits.

In fact this property of injective maps splitting is all we need to prove that M (the one we "initialized" in the first sentence of the above paragraph) has no non-trivial essential extensions. This is because if we have $\iota : M \hookrightarrow N$ and $s : N \to M$ s.t. $s \circ \iota = \mathrm{id}_M$, then obviously s must be surjective, but also we see that s must be injective since if $\ker s$ is a non-zero submodule of N, then by definition of essential extension, $M \cap \ker s \neq 0$, implying that there exists $m \in M$ s.t. $s(m) = 0$, which contradicts that $s \circ \iota = \mathrm{id}_M$ (recall $M \subseteq N \implies \iota : M \hookrightarrow N$ is defined as $m \mapsto m$). Thus, s is a bijective homomorphism $N \to M$, meaning $M \simeq N$.

($\implies$): suppose we have an A-module M that has no non-trivial essential extensions. We will use the fact from Problem 0 that there is some injective A-module I s.t. $M \hookrightarrow I$. Let us just think of things as $M \subseteq I$ just so we don't have to be picky with our notation regarding isomorphic copies. I a moment, we will show that there is some "maximal" submodule N of I s.t. $M \cap N = 0$. Supposing we have this fact, then the injective map $M \hookrightarrow I$ will induce another injective map $M \hookrightarrow I/N$ (so $M + N \subseteq I/N$).

I claim that I/N is an essential extension of M: suppose we have a submodule of I/N — we know by the 3rd isomorphism theorem for modules that such a submodule is of the form L/N for some $N \subseteq L \subseteq I$ — s.t. $L/N \cap M + N = 0$; then $L \cap M = 0$, and so by maximality of N, $L = N$, i.e. the submodule of I/N with zero intersection with $M + N$ must have been the zero submodule. Since we said at the beginning that M had no non-trivial essential extensions, it must be that $M \simeq I/N$ (or $M + N = I/N$).

Then I claim that $I \simeq M \oplus N$: consider the maps $\varphi : I/N \oplus N \to I$ defined as $(i + N, n) \mapsto m + n$ (where m is the unique $m \in M$ s.t. $m+N = i+N$) and $\psi : I \to I/N \oplus N$ defined as $i \mapsto (i+N, i-m)$. It is clear that these maps are the inverses of each other. Lec 4 on 4/5/21 states that a direct sum of two modules is injective iff each of those two modules is injective (($\impliedby$) is given by the isomorphism $\mathrm{Hom}(-, M \oplus N) \simeq \mathrm{Hom}(-, M) \oplus \mathrm{Hom}(-, N)$ where the backwards map is $(f, g) \mapsto [- \mapsto (f(-), g(-))]$, and ($\implies$) is true because for any $f : B \hookrightarrow C$, and $\phi : B \to I$, we can define $\phi' : B \to I \oplus J$ by $b \mapsto (\phi(b), 0)$, and the triangle diagram gives that there is some $\psi' : C \to I \oplus J$ s.t. $\phi' = \psi' \circ f$, implying that $\psi : C \to I$ defined by $c \mapsto \pi_1(\psi'(c))$ satisfies $\phi = \psi \circ f$). This result gives finally that because $I \simeq M \oplus N$ is injective, M must be as well.

We are not done yet! We still have to prove the existence of the "maximal" submodule N of I s.t. $M \cap N = 0$. This is just an easy application of . We just need to show that there's an upper bound for every chain. Suppose we have $N_1 \subseteq N_2 \subseteq \ldots$ s.t. $M \cap N_i = 0$. Then, it is clear that $M \cap \bigcup_{i=1}^{\infty} N_i$ must also be 0. Thus, we have found an upper bound $\bigcup_{i=1}^{\infty} N_i$ for every chain $N_1 \subseteq N_2 \subseteq \ldots$, and so Zorn's lemma tells us there must exist some maximal submodule $N \subseteq I$ s.t. $M \cap N = 0$, and we are finally finished.

Remark: note that we have actually proved that M injective $\iff$ any injective map $M \hookrightarrow N$ splits, by showing M injective $\implies$ $M \hookrightarrow N$ splits $\implies$ M has no non-trivial ess. ext. $\implies$ M injective.

Problem 2

We want to prove that every module M has a unique (up to isomorphism) maximal essential extension. This (isomorphism class of such a) module is called the *injective hull* and is denoted $E(M)$. For ease, we will adopt the notation $M \subseteq_{\text{ess}} N$ for N is an essential extension of M.

We first prove that $M \subseteq_{\text{ess}} L \iff M \subseteq_{\text{ess}} N$ and $N \subseteq_{\text{ess}} L$ for any modules $M \subseteq N \subseteq L$. ($\Longrightarrow$): suppose there was a non-zero submodule S of N s.t. $S \cap M = 0$. Then since $S \subseteq L$, this contradicts that $M \subseteq_{\text{ess}} L$. If there was a non-zero submodule S of L s.t. $S \cap N = 0$, then since $M \subseteq N$, $S \cap M$ would also have to be 0, again contradiction. ($\Longleftarrow$): suppose that we are given some non-zero submodule $S \subseteq L$. Well we know by $N \subseteq_{\text{ess}} L$ that $S \cap N \neq 0$. This is a non-zero submodule of N, so by $M \subseteq_{\text{ess}} N$, it must be that $(S \cap N) \cap M \neq 0$. But $(S \cap N) \cap M = S \cap M$, so $S \cap M \neq 0$.

We also prove that for $M \subseteq N$, N is an essential extension of $M \iff$ for all non-zero $n \in N$, $An \cap M \neq 0$. ($\Longrightarrow$) is obvious since An is indeed a submodule of N. ($\Longleftarrow$): suppose S is a non-zero submodule of N s.t. $S \cap M = 0$. Since $S \subseteq N$ is non-zero, there is some non-zero $n \in N$ also in S; then $An \cap M$ would have to be 0 since $An \subseteq S$; contradiction. This result and the one in the paragraph above will be referred to resp. as **baby lemma 2** and **baby lemma 1**.

We are now ready to use Zorn's lemma to prove that there is a maximal essential extension. Suppose we have $N_1, N_2, \dots$ that are all essential extensions of M, s.t. $N_1 \subseteq N_2 \subseteq \dots$. Then, $E(M) := \bigcup_{i=1}^{\infty} N_i$ is also an essential extension (for any $n \in \bigcup_{i=1}^{\infty} N_i$, it's in some N_i, and by the 2nd baby lemma, it must be that $An \cap M \neq 0$). Thus, all chains have an upper bound, and Zorn's lemma tells us there must exist a maximal essential extension.

From the 1st baby lemma, we know that any essential extension of $E(M)$ would also be an essential extension of M containing N, so by maximality it must be that N has no non-trivial essential extensions. By Problem 1, we have that N is an injective module. Since we have $E(M)$ is an essential extension of M, we obviously have an injection $\iota : M \hookrightarrow E(M)$. We now want to prove that for any embedding $j : M \hookrightarrow I$ for an injective module I, there is an embedding $\ell : E(M) \hookrightarrow I$ s.t. $j = \ell \circ \iota$.

Let us repeat the argument we made earlier with Zorn's lemma, but now restricting ourselves to only consider essential extensions of M (or I guess an isomorphic copy of M, $\tilde{M} \subseteq I$) INSIDE I. A union of submodules of I is still a submodule of I, so indeed all chains of essential extensions of M inside I have an upper bound, so there is some maximal element $E_I(M)$. We show that $E_I(M)$ is maximal in general (i.e. not just in I): suppose that we have some essential extension N of M that contains $E_I(M)$; then we would have an inclusion $f : E_I(M) \hookrightarrow N$. Because I is injective, the inclusion $i : E_I(M) \to I$ can be extended to some map $g : N \to I$ s.t. $i = g \circ f$ (see the triangle diagram). Because $M \subseteq_{\text{ess}} N$, supposing $\ker g$ is non-zero, we have that $\ker g \cap M \neq 0$. But then that would mean that for some non-zero $m \in \ker g \cap M$, i would map $m \mapsto m$ of course but $g \circ f$ would map $m \mapsto m \mapsto 0$, contradiction $i = g \circ f$. Thus, it must be that $\ker g = 0$, i.e. g is injective, i.e. $N \hookrightarrow I$, i.e. N is also a submodule in I hence N must equal $E_I(M)$.

This almost proves the claim; we just need to prove that any maximal essential extensions of M are isomorphic (so then we can just put $E(M)$ in place of $E_I(M)$ above). Well, suppose we have N_1, N_2 both maximal essential extensions of M (so in particular they are injective modules). Then by injectivity of N_2 and the inclusion map $M \hookrightarrow N_1$, the inclusion map $M \hookrightarrow N_2$ can be extended to a map $g : N_1 \to N_2$ that is the identity on M. The same argument from the end of the previous paragraph tells us that $\ker g = 0 \iff g$ is injective. So now we have $M \subseteq N_1 \subseteq N_2$. We know from the end of Problem 1 that N_1 injective means that the map $g : N_1 \hookrightarrow N_2$ splits, i.e. we have $s : N_2 \to N_1$ s.t. $s \circ g = \mathrm{id}_{N_1}$. Applying the same argument from 1st paragraph of the 2nd page of Problem 1, we see that $N_1 \simeq N_2$.

Problem 3

We want to prove that an abelian group G, i.e. $\mathbb{Z}$-module M is divisible if and only if M is injective, where M being divisible means that for every non-zero $n \in \mathbb{Z}$ and $m \in M$, there is some $m' \in M$ s.t. $nm' = m$. Here's the plan. We reprove the claim I proved in Problem 1 (assuming Problem 0) that I injective $\iff$ every $I \hookrightarrow M$ splits, this time without assuming Problem 0; then we prove Baer's lemma; and then we finally get to the problem.

I injective $\iff$ every $I \hookrightarrow -$ splits: ($\implies$) was proved in the 1st page of Problem 1. Now for ($\impliedby$). Suppose we have $f : M \hookrightarrow N$ and a map $\varphi : M \to I$, like in the triangle diagram. Consider the submodule $S \subseteq N \oplus I$ defined as $S := \{(f(m), -\varphi(m)) : m \in M\}$; since $N \oplus I$ is an abelian group (w.r.t. $+$), S is a normal subgroup and we can quotient giving us $M' := {}^{N \oplus I}/_{S}$. Let ι_1, ι_2 be maps from N and I resp. to M', defined in the obvious fashion as $\iota_1(n) = (n, 0) + S$ and $\iota_2(i) = (0, i) + S$. Note that because f is injective, ι_2 is also injective: $(0, i) + S = (0, 0) + S \implies (f(m), i - \varphi(m)) = (0, 0) \implies f(m) = 0 \implies m = 0 \implies i = i - \varphi(m) = 0$. Furthermore, from the definitions of ι_1, ι_2, we have that following square is commutative (right then down yields $m \mapsto f(m) \mapsto (f(m), 0) + S$, and down then right yields $m \mapsto \varphi(m) \mapsto (0, \varphi(m)) + S$ and by definition of S these two cosets are the same):

$$\begin{tikzcd}
M \arrow[r, hook, "f"] \arrow[d, "\varphi"'] & N \arrow[d, "\iota_1"] \\
I \arrow[r, hook, "\iota_2"'] & {}^{N \oplus I}/_{S}
\end{tikzcd}$$

Because $\iota_2 : I \hookrightarrow M'$ is injective, the splitting condition gives that there is $s : M' \to I$ s.t. $s \circ \iota_2 = \mathrm{id}_I$. We can now define $\psi : N \to I$ as $\psi = s \circ \iota_1$ and verify: $\psi \circ f = s \circ \iota_1 \circ f = s \circ \iota_2 \circ \varphi = \mathrm{id}_I \circ \varphi = \varphi$.

Baer's lemma states that an A-module M is injective $\iff$ we show the triangle diagram holds for all injections $f : \mathfrak{a} \hookrightarrow A$ for ideals $\mathfrak{a} \subseteq A$. The ($\implies$) direction is obvious. Now suppose have some modules M, N s.t. $f : M \hookrightarrow N$ and $\varphi : M \to I$. For ease, let's just think of $M \subseteq N$ (otherwise, we would have just have more notation, nothing new conceptually: let $\tilde{M}$ be the isomorphic copy of M in L, inducing $\tilde{f}, \tilde{g} : \tilde{M} \to N, I$ s.t. $f = \tilde{f} \circ f$ (so $\tilde{f}(\tilde{m}) = \tilde{m} = f(m)$) and $\varphi = \tilde{\varphi} \circ f$, etc.).

Let us now define the set S of pairs (L, ψ_L) s.t. $M \subseteq L \subseteq N$ and ψ_L restricted to M equals φ. We equip S with the partial order $(L_1, \psi_1) \le (L_2, \psi_2) \iff L_1 \subset L_2$ and $\psi_2|_{L_1} = \psi_1$. Notice also that S is non-empty since $(M, \varphi) \in S$. Given a (non-empty) chain (L_i, ψ_i), it has the upper bound $(\bigcup_{i=1}^{\infty} L_i, \psi)$ for ψ defined as ψ_i for all $x \in L_i$ (every $l \in \bigcup_{i=1}^{\infty} L_i$ is in some L_i, and so $\psi(l)$ can be defined as $\psi_i(l)$). Thus, by Zorn's lemma, there is some maximal element (L, ψ_L). We claim that $L = N$, thus proving that there is an extension of φ to $\psi : N \to I$.

Ok, suppose $L \subsetneq N$. Then let $x \in N \backslash L$, and define the ideal $\mathfrak{a} := \{a \in A : ax \in L\} \subseteq A$. Then the triangle diagram for $\mathfrak{a} \hookrightarrow A$ and the map $a \mapsto \psi_L(ax) : \mathfrak{a} \to M$ gives that there exists a map $\xi : A \to M$ s.t. for any $a \in \mathfrak{a}$, $\xi(a) = \psi_L(ax)$. Let us now define $\psi : Ax + L \to M$ by mapping $ax + l \mapsto \xi(a) + \psi_L(l)$. First, observe that ψ is well defined: if $a_1 x + l_1 = a_2 x + l_2$, then $l_1 - l_2 = (a_2 - a_1)x \implies (a_2 - a_1) \in \mathfrak{a}$, and we verify that indeed $\psi_L(l_1 - l_2) = \xi(a_2 - a_1) = \psi_L((a_2 - a_1)x)$ since $\xi|_{\mathfrak{a}} = \psi_L(- \cdot x)$; and second, we observe that $\psi|_L = \psi_L$. Thus, we have that $(L, \psi_L) < (Ax + L, \psi)$, contradicting maximality. Thus, it must have been that $L = N$, and as promised, we are done.

We may now finally begin the problem. ($\impliedby$): suppose that M is injective. Let us fix some $m \in M$, and non-zero $n_0 \in \mathbb{Z}$. We want to find some $m' \in M$ s.t. $n_0 m' = m$. Then, multiplication by n_0 is an injective map $\mathbb{Z} \hookrightarrow \mathbb{Z}$ (because $n_0 \neq 0$ and $\mathbb{Z}$ is an integral domain). Let us now define $\varphi : \mathbb{Z} \to M$ by $n \mapsto nm$. The triangle diagram now gives us a homomorphism $\psi : \mathbb{Z} \to M$ s.t. $nm = \varphi(n) = \psi(n_0 n) = n_0 n \psi(1)$ (last equality by homomorphism properties).Thus, taking $n = 1$ and $m' = \psi(1)$, we do get that $m = n_0 m'$.

($\implies$): to show that M is injective, Baer's lemma tells us we only need to prove that the triangle diagram holds for all $\mathfrak{a} \hookrightarrow A$ for ideals $\mathfrak{a} \subseteq A$. Because $\mathbb{Z}$ is a PID, all such ideals are (n) for some $n \in \mathbb{Z}$. Suppose we are given some $n \neq 0$ (if $n = 0$, then the zero map $\mathbb{Z} \to M$ would make the triangle diagram hold), and $\varphi : (n) \to M$. By divisibility of M, we know that there must be some $m' \in M$ s.t. $nm' = \varphi(n)$. Then, defining $\psi : \mathbb{Z} \to M$ by $z \mapsto zm'$, we do indeed see that $\psi|_{(n)} = \varphi$.

Finally, we show that $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are divisible and hence injective $\mathbb{Z}$-modules. Well, $\mathbb{Q}$ is a field and hence obviously divisible. For $\mathbb{Q}/\mathbb{Z}$: let us fix non-zero $n \in \mathbb{Z}$, and some $\frac{p}{q} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. Then, $\frac{p}{nq} + Z \in \mathbb{Q}/\mathbb{Z}$ is s.t. multiplying by n gives exactly the original element, and so $\mathbb{Q}/\mathbb{Z}$ is divisible.

Problem 4

Recall that an A-module P being projective means that $\mathrm{Hom}_A(P, -)$ is exact. Similar to above in the injective case, this functor is covariant and left exact, and so its exactness is equivalent to [$f : C \to D$ surjective $\implies$ $f \circ - : \mathrm{Hom}(P, C) \to \mathrm{Hom}(P, D)$ also surjective]. There are two other equivalent definitions: ① [every surjection $M \twoheadrightarrow P$ splits], and ② [P is a direct summand of a free module]. Recall that we proved the first alternative definition in Lec 4 on 4/5/21; also in that lecture, we said that $P \oplus Q$ projective $\iff$ P, Q both projective (this is more generally true for arbitrary number of direct sums). This proves that ② implies P projective (as well as the fact that free modules are projective; since $\mathrm{Hom}_A(A, P) \sim P$, A is projective, so $\bigoplus_{i \in I} A$ is projective).

I will now prove ① $\implies$ ②. Recall from Lec 4 on 4/5/21 that for any A-module, in particular P, there is a free A-module F s.t. $\pi : F \twoheadrightarrow P$. ① tells us that this splits, so there is some homomorphism $s : P \to F$ s.t. $\pi \circ s = \mathrm{id}_P$. Then, I claim that $P \oplus \ker \pi \simeq F$, with forward map $(p, x) \mapsto s(p) + x$ and backwards map $f \mapsto (\pi(f), f - s(\pi(f)))$: composing in either order gives $(p, x) \mapsto s(p) + x \mapsto (\pi(s(p) + x), s(p) + x - s(\text{1st comp.})) = (p + 0, s(p) + x - s(p)) = (p, x)$ and $f \mapsto (\pi(f), f - s(\pi(f))) \mapsto s(\pi(f)) + f - s(\pi(f)) = f$.

In fact, the proof we just did holds for all $M \twoheadrightarrow P$, not just free modules F; i.e. if $\pi : M \twoheadrightarrow P$ splits, then $M \simeq P \oplus \ker \pi$. We will use this shortly. Call this the "splitting to direct sum fact".

Now for the problem: let P, P' be two projective modules over a (c1)-ring A and let M be an A-module. We assume that there are surjective homomorphisms $\phi : P \to M$ and $\phi' : P' \to M$. We want to prove that $P \oplus \ker \phi' \simeq P' \oplus \ker \phi$.

The condition we had above, $[f : C \twoheadrightarrow D \implies f \circ - : \mathrm{Hom}(P, C) \twoheadrightarrow \mathrm{Hom}(P, D)]$, is equivalent to having the triangle diagram:

$$\begin{tikzcd}
 & P \arrow[dl, dashed, "\exists\psi"'] \arrow[d, "\varphi"] \\
C \arrow[r, two heads, "f"'] & D
\end{tikzcd}.$$

Well, we have a surjective map $\phi : P \twoheadrightarrow M$, and a map $\phi' : P' \to M$, so the triangle diagram gives us $\psi : P' \to P$ s.t. $\phi' = \phi \circ \psi$. Let us now find a surjection $\pi : \ker \phi \oplus P' \to P$ with kernel isomorphic to $\ker \phi'$ so that we can use projectivity of P to say that π splits, and then the "splitting to direct sum fact" to prove that $\ker \phi \oplus P' = \ker \phi' \oplus P$.

Let us define π by $(k, p') \mapsto k + \psi(p')$. I claim that for every $p + \ker \phi \in {}^{P}\!/_{\ker \phi}$, there must be some $p' \in P'$ s.t. $\psi(p') - p \in \ker \phi$. Suppose not; then $\phi(\psi(p') - p) = \phi'(p') - \phi(p) \neq 0$ for all $p' \in P'$. But $\phi' : P' \to M$ is surjective and $\phi(p)$ is just some element of M, so there must be some $p' \in P'$ s.t. $\phi'(p') = \phi(p)$; contradiction. Thus, π is surjective because for any $p \in P$, I set $p' \in P'$ to be the one we just found (i.e. satisifies $p - \psi(p') \in \ker \phi$), implying there is some $k \in \ker \phi$ s.t. $p = k + \psi(p')$.

Then $\ker \pi = \{(k, p') : k \in \ker \phi, p' \in P', k = -\psi(p')\}$. Notice that $\psi(p') \in \ker \phi \iff \phi'(p') = \phi(\psi(p')) = 0 \iff p' \in \ker \phi'$, and so $\ker \pi = \{(-\psi(p'), p') : p' \in \ker \phi'\}$, which is obviously isomorphic to $\ker \phi'$. Thus, π is surjective with kernel isomorphic to $\ker \phi'$, and so we can use projectivity of P to say that π splits, and then the "splitting to direct sum fact" tells us that $\ker \phi \oplus P' = \ker \phi' \oplus P$.

Counterexample: if one of P, P' are not projective, the result may not hold. Consider $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2$ and $\phi' : \mathbb{Z} \to \mathbb{Z}^2$ (considered as $\mathbb{Z}$-modules); in this case we have $P \oplus \ker \phi' = \mathbb{Z}_4 \oplus 2\mathbb{Z} \simeq \mathbb{Z}_4 \oplus \mathbb{Z}$, and $\ker \phi \oplus \mathbb{Z} = \mathbb{Z} \oplus \mathbb{Z}_2$, but these are not isomorphic since $\mathbb{Z}_4 \oplus \mathbb{Z}$ has order-4 elements, but $\mathbb{Z} \oplus \mathbb{Z}_2$ doesn't.

Problem 5

Let P' be a finitely generated A-module and P be a free A-module (hence projective; see 1st paragraph of Problem 4) of infinite rank (so P' is generated by a finite set S' and P is free generated by an infinite set S). We assume that the following condition holds: for any A-module M, if there are surjective homomorphisms $\phi : P \to M$ and $\phi' : P' \to M$, then $P \oplus \ker \phi' \simeq P' \oplus \ker \phi$. We want to prove that P' must also be a projective module.

We show that we can take $M = P'$ in the above (so $\phi' : P' \to P'$ is the identity map) to get that $P \simeq P \oplus \ker \mathrm{id}_{P'} P' \simeq \ker \phi$, implying that because P is projective, $P', \ker \phi$ must also be projective (see Lec 4 on 4/5/21, or 1st paragraph of Problem 4).

Let us define a surjective map $\phi : P \to P'$ as follows: for every $s' \in S'$, just choose an $s \in S$ (no two s' can choose the same s, but since S is infinite and S' is finite, this are way more than enough). Then, define $\phi(s) = s'$, and extend via linearity; then, since any $p' \in P'$ can be written as $\sum_{s' \in S'} a_{s'} s'$, $\phi(\sum_{s' \in S'} a_{s'} s) = \sum_{s' \in S'} a_{s'} s' = p'$ and so indeed ϕ is surjective (here we used that P was free so that $\sum_{s' \in S'} a_{s'} s$ were not the same for different p'). Thus $\phi : P \to P'$ and $\phi' = \mathrm{id}_{P'} : P' \to P'$, so by the assumed condition, we have $P \simeq P \oplus \ker \mathrm{id}_{P'} P' \simeq \ker \phi$, implying that P' is projective as I already explained above.

In general, this proof only requires that there exist a surjection $P \to P'$ and that P is projective. The free/finitely generated stuff in this particular problem gave us that such a surjection existed, but I'm sure there are many other conditions out there that guarantee such a surjection.

Problem 0, proof (Extra Credit Problem 1)

We want to prove the following major theorem: for any A-module M, there is an injective A-module I s.t. $M \hookrightarrow I$.

Part 1: proving for $A = \mathbb{Z}$. I was very careful in making sure Problem 3 of 506hw2 did not depend on Problem 0; this is because I will use the results of Problem 3 here. So M is a $\mathbb{Z}$-module. Pick $x \in M$ non-zero and consider the inclusion map $f : \mathbb{Z}x \hookrightarrow M$. I now claim that there is a non-zero map from $\varphi : \mathbb{Z}x \to \mathbb{Q}/\mathbb{Z}$; simply take $f(x) = \frac{1}{2} + \mathbb{Z}$ or something. Then, by the triangle diagram (because we know from Problem 3 that $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module), we know that there exists a non-zero map $\psi_x : M \to \mathbb{Q}/\mathbb{Z}$ that equals φ on $\mathbb{Z}x$. Now we construct a map $\iota : M \to \prod_{\mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Q}/\mathbb{Z})} \mathbb{Q}/\mathbb{Z}$ defined by $x \mapsto (f(x))_{f \in \mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Q}/\mathbb{Z})}$. This is injective because if for all $f \in \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$, $f(x) = 0$, then it must be that $x = 0$ since if $x \neq 0$, we could find a homomorphism (say φ_x from above) that is non-zero on x.

Finally, this product of $\mathbb{Q}/\mathbb{Z}$ is also an injective $\mathbb{Z}$-module by the following **baby lemma:** $\prod_{i \in I} M_i$ is injective if and only if all the M_i are injective. This comes from the "$\mathrm{Hom}_A(-, M)$ is exact" definition of injective module, and the fact that $\mathrm{Hom}_A(-, \prod_{i\in I} M_i) = \prod_{i \in I} \mathrm{Hom}_A(-, M_i)$.

Part 2: for a c1-ring A, if P is an injective A-module and I is an injective $\mathbb{Z}$-module, then $\mathrm{Hom}_{\mathbb{Z}}(P, I)$ is an injective A-module. Not quite what Sándor wrote in the EC Problem statement, but I like this proof better. We want to show that $\mathrm{Hom}_A(-, \mathrm{Hom}_{\mathbb{Z}}(P, I))$ is exact. Recall from Lec 3 on 4/2/21 (Corollary 1.17) that $\mathrm{Hom}_A(-, \mathrm{Hom}_{\mathbb{Z}}(P, I)) \simeq \mathrm{Hom}_{\mathbb{Z}}(- \otimes_A P, I)$.

To elaborate on this, look at Lec 2 of 3/31/21 and see that the universal property of the tensor product implies that for any $\mathbb{Z}$-bilinear map $\lambda : M \times N \to L$, there is a unique map $\nu : M \otimes_A N \to L$ s.t. $\lambda = \nu \circ \otimes$; but this map ν is in fact a $\mathbb{Z}$-linear map! Thus we have that $\mathrm{BiLin}_{\mathbb{Z}}(M \times N, L) \simeq \mathrm{Hom}_{\mathbb{Z}}(M \otimes_A N, L)$. Then look at Lec 3 on 4/2/21; the maps we define between $\mathrm{BiLin}_A(M \times N, L)$ and $\mathrm{Hom}_A(M, \mathrm{Hom}_A(N, L))$, which recall were:

$$\lambda : M \times N \to L \longmapsto \Big(m \mapsto [\lambda(m, -) : N \to L]\Big)$$

$$\Big((m, n) \mapsto [\phi(m)](n)\Big) \longleftarrow\!\!\shortmid \phi : M \to \mathrm{Hom}_A(N, L)$$

can be restricted to only dealing with $\mathbb{Z}$-bilinear maps $M \times N \to L$ and $\mathbb{Z}$-linear maps $N \to L$ and still remain inverse to each other, giving us that $\mathrm{BiLin}_{\mathbb{Z}}(M \times N, L) \simeq \mathrm{Hom}_A(M, \mathrm{Hom}_{\mathbb{Z}}(N, L))$.

Back to the original train of reasoning: because P is projective A-module, $- \otimes_A P$ is exact, and because I is injective $\mathbb{Z}$-module, $\mathrm{Hom}_{\mathbb{Z}}(-, I)$ is exact, and so $\mathrm{Hom}_{\mathbb{Z}}(- \otimes_A P, I)$ must be exact as well (take in exact sequence, tensor spits out exact sequence, then hom spits out exact sequence again).

Part 3: proving for arbitrary A. We have an arbitrary c1-ring A and an A-module M. Since M is an abelian group w.r.t + and all abelian groups can be thought of as $\mathbb{Z}$-modules, M can be thought of as a $\mathbb{Z}$-module. Part 1 gives that there is an injective $\mathbb{Z}$-modules I_Z s.t. we have $\iota_Z : M \hookrightarrow I_Z$. Part 2 tells us since A is a projective A-module (see 1st paragraph of Problem 4) and I_Z is an injective $\mathbb{Z}$-module, $\mathrm{Hom}_{\mathbb{Z}}(A, I_Z)$ is an injective A-module. Then, consider the map $\iota : M \to \mathrm{Hom}_{\mathbb{Z}}(A, I_Z)$ defined by $m \mapsto [a \mapsto \iota_Z(am)]$, which is a module homomorphism because $a_0(m_1 + m_2) \mapsto [a \mapsto \iota_Z(aa_0(m_1 + m_2))] = [a \mapsto a_0\big(\iota_Z(am_0) + \iota_Z(am_1)\big)] = a_0\big(\iota(m_0) + \iota(m_1)\big)$, and is injective because $\iota(m) = 0 \implies \iota_Z(am) = 0$ for all $a \in A$ (in particular $a = 1$), implying $m = 0$ by injectivity of ι_Z.

506 Homework 1

Daniel Rui - 4/6/21 (actually 4/9/21 T-T)

In all of these problems, A is a commutative ring with unity. Also, we define what it means for an A-module F to be flat: F flat means that the functor $-\otimes_A F$ is exact; i.e. for any exact sequence $M \to N \to L$ of A-modules, the sequence $M \otimes_A F \to N \otimes_A F \to L \otimes_A F$ is also exact.

Also, recall that for an A-module M, an element $x \in M$ is *torsion* if there is an element (non zero-divisor) $a \in A$ s.t. $ax = 0$. M is *torsion-free* if it does not contain a non-zero torsion element.

Major problem! I used the "fact" that many of my diagrams were commutative, but never proved it. So why can we stitch together these exact sequences and have the resulting diagram be commutative? Ok, I talked to Brendan and he said that it comes from the fact that $-\otimes_A M$ is a functor A-**mod** $\to$ A-**mod** (so it preserves commutative diagrams in Problem 2b, though the preliminary diagram must be proved commutative by hand; after all, we do define the objects and the maps between them), and that $-\otimes_A -$ is a functor on the product category A-**mod** $\times$ A-**mod** $\to$ A-**mod** (allowing us to use interchange property $[f \otimes \mathrm{id}] \circ [g \otimes \mathrm{id}] = [g \otimes \mathrm{id}] \circ [f \otimes \mathrm{id}]$ to prove Problem 4 diagram commutative).

Problem 1

Let F be a flat A-module. We want to show that for each non zero-divisor element $a \in A$ and $x \in F$, $ax = 0 \implies x = 0$ (this in particular implies that F is torsion-free). Let us fix some arbitrary non zero-divisor element $a \in A$, and consider the exact sequence $0 \xrightarrow{0} A \xrightarrow{\varphi} A$, where we define $\varphi(b) = ab$. Because a is not a zero-divisor, the kernel of φ is in fact trivial, so φ is injective, making the aforementioned sequence exact. By the definition of flat, we have that the following sequence is also exact:

$$0 \otimes_A F \xrightarrow{0\otimes\mathrm{id}} A \otimes_A F \xrightarrow{\varphi\otimes\mathrm{id}} A \otimes_A F.$$

In a moment, we'll prove that $0 \otimes_A F \simeq 0$ and $A \otimes_A F \simeq F$, but the end result is that the sequence $0 \xrightarrow{0} F \xrightarrow{x\mapsto ax} F$ is exact, implying that $x \mapsto ax : F \to F$ is injective/has trivial kernel, i.e. there is no non-zero element $x \in F$ for which $ax = 0$ for some non zero-divisor $a \in A \iff F$ is torsion free.

To show $0 \otimes_A F \simeq 0$: the elements of $0 \otimes_A F$ are just sums of $0 \otimes_A x$ for $x \in F$, but these are simply the zero element in $0 \otimes_A F$, implying that all elements of $0 \otimes_A F$ are just the zero element.

To show $A \otimes_A F \simeq F$: we just construct two maps and show that they are each other's inverse. To construct a map $f : A \otimes_A F \to F$, we define a A-bilinear map $\lambda : A \times F \to F$ by $(a, x) \mapsto ax$ and use the universal property of the tensor product to get the existence of $f : A \otimes_A F \to F$ satisfying $f \circ \otimes = \lambda$, i.e. f maps $a \otimes x \mapsto ax$, extended to all elements of $A \otimes_A F$ by linearity. We also define $g : F \to A \otimes_A F$ by $x \mapsto 1 \otimes x$. Observe that $g \circ f = a \otimes x \mapsto ax \mapsto 1 \otimes ax$ where indeed $1 \otimes ax = a \otimes x$, and $f \circ g = x \mapsto 1 \otimes x \mapsto x$. Lastly, $A \otimes_A F \xrightarrow{\varphi\otimes\mathrm{id}} A \otimes_A F$ induces the map $[x \overset{g}{\mapsto} 1 \otimes x \xmapsto{\varphi\otimes\mathrm{id}} a \otimes x \overset{f}{\mapsto} ax] = [x \mapsto ax] : F \to F$, exactly as I wrote above.

Problem 2a

Let F be any A-module. We want to show that $- \otimes_A F$ is right exact. This is a covariant functor, so seeing pg. 10 of the class CT-HA notes pdf, we need to show that for any exact $0 \to B \overset{f}{\hookrightarrow} C \overset{g}{\twoheadrightarrow} D \to 0$, the sequence $B \otimes_A F \xrightarrow{f \otimes \mathrm{id}} C \otimes_A F \xrightarrow{g \otimes \mathrm{id}} D \otimes_A F \xrightarrow{0} 0$ is exact.

First, we show that $g \otimes \mathrm{id}$ is surjective. It suffices to show that there is a preimage for all $d \otimes x$, $d \in D, x \in F$ because for any arbitrary element of $D \otimes_A F$ (i.e. some arbitrary finite linear combination of these basis elements), we can just add/scalar multiple and use the homomorphism property to get a preimage. Well, let us fix $d \in D$ and $x \in F$. By the surjectivity of g, there is some $c \in C$ s.t. $g(c) = d$, so then $[g \otimes \mathrm{id}](c \otimes x) = g(c) \otimes \mathrm{id}(x) = d \otimes x$, as desired.

We now want to show that $\mathrm{im}[f \otimes \mathrm{id}] = \ker[g \otimes \mathrm{id}]$. The $(\subseteq)$ assertion (i.e. $[g \otimes \mathrm{id}] \circ [f \otimes \mathrm{id}] = 0$) is obvious, because (for any $b \in B, x \in F$), $b \otimes x \overset{f \otimes \mathrm{id}}{\longmapsto} f(b) \otimes x \overset{g \otimes \mathrm{id}}{\longmapsto} g(f(b)) \otimes x = 0 \otimes x = 0_{D \otimes_A F}$, where the second to last equality is because $\mathrm{im}\, f = \ker g \implies g \circ f = 0$.

$[g \otimes \mathrm{id}] \circ [f \otimes \mathrm{id}] = 0$ gives us that the map $\mu := [c \otimes x + I \mapsto [g \otimes \mathrm{id}](c \otimes x)] : {C \otimes_A F}/{I} \to D \otimes_A F$ (also known as the map "$[g \otimes \mathrm{id}] \mod I$") is well defined, where I is the image of $f \otimes \mathrm{id}$ in $C \otimes_A F$. I claim that we can actually find an inverse to this map, and prove that ${C \otimes_A F}/{I} \simeq D \otimes_A F$. But recall that the 1st isomorphism theorem gives us that for $K = \ker[g \otimes \mathrm{id}]$, ${C \otimes_A F}/{K} \simeq D \otimes_A F$ with forward $(\to)$ map "$[g \otimes \mathrm{id}] \mod K$", and backward map $[g \otimes \mathrm{id}]^{-1}$ (well defined by the definition of the kernel).

Putting things together, we have that ${C \otimes_A F}/{I} \simeq {C \otimes_A F}/{K}$, with forward map $\sigma := [g \otimes \mathrm{id}]^{-1} \circ \mu$ which maps $(c \otimes x) + I \mapsto [g \otimes \mathrm{id}](c \otimes x) \mapsto [g \otimes \mathrm{id}]^{-1}\big([g \otimes \mathrm{id}](c \otimes x)\big) = (c \otimes x) + K$. That is to say, for all elements $\varepsilon \in C \otimes_A F$, σ maps $\varepsilon + I \mapsto \varepsilon + K$, where σ is an isomorphism. If we supposed that the $(\subseteq)$ assertion above was actually strict, $(\subsetneq)$, say $\eta \in \ker[g \otimes \mathrm{id}] \setminus \mathrm{im}[f \otimes \mathrm{id}]$, then $0 \neq \eta + I \mapsto \eta + K = 0$, contradicting σ being an isomorphism.

To finish, we will find the inverse to μ that I claimed existed above. Let us define $\lambda : D \times F \to {C \otimes_A F}/{I}$ as follows: for all $(d, x) \in D \times F$, we know from the surjectivity of g that there is $c \in C$ s.t. $g(c) = d$. We map $(d, x) \mapsto c \otimes x + I$. This is well defined because if c' also satisfies $g(c') = d$, then $c - c' \in \ker g = \mathrm{im}\, f$, so $([c - c'] \otimes x) \in I = \mathrm{im}[f \otimes \mathrm{id}]$, so $c' \otimes x + I = c' \otimes x + [c - c'] \otimes x + I = c \otimes x + I$. λ is bilinear because $(a_1 d_1 + a_2 d_2, x) \mapsto [a_1 c_1 + a_2 c_2] \otimes x + I$ since $g(c_1) = d_1, g(c_2) = d_2 \implies g(a_1 c_1 + a_2 c_2) = a_1 d_1 + a_2 d_2$ by homomorphism properties of g; linearity in 2nd component comes from bilinearity of $\otimes : D \times F \to D \otimes_A F$. Using the universal property, we extend λ to $\nu : D \otimes_A F \to {C \otimes_A F}/{I}$. Verify:

$$\nu \circ \mu = (c \otimes x) + I \mapsto g(c) \otimes x \mapsto (c \otimes x) + I$$

$$\mu \circ \nu = d \otimes x \mapsto (c \otimes x) + I \mapsto g(c) \otimes x = d \otimes x.$$

Note that we did not use anywhere that f was injective, so in fact our argument shows that for any exact sequence $B \xrightarrow{f} C \overset{g}{\twoheadrightarrow} D \to 0$, the sequence $B \otimes_A F \xrightarrow{f \otimes \mathrm{id}} C \otimes_A F \xrightarrow{g \otimes \mathrm{id}} D \otimes_A F \xrightarrow{0} 0$ is exact (in fact, this is true in general).

Problem 2b

We want to show that F is flat $\iff$ for every ideal $I \trianglelefteq A$, the functor $- \otimes_A F$ induces an embedding $I \otimes_A F \hookrightarrow F$. ($\implies$) is easy; given the exact sequence $0 \xrightarrow{0} I \xhookrightarrow{\phi=[i\mapsto i]} A$, flatness tells us that $0 \otimes_A F \xrightarrow{0\otimes\text{id}} I \otimes_A F \xhookrightarrow{\phi\otimes\text{id}} A \otimes_A F$ is exact, but recalling from Problem 1 that $A \otimes_A F \simeq F$, this tells us that we have an injection $I \otimes_A F \hookrightarrow F$, as desired.

($\impliedby$): first, note that an equivalent definition of exactness is that for any sequence of A-modules $0 \to M \to N \to L \to 0$ that's exact, the sequence $0 \to M \otimes_A F \to N \otimes_A F \to L \otimes_A F \to 0$ is also exact. Since we know that $- \otimes_A F$ is right-exact from Problem 2a, all that we need to prove is that $M \hookrightarrow N$ implies $M \otimes_A F \hookrightarrow N \otimes_A F$. The **outline** is to prove the claim for all free modules N of finite rank by induction, and then prove it for an arbitrary A-module.

The base case for our induction is if N is free of rank 1, i.e. it's isomorphic to A. Then, since $A \otimes_A F \simeq F$, what we want to show becomes $M \hookrightarrow A \implies M \otimes_A F \hookrightarrow F$. But M being an A-module that embeds into A means that it's isomorphic to some ideal $I \trianglelefteq A$, and so the desired claim is given exactly by our assumption that any ideal $I \trianglelefteq A$ admits an embedding $I \otimes_A F \hookrightarrow F$.

Now let us suppose that we have proved the result for N free of rank r for all $r < n$, $n \geq 2$, and that we are given N free of rank n and M s.t. $M \hookrightarrow N$. Then because $N \simeq \bigoplus_{i=1}^{n} A$, we can split N up into a direct sum of two free submodules N_1, N_2 of rank $< n$ (say they have rank r_1, r_2 resp. and think of them as $N_1 = \{(a_1, \ldots, a_{r_1}, 0, \ldots, 0) \in N : a_i \in A\}$ and $N_2 = \{(0, \ldots, 0, a_1, \ldots, a_{r_2}) \in N : a_i \in A\}$). Notice that $N_2 \simeq {}^{N}/_{N_1}$. As $M \hookrightarrow N$, we can say that $M \simeq \tilde{M} \subseteq N$. Now we can define $M_1 := N_1 \cap \tilde{M}$ and M_2 to be the image of $\tilde{M}$ in ${}^{N}/_{N_1} \simeq N_2$, i.e. $M_2 = \{m + N_1 \in {}^{N}/_{N_1} : m \in M\}$. Then, we have the following diagram

$$\begin{tikzcd}
0 \arrow[r] & M_1 \arrow[r, hook, "\iota|_M"] \arrow[d, hook] & \tilde{M} \arrow[r, two heads, "\pi|_M"] \arrow[d, hook] & M_2 \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & N_1 \arrow[r, hook, "\iota"'] & N \arrow[r, two heads, "\pi"'] & N_2 \arrow[r] & 0
\end{tikzcd}.$$

All the downward pointing arrows denote injective maps since by definition M_1, M_2 are submodules (or isomorphic to submodules) of N_1, N_2, and we assumed $\tilde{M} \simeq M \hookrightarrow N$; the rows are the way they are by our definitions of N_1, M_1, N_2, M_2 (ι is just the map that takes $x \mapsto x$ since $N_1 \subseteq N$ and $M_1 \subseteq \tilde{M}$, and π is the map that takes $x \mapsto x + N_1$). We can now tensor by $- \otimes_A F$ and use right-exactness to get that the rows in the following diagram are also exact:

$$\begin{tikzcd}
M_1 \otimes_A F \arrow[r, hook, "\iota|_M\otimes\text{id}"] \arrow[d, hook] & \tilde{M} \otimes_A F \arrow[r, two heads, "\pi|_M\otimes\text{id}"] \arrow[d] & M_2 \otimes_A F \arrow[r] \arrow[d, hook] & 0 \otimes_A F \\
N_1 \otimes_A F \arrow[r, hook, "\iota\otimes\text{id}"'] & N \otimes_A F \arrow[r, two heads, "\pi\otimes\text{id}"'] & N_2 \otimes_A F \arrow[r] & 0 \otimes_A F
\end{tikzcd},$$

where the left and right downward pointing arrows are injective maps by the induction hypothesis, and where $\iota \otimes \text{id}$ and $\iota_M \otimes \text{id}$ are injective by the following lemma:

Lemma: $(\bigoplus_{i\in I} M_i)\otimes_A N \simeq \bigoplus_{i\in I}(M_i\otimes_A N)$. *Proof:* let $\lambda : (\bigoplus_{i\in I} M_i)\times N \to L$ be an arbitrary bilinear map. This induces a bilinear map, for each $i\in I$: $\lambda_i : M_i \times N \to L$. The universal property for tensor products gives the existence of $f_i : M_i \otimes_A N \to L$ satisfying $\lambda_i = f_i \circ \otimes$, and so defining $f := \bigoplus_{i\in I} f_i : \bigoplus_{i\in I}(M_i\otimes_A N) \to L$, we have that λ factors uniquely as $\lambda = f\circ\phi\circ\otimes$, where $\phi : (\bigoplus_{i\in I} M_i)\otimes_A N \to \bigoplus_{i\in I}(M_i\otimes_A N)$ is the map $(\bigoplus_{i\in I} m_i, n)\mapsto \bigoplus_{i\in I}(m_i\otimes n)$. By the universal property definition of the tensor product, the claim is proven.

Looking at the first square in the diagram, it is clear to see that the middle downward arrow must be injective as well, completing the induction.

We've proven the claim for N free of finite rank, so now suppose N is free of infinite rank, i.e. $N = \bigoplus_{i\in I} R$ where I is infinite. Let N_1 be a direct factor of N of finite rank, so like $N_1 = \bigoplus_{i=1}^n R$ for some $n\in\mathbb{N}$. Analogous to the above analysis with $M_1 := N_1 \cap \tilde{M}$ and company, we again have that $M_1\otimes_A F \to N_1 \otimes_A F$ is injective (we just proved that the claim holds for free modules with finite rank, and indeed N_1 *is* free with finite rank). Because N_1 is a direct factor of N, the Lemma we just proved again gives that $\iota\otimes\mathrm{id}$ is injective, so we do have an injection $M_1\otimes_A F \hookrightarrow N\otimes_A F$. Since any element $\epsilon\in\tilde{M}\otimes_A F$ is just a finite sum of elements $m\otimes x$ for $m\in\tilde{M}, x\in F$, there is some N_1 s.t. $\epsilon\in(N_1\cap\tilde{M})\otimes_A F$ (just choose n large enough so that all the elements of m that made up ϵ are 0 for components past the nth component). In this fashion, we will be able to find a map $M\otimes_A F\simeq \tilde{M}\otimes_A F\hookrightarrow N\otimes_A F$.

Finally, we can now tackle the case where N is arbitrary. We know from Lec 4 on 4/5/21 that there is some free A-module P s.t. $P\twoheadrightarrow N$ via say some map π (i.e. $\pi : P\to N$ is surjective). Set $Q := \pi^{-1}(\tilde{M})$. We then have the following diagram ($\ker\pi\subseteq Q$ because $\ker\pi = \pi^{-1}(\{0\})\subseteq\pi^{-1}(\tilde{M})$) with exact rows:

$$\begin{tikzcd}
\ker\pi \arrow[r, hook] \arrow[rd, hook] & Q \arrow[r, two heads, "\pi|_Q"] \arrow[d, hook] & M \arrow[r] \arrow[d, hook] & 0 \\
 & P \arrow[r, two heads, "\pi"'] & N \arrow[r] & 0
\end{tikzcd}$$

By right-exactness of $-\otimes_A F$, the following diagram also has exact rows:

$$\begin{tikzcd}
\ker\pi\otimes_A F \arrow[r] \arrow[rd] & Q\otimes_A F \arrow[r, two heads, "\pi|_Q\otimes\mathrm{id}"] \arrow[d, hook] & M\otimes_A F \arrow[r] \arrow[d] & 0 \\
 & P\otimes_A F \arrow[r, two heads, "\pi\otimes\mathrm{id}"'] & N\otimes_A F \arrow[r] & 0
\end{tikzcd}$$

where the middle arrow is injective because we just proved that $Q\hookrightarrow P$ implies $Q\otimes_A F\hookrightarrow P\otimes_A F$ for P an arbitrary free module. Thus, the map $M\otimes_A F\to N\otimes_A F$ is also injective (by say the four lemma), and we are finally done.

Redrawn diagram to make four lemma application more obvious:

$$\begin{tikzcd}
\ker\pi \otimes_A F \arrow[r] \arrow[d] & Q \otimes_A F \arrow[r, two heads, "\pi|_Q\otimes\mathrm{id}"] \arrow[d, hook] & M \otimes_A F \arrow[r] \arrow[d] & 0 \arrow[d, hook] \\
\ker\pi \otimes_A F \arrow[r] & P \otimes_A F \arrow[r, two heads, "\pi\otimes\mathrm{id}"'] & N \otimes_A F \arrow[r] & 0
\end{tikzcd}$$

Problem 3

Let A be a principal ideal domain. We want to prove that F (an A-module) is flat if and only if it is torsion-free. Let $I = aA$ be a non-zero ideal of A. Looking at the first paragraph of Problem 2b and at how I came across the $[x \mapsto ax]$ map from Problem 1, we see that for a flat module F, we have more specifically that the map $(i \otimes x) \mapsto ix$ (for $i \in I, x \in F$) is an injective map $I \otimes_A F \hookrightarrow F$. Because $I = aA$, the map is actually generated by $(a \otimes x) \mapsto ax$. Let us call this map φ_a. It is clear that the image of this map is exactly $IF = aF$. Now consider the following commutative diagram:

$$\begin{tikzcd}
F \arrow[r, hook, two heads] \arrow[d, two heads, "{[x\mapsto ax]:F\to aF}"'] & A \otimes_A F \arrow[r, hook, two heads, "{[b\mapsto ab]\otimes\mathrm{id}}"] & I \otimes_A F \arrow[dll, two heads, "\varphi_a"] \\
aF & &
\end{tikzcd}$$

where the first $\hookrightarrow\!\!\!\!\!\rightarrow$ refers to the fact from Problem 1 that $F \simeq A \otimes_A F$, and the second $\hookrightarrow\!\!\!\!\!\rightarrow$ refers to the fact that $[b \mapsto ab] : A \to I$ is an isomorphism and of course $\mathrm{id} : F \to F$ is also an isomorphism. This diagram tells us that φ_a is injective (i.e. bijective) if and only if the map $[x \mapsto ax] : F \to aF$ is injective (i.e. bijective), but this map is injective iff $ax = 0 \implies x = 0$.

Thus, we have that for all $a \in A$ s.t. aA is a non-zero ideal, φ_a is injective if and only if for all $a \in A$ (non zero-divisor) and $x \in F$, $ax = 0 \implies x = 0$, i.e. all non-zero $x \in F$ are not torsion, i.e. F is torsion free. From Problem 2b, we know that F is flat if and only if for all ideals $I \trianglelefteq A$, $I \otimes_A F \hookrightarrow F$, so the previous sentence is just an extremely long winded way of saying exactly the desired claim for this problem.

Not over PIDs, this claim is not necessarily true. See Exercise 3 in this pdf; I will write up later. Letting $A = k[x, y]$ (indeed commutative with unity), consider the ideal $I = (x, y)$ (recall that ideals can be thought of as A-modules). A is an integral domain, so I has to be torsion free. It suffices to show that the map ϕ from above $(i \otimes_A x) \mapsto ix : I \otimes_A I \to I$ is not injective. We claim that $(x \otimes y) \neq (y \otimes x)$, but ϕ maps both to $xy \in I$. Warning: we can't say that $(x \otimes y) = (1 \otimes xy)$ since $1 \notin I$. See https://math.stackexchange.com/questions/542214/determining-whether-a-certain-element-in-a-tensor-product-is-zero and https://math.stackexchange.com/questions/3018727/equality-of-two-simple-tensors-in-r-kx-y for a complete proof.

Problem 4

Letting F be a flat A-module and $0 \to N \to M \to F \to 0$ and exact sequence of A-modules. We want to show that for an arbitrary A-module L, the sequence $0 \to L \otimes_A N \to L \otimes_A M \to L \otimes_A F \to 0$ is also exact. Right-exactness of $L \otimes_A -$ (right-exact by symmetry; the argument from Problem 2a doesn't care on which side we tensor) almost gives us the claim; we just need to prove furthermore that $L \otimes_A N \to L \otimes_A M$ is injective.

From Lec 4 on 4/5/21, we know that there is some free module P s.t. there is a surjection $P \twoheadrightarrow L$. By the 1st isomorphism theorem for modules, we have that ${}^{P}\big/_{K} \simeq L$ where K is the kernel of the surjection $P \twoheadrightarrow L$. That means that $0 \to K \to P \to L \to 0$ is an exact sequence.

By right-exactness of the tensor functor, the rows and columns of the following commutative diagram are exact:

$$\begin{tikzcd}
 & & & 0 \arrow[d] & \\
 & K \otimes_A N \arrow[r] \arrow[d, "\gamma"] & K \otimes_A M \arrow[r, two heads] \arrow[d] & K \otimes_A F \arrow[r] \arrow[d, hook, "\alpha"] & 0 \\
0 \arrow[r] & P \otimes_A N \arrow[r, hook] \arrow[d, two heads, "\beta"] & P \otimes_A M \arrow[r, two heads] \arrow[d, two heads] & P \otimes_A F \arrow[r] \arrow[d, two heads] & 0 \cdot \\
 & L \otimes_A N \arrow[r, "f"'] \arrow[d] & L \otimes_A M \arrow[r, two heads] \arrow[d] & L \otimes_A F \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

The right column has an extra 0 at the front because F is flat, and the middle row has an extra 0 at the front because P is a free module, and we know from the Lemma from Problem 2b that injective maps are preserved under the tensor functor in the case of free modules.

The snake lemma tells us that there is a map

$$0 \simeq \ker \alpha \to \operatorname{coker} \gamma = {}^{P \otimes_A N}\big/_{\operatorname{im} \gamma} = {}^{P \otimes_A N}\big/_{\ker \beta} \simeq \operatorname{im} \beta = L \otimes_A N$$

that makes $\ldots \to \ker \alpha \to \operatorname{coker} \beta \xrightarrow{f} L \otimes_A M \to \ldots$ an exact sequence. In other words, we have that $0 \to L \otimes_A N \xrightarrow{f} L \otimes_A M$ is exact, which tells us that f is injective, as desired.

Problem 5

Let F be a flat A-module and $0 \to N \to M \to F \to 0$ be an exact sequence of A-modules. We want to show that N if flat if and only if M is flat. Recall from Problem 2b that N is flat $\iff$ for every ideal $I \trianglelefteq A$, we have $I \otimes_A N \hookrightarrow N$. Let $I \trianglelefteq A$ be any arbitrary ideal of A and consider the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r, hook] & M \arrow[r, two heads] & F \arrow[r] & 0 \\
0 \arrow[r] & I \otimes_A N \arrow[r, hook] \arrow[u] & I \otimes_A M \arrow[r, two heads] \arrow[u] & I \otimes_A F \arrow[r] \arrow[u, hook] & 0
\end{tikzcd}$$

where the top row is exact by assumption, the bottom row is exact by Problem 4, and the right upward pointing arrow is injective by the flatness assumption on F. If the left upward pointing arrow is an injective map, then because the upper left arrow is also injective, that forces the middle arrow $I \otimes_A M \to M$ to be an injective map also. Similarly, if the middle upward pointing arrow is an injective map, then because the lower left arrow is also injective, that forces the left arrow $I \otimes_A N \to N$ to be an injective map also. Because $I \trianglelefteq A$ was arbitrary, this proves the desired claim.

Problem 6