210B Final

Daniel Rui - 3/16/21

Problem 1

Let $R := \mathbb{Z}[i] := \mathbb{Z}[\sqrt{-1}]$. We are asked to determine whether there exist non-zero R-modules N, L s.t. $N \oplus L \simeq R/5R =: M$. We know from 1/3/22 that R is a EuD $\implies$ PID, with "Euclidean function" $\varphi(a+bi) := |a+bi|_{\mathbb{C}} = a^2 + b^2$. We know from the multiplicativity of the norm on $\mathbb{C}$ that φ is multiplicative — I will now refer to φ as the norm on $R := \mathbb{Z}[i]$. Then because all non-zero elements of $R := \mathbb{Z}[i]$ have norm $\geqslant 1$, all non-zero elements of $5R$ have norm $\geqslant 25$. This in particular implies that $(2+i), (2-i)$ are not in $5R$, since $\varphi(2 \pm i) = 5$. The fact that 5 is prime $\equiv$ irreducible in $\mathbb{Z}$ also implies that $(2 \pm i)$ are prime $\equiv$ irreducible in R (recall from 1/5/22 that prime $\equiv$ irreducible in PIDs and UFDs), because $r \cdot s = (2 \pm i) \implies \varphi(r)\varphi(s) = 5 \implies$ w.l.o.g. $\varphi(r) = 1 \iff r \in \{\pm 1, \pm i\} = R^\times$.

Recall now the result from 1/24/22 that every torsion finitely generated (f.g.) module M over a PID R is the direct sum of its P-primary parts $M(P) := \{m \in M : P^n m = 0 \text{ for some } n > 0\}$, where P is a prime ideal $\triangleleft R$, and all but finitely many of the $M(P)$ are 0. In our case, $M := R/5R$ is obviously f.g. (by $1+5R \in R/MR =: M$) and is torsion (because $5 \cdot M = 0_{R/5R}$). I also showed in the above paragraph that $(2 \pm i)R$ are two prime ideals in R, where $(2-i)(2+i) = 5 = 0_M := 0_{R/5R} \implies (2 \pm i) \in M((2 \mp i)R)$. Thus $M((2 \mp i)R)$ are two non-zero R-modules, and so $N := M((2+i)R) \oplus \prod_{P \triangleleft R, P \neq (2 \pm i)R} M(P)$ and $L := M((2-i)R)$ are two non-zero R-modules s.t. $N \oplus L = M := R/5R$.

Problem 2

We are asked to determine the invariant factors of the abelian group $G := (\mathbb{Z}/1000\mathbb{Z})^\times$ of invertible elements in $\mathbb{Z}/1000\mathbb{Z}$. Recall that abelian groups $\equiv \mathbb{Z}$-modules ($\mathbb{Z}$-action on G notated $n \bullet g$, defined as addition n times in additive group and multiplication n times in multiplicative group), and G finite $\implies |G| \bullet g := g^{|G|} = e_G$ for all $g \in G$, so G is a torsion finite (hence finitely generated) $\mathbb{Z}$-module. Recall from class 1/28/22 the statement of the decomposition theorem for torsion f.g. modules over a PID R in invariant factor form: for a torsion f.g. module $M = M_{\text{tors}}$ over a PID R, we can decompose M_{tors} into $M_{\text{tors}} \simeq {}^R/_{I_1} \oplus \ldots \oplus {}^R/_{I_s}$ for some ideals $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_s \triangleleft R$; moreover, the invariant factors $\{I_1, \ldots, I_s\}$ are uniquely determined by M, so two torsion f.g. R-modules are isomorphic $\iff$ they have the same set of invariant factors.

In our situation, $R := \mathbb{Z}$, and the principal ideals $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_s$ correspond to $a_s \mid \ldots \mid a_2 \mid a_1$ (where $I_i = a_i\mathbb{Z}$), so for any finite abelian group A, $|A| = |\mathbb{Z}/a_1\mathbb{Z}| \cdots |\mathbb{Z}/a_s\mathbb{Z}| = a_1 \cdots a_s$. Before we go further with this, let us first observe that from the Chinese remainder theorem, $\gcd(8, 125) = 1, 8 \cdot 125 = 1000 \implies \mathbb{Z}/1000\mathbb{Z} \simeq \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/125\mathbb{Z}$. Also, I claim that for any rings R_1, R_2, we have $R_1^\times \times R_2^\times \simeq (R_1 \times R_2)^\times$. This is because (r_1, r_2) is a unit in $R_1 \times R_2 \iff \exists (s_1, s_2) \in R_1 \times R_2$ s.t. $(r_1, r_2)(s_1, s_2) = 1_{R_1 \times R_2} = (1, 1) \iff \exists s_1 \in R_1 : r_1 s_1 = 1$ and $\exists s_2 \in R_2 : r_2 s_2 = 1 \iff r_1$ is a unit in R_1 and r_2 is a unit in R_2.

Therefore, we arrive at $G := (\mathbb{Z}/1000\mathbb{Z})^\times \simeq (\mathbb{Z}/8\mathbb{Z})^\times \times (\mathbb{Z}/125\mathbb{Z})^\times$. We know that $|(\mathbb{Z}/8\mathbb{Z})^\times| = \varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4$, and $|(\mathbb{Z}/125\mathbb{Z})^\times| = \varphi(125) = 125 - 25 = 100$ (using the formulas for the totient function I discuss in more detail in Problem 10 below). By the above mentioned invariant factor decomposition for $\mathbb{Z}$-modules (more commonly known as the "fundamental theorem of finitely generated/finite abelian groups"), we have that $(\mathbb{Z}/8\mathbb{Z})^\times$ is either $\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\simeq \mathbb{Z}/4\mathbb{Z}$. But it can't be $\mathbb{Z}/4\mathbb{Z}$ because every element of $(\mathbb{Z}/8\mathbb{Z})^\times$, namely $\{1, 3, 5, 7\}$, have order 2 (e.g. $5^2 = 25 = 1$ in $\mathbb{Z}/8\mathbb{Z}$), while $\mathbb{Z}/4\mathbb{Z}$ has an order 4 element.

Now we look at $(\mathbb{Z}/125\mathbb{Z})^\times$. The possible invariant factors for this are $\{2, 50\}, \{10, 10\}$, and $\{100\}$. So, having no better idea, I just start calculating orders of elements. Starting with 2 (which is relatively prime to 125 and hence $\in (\mathbb{Z}/125\mathbb{Z})^\times$), I calculate $\{2^1, 2^2, 2^3, \ldots\} = \{2, 4, 8, 16, 32, 64, 128 = 3, 6, \ldots\}$ (modulo 125). Looking at these modulo 5 (important because 125 is 0 modulo 5, and hence subtracting multiples of 125 after I multiply by 2 has no effect on the last digit), I get the repeating pattern $\{2, 4, 3, 1, 2, 4, 3, 1, \ldots\}$. Thus, the order n of 2 in $(\mathbb{Z}/125\mathbb{Z})^\times$ must be a multiple of 4. By Lagrange, we must have that $n \mid 100$, leaving the possibilities $n = 4, 20, 100$. Obviously, $2^4 = 16 \neq 1$, so n is either 20 or 100. Finally, I simply calculate the value of 2^20 modulo 125: $2^5 = 32 \rightsquigarrow 2^10 = 24 \rightsquigarrow 2^20 = 76 \neq 1$, meaning 2 is order 100 in $(\mathbb{Z}/125\mathbb{Z})^\times$, meaning $(\mathbb{Z}/125\mathbb{Z})^\times \simeq \mathbb{Z}/100\mathbb{Z}$.

In summary, we have $G := (\mathbb{Z}/1000\mathbb{Z})^\times \simeq (\mathbb{Z}/8\mathbb{Z})^\times \times (\mathbb{Z}/125\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/100\mathbb{Z}$, so the invariant factors of G are exactly $\boxed{\{2, 2, 100\}}$.

Problem 3

Let $\mathrm{GL}_n(\mathbb{C})$ be the multiplicative group of invertible $n \times n$ matrices over $\mathbb{C}$. We want to prove that every element of finite order in G is conjugate to a diagonal matrix. This problem is essentially all about the content of lecture 2/2/22. To use those results, let us establish the notation $F := \mathbb{C}$, $R := F[x]$, and $V := \mathbb{C}^n$ (a vector space over F). Let us fix such an element $A \in \mathrm{GL}_n(\mathbb{C})$, with say order $N \in \mathbb{N}^+$. This matrix can be understood as a linear transformation $V \to V$ (using standard matrix multiplication Av for a vector $v \in V := \mathbb{C}^n$), which I'll denote as S to emphasize that A is a matrix, whereas S is a function. Using the notation of 1/28/22, the matrix of S w.r.t. the standard basis $\mathscr{E}$ of $V := \mathbb{C}^n$ is $[S]_{\mathscr{E}} = A$. With S, we can equip V with and R-module structure by defining $(a_n x^n + \ldots + a_1 x + a_0) \bullet v := a_n A^n(v) + \ldots + a_1 A(v) + a_0 v$ — see 1/28/22 for more details.

The fact that A has order $N \iff A^N = \mathrm{Id}$ means that $x^N - 1 \in \mathrm{Ann}(V) := \{f \in R : f \bullet V = 0\} = \{f \in F[x] : [f(A)](v) = 0,\ \forall v \in V\}$. But we know (again from 2/2/22) that there is $f_{\min} \in R := F[x]$ s.t. $\mathrm{Ann}(V) = f_{\min} \cdot R$. In particular, $f_{\min} \mid x^N - 1$, and because $x^N - 1$ factors into a product of irreducibles $x^N - 1 = \prod_{k=0}^{N-1}(x - \xi_N^k)$ in $R := F[x] := \mathbb{C}[x]$ (where $\xi_N := e^{2\pi i/N}$ is a primitive Nth root of unity), the fact that $R := F[x]$ is a EuD $\implies$ UFD means that $f_{\min}$ must also factor as a product of some of the $(x - \xi_N^k)$, which are all distinct linear factors (I explain this step in more detail in Problem 9 below).

We know from the end of lecture 2/2/22 that S is diagonalizable (i.e. there is some basis $\mathscr{B}$ of V s.t. $[S]_{\mathscr{B}}$ is diagonal) $\iff$ the minimal polynomial $f_{\min}$ is a product of distinct linear polynomials, so indeed $[S]_{\mathscr{B}}$ is diagonal for some basis $\mathscr{B}$. Finally, we know from 1/28/22 that the matrices of S w.r.t. any basis of V are all conjugate, so indeed A is conjugate to the diagonal matrix $[S]_{\mathscr{B}}$, as desired.

Problem 4

We are asked to find the number of conjugacy classes in $\mathrm{GL}_3(\mathbb{F}_2) := \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$. This problem is very similar to an example we did in class 2/2/22, so we again (as in Problem 3 above) establish the notation the notation $F := \mathbb{F}_2 := \mathbb{Z}/2\mathbb{Z}$, $R := F[x]$, and $V := F^3$ (a vector space over F). I again point out that a matrix $A \in \mathrm{GL}_3(\mathbb{F}_2)$ can be understood as a linear transformation $V \to V$ (using standard matrix multiplication Av for a vector $v \in V := \mathbb{F}_2^3$), which I'll denote as $S := S_A$ to emphasize that A is a matrix, whereas S is a function. Using the notation of 1/28/22, the matrix of S w.r.t. the standard basis $\mathscr{E}$ of $V := \mathbb{F}_2^3$ is $[S]_{\mathscr{E}} = A$. With S, we can again equip V with an R-module structure by defining $f \bullet v := [f(A)](v)$.

From 1/31/22, the IF decomposition for operators states that given a linear operator $S : V \to V$ (like the linear operator S_A corresponding to A defined in the above paragraph), there are unique monic polynomials $f_1 \mid f_2 \mid \ldots \mid f_s$ s.t. the matrix of S in some basis is a block diagonal matrix with the blocks $C(f_i)$ $(i \in [s]^+)$ making up the diagonal (the companion matrix $C(f_i)$ defined at the end of the table from lectures 1/28/22 and 1/31/22) — this is known as the "canonical form of S". Obviously, given a collection of monic polynomials $f_1 \mid f_2 \mid \ldots \mid f_s$ and forming the block diagonal matrix A consisting of blocks $C(f_i)$, we can define a linear operator $S_A : V \to V$ s.t. $[S]_{\mathscr{E}} = A$. The aforementioned table from 1/28/22 and 1/31/22 also mentions that given two bases $\mathscr{B}_1, \mathscr{B}_2$ of V, the matrices $[S]_{\mathscr{B}_1}, [S]_{\mathscr{B}_2}$ are conjugate.

Thus in summary we have that every matrix $A \in M_3(\mathbb{F}_2)$ (3×3 matrices over $\mathbb{F}_2$) produces a linear operator $S_A : V \to V$ with a canonical form $[S_A]_{\mathscr{B}}$, which is similar/conjugate to A, and which uniquely determines (and is uniquely determined by) a collection of monic polynomials $f_1 \mid f_2 \mid \ldots \mid f_s$ s.t. $\sum_{i=1}^s \deg(f_i) = \sum_{i=1}^s$[width of the square block $C(f_i)$] = [width of the canonical form of S_A] = $\dim_F(V)$. Or more succinctly, the conjugacy classes of $M_3(\mathbb{F}_2)$ are in one-to-one correspondence with the collections of monic polynomials $f_1 \mid f_2 \mid \ldots \mid f_s$ in $R := F[x] := \mathbb{F}_2[x]$ s.t. $\sum_{i=1}^s \deg(f_i) = \dim_F(V) = 3$. To get to the conjugacy classes of $\mathrm{GL}_n(\mathbb{F}_2)$ like we want, recall from 2/2/22 that the characteristic polynomial $\chi_A(x) := \det(xI_n - A) = \prod_{i=1}^s f_i$, so $\det(A) = \pm\chi_A(0) = \pm\prod_{i=1}^s f_i(0)$, so $A \in \mathrm{GL}_3(\mathbb{F}_2) \iff \det(A) \neq 0 \iff$ all $f_i(0) \neq 0$ for $i \in [s]^+$.

The collection of monic polynomials $f_1 \mid f_2 \mid \ldots \mid f_s$ for S_A is known as the "invariant factors of A". The restriction that $\sum_{i=1}^s \deg(f_i) = 3$ and $f_1 \mid f_2 \mid \ldots \mid f_s$ leaves us with 3 possibilities:

- $\mathrm{IF}(A) = \{f_1\} \implies f_1 = x^3 + ax^2 + bx + c$ with $c \neq 0$ (since we want $f_1(0) \neq 0$), and no other restrictions $\rightsquigarrow p$ choices for each of a, b and $(p-1)$ choices for $c \rightsquigarrow p^2(p-1)$ conjugacy classes with IFs of this type;

- $\mathrm{IF}(A) = \{f_1, f_2\} \implies f_1 = x + a, f_2 = (x + a)(x + b)$ with $a, b \neq 0$, and no other restrictions $\rightsquigarrow (p-1)$ choices for each of $a, b \rightsquigarrow (p-1)^2$ conjugacy classes with IFs of this type;
- and $\mathrm{IF}(A) = \{f_1, f_2, f_3\} \implies f_1 = f_2 = f_3 = x + a$ with $a \neq 0$, and no other restrictions $\rightsquigarrow (p-1)$ choices for $a \rightsquigarrow (p-1)$ conjugacy classes with IFs of this type.

Thus in total, we have $p^2(p-1) + (p-1)^2 + p - 1 = (p-1)(p^2 + (p-1) + 1) = \boxed{p(p-1)(p+1)}$ conjugacy classes in $\mathrm{GL}_3(\mathbb{F}_2)$.

Problem 5

We are asked to determine the Galois group of a normal closure of $E := \mathbb{Q}(\sqrt{-3} + \sqrt[3]{2})$ over $\mathbb{Q}$. I claim that $K := \mathbb{Q}(\sqrt[3]{2}, \xi_3)$ (where $\xi_3^3 = 1, \xi_3 \neq 1$) is a normal closure of E (over $\mathbb{Q}$), where we know from 2/14/22 that K is a normal, in fact Galois, extension of $\mathbb{Q}$ (it's a splitting field of the separable polynomial $x^3 - 2$), with Galois group $G \simeq S_3$ (this latter result is from 2/25/22). By the Galois correspondence (2/25/22) plus the relationship/equivalence between normal field extensions and normal subgroups of the Galois group (2/28/22), and the fact (Problem 9 of 210A Homework 4) that S_3 has 4 subgroups: 3 (non-normal) subgroups of order 2, and 1 normal (index 2) subgroup of order 3; we know that there are exactly 4 (strictly) intermediate fields between $\mathbb{Q}$ and K, exactly one of which is normal (again actually Galois) over $\mathbb{Q}$, namely $\mathbb{Q}(\xi_3)$ (a splitting field of the separable polynomial $x^3 - 1$)).

Since E is a field (not necessarily strictly) between $\mathbb{Q}$ and $K := \mathbb{Q}(\sqrt[3]{2}, \xi_3) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ (equality because[†] $\xi_3 = \frac{-1+\sqrt{-3}}{2}$), and K is normal over $\mathbb{Q}$, we must have that the normal closure of E, denoted say L, is also an intermediate (normal!) field over $\mathbb{Q}$ contained in K. The above paragraph narrows it down to 3 possibilities: $L = \mathbb{Q}, \mathbb{Q}(\xi_3)$, or K itself. Well, if $\alpha := \sqrt{-3} + \sqrt[3]{2} \in \mathbb{Q}(\xi_3) = \mathbb{Q}(\sqrt{-3})$, then $\sqrt[3]{2} = \alpha - \sqrt{-3} \in \mathbb{Q}(\xi_3)$, implying that $\mathbb{Q}(\sqrt[3]{2}, \xi_3) = \mathbb{Q}(\xi_3)$. But we know form Problem 5 of Homework 6 that $[\mathbb{Q}(\sqrt[3]{2}, \xi_3) : \mathbb{Q}] = 6$, while $[\mathbb{Q}(\xi_3) : \mathbb{Q}] = \deg(\mathrm{Irr}(\xi_3, \mathbb{Q})) = \deg(x^2 + x + 1) = 2$. Hence, $\alpha \notin \mathbb{Q}(\xi_3) \implies \alpha \notin \mathbb{Q}$, forcing $L = K$, and as mentioned above, $\boxed{\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q}) \simeq S_3}$.

Problem 6

We are asked to determine the Galois group of the polynomial $f := x^8 - 2$ over $\mathbb{Q}$. Note that f is irreducible over $\mathbb{Q}$ by Eisenstein, and hence separable because $\mathbb{Q}$ is characteristic 0 and hence perfect (see 2/14/22). By definition (from 3/2/22) the Galois group of the (separable) polynomial f over $\mathbb{Q}$ is the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ of any splitting field K of f over $\mathbb{Q}$ (we know from 2/9/22 that any 2 splitting fields of a polynomial over a base field are isomorphic). For convenience, let us take K to be the unique[‡] splitting field of f (over $\mathbb{Q}$) contained in $\mathbb{C}$. We know from real analysis that there is an element $\sqrt[8]{2} \in \mathbb{R}$ that is a root of $f := x^8 - 2$, and we know that $\xi_8 := e^{2\pi i/8} = \frac{1+i}{\sqrt{2}}$ is an element of order 8, so $\{\xi_8^0 \cdot \sqrt[8]{2}, \ldots, \xi_8^7 \cdot \sqrt[8]{2}\}$ are all 8 distinct roots of f in $\mathbb{C}$. Since $\xi_8 = \frac{1+i}{\sqrt{2}} \in \mathbb{Q}(\sqrt[8]{2}, i)$, we have that the splitting field $K := \mathbb{Q}(\xi_8^0 \cdot \sqrt[8]{2}, \ldots, \xi_8^7 \cdot \sqrt[8]{2}) = \mathbb{Q}(\sqrt[8]{2}, i)$.

[†] which we can verify by checking $(2\xi_3 + 1)^2 = 4\xi_3^2 + 4\xi_3 + 1 = 4(\xi_3^2 + \xi_3 + 1) - 3 = -3$, where we use that ξ_3 is a root of $(x^2 + x + 1)$, because ξ_3 is a root of $x^3 - 1 = (x-1)(x^2 + x + 1)$ but not a root of $(x - 1)$

[‡] since f splits in $\mathbb{C}$ by the fundamental theorem of algebra, we know from 2/9/22 that there is a unique splitting field of f contained in $\mathbb{C}$.

By the tower property (2/4/22), $[K:\mathbb{Q}] = [K:\mathbb{Q}(\sqrt[8]{2})]\cdot[\mathbb{Q}(\sqrt[8]{2}),\mathbb{Q}]$. As said previously, $f = x^8-2$ is (monic and) irreducible over $\mathbb{Q}$ with $\sqrt[8]{2}$ as a root, so $f = \mathrm{Irr}(\sqrt[8]{2},\mathbb{Q}) \implies [\mathbb{Q}(\sqrt[8]{2}),\mathbb{Q}] = \deg(\mathrm{Irr}(\sqrt[8]{2},\mathbb{Q})) = \deg(f) = 8$. Regarding $[K:\mathbb{Q}(\sqrt[8]{2})] = \deg(\mathrm{Irr}(i,\mathbb{Q}(\sqrt[8]{2})))$, because $\mathrm{Irr}(i,\mathbb{Q}(\sqrt[8]{2}))$, $\mathrm{Irr}(i,\mathbb{Q})$ are both $\in \mathbb{Q}(\sqrt[8]{2})[x]$ and $\mathrm{Irr}(i,\mathbb{Q}), x^2+1$ are both $\in \mathbb{Q}[x]$, and all three polynomials have i as a root, minimality (see 2/7/22) leads to $\mathrm{Irr}(i,\mathbb{Q}(\sqrt[8]{2})) \mid \mathrm{Irr}(i,\mathbb{Q}) \mid x^2+1$, implying that $[K:\mathbb{Q}(\sqrt[8]{2})] = \deg(\mathrm{Irr}(i,\mathbb{Q}(\sqrt[8]{2})))$ is either 1 or 2, where $[K:\mathbb{Q}(\sqrt[8]{2})] = 1 \iff K := \mathbb{Q}(\sqrt[8]{2},i) = \mathbb{Q}(\sqrt[8]{2})$.

But $\mathbb{Q}(\sqrt[8]{2})) \subseteq \mathbb{R}$ and $i \notin \mathbb{R}$, so $i \notin \mathbb{Q}(\sqrt[8]{2})) \implies [K:\mathbb{Q}(\sqrt[8]{2})] = 2$ ($\implies \mathrm{Irr}(i,\mathbb{Q}(\sqrt[8]{2})) = \mathrm{Irr}(i,\mathbb{Q}) = x^2+1$). Thus in total $[K:\mathbb{Q}] = 16$. We know any automorphism $\rho \in \mathrm{Gal}(K/\mathbb{Q})$ must map any element α to some other root of $\mathrm{Irr}(\alpha,\mathbb{Q})$, so the only possibilities for such an automorphism $\rho \in G := \mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Aut}_{\mathbb{Q}}(K)$ are to map $\sqrt[8]{2} \mapsto \xi_8^{0,1,\ldots,8}\sqrt[8]{2}$ and $i \mapsto \pm i$ (any automorphism of $K = \mathbb{Q}(\sqrt[8]{2},i)$ fixing $\mathbb{Q}$ is determined by its action on $\sqrt[8]{2}$ and i). There are 8 possible choices to which ρ can send $\sqrt[8]{2}$, and 2 possible choices to which ρ can send i, making for 16 possible choices. But $|\mathrm{Gal}(K/\mathbb{Q})| = [K:\mathbb{Q}] = 16$, meaning every single one of these possibilities is realized (i.e. for every $i \in [8]^+, j \in [2]^+$, there is exactly one $\rho_{i,j} \in G$ that maps $\sqrt[8]{2} \mapsto \xi_8^i \cdot \sqrt[8]{2}$ and $i \mapsto (-1)^j i$)!

Define now $\sigma,\tau \in G$ to be the automorphisms that map $\sqrt[8]{2} \mapsto \xi_8^1\sqrt[8]{2}, i \mapsto i$ and $\sqrt[8]{2} \mapsto \sqrt[8]{2}, i \mapsto -i$ respectively. It is clear that $\rho_{i,j} = \sigma^i \circ \tau^j$, and so σ,τ generate G. Furthermore, the cyclic subgroups $\langle\tau\rangle$ and $\langle\sigma\rangle$ are respectively order 2 and order 8 (because ξ_8 is order 8) $\implies \langle\sigma\rangle$ is index 2 $\implies$ normal in G; and have trivial intersection (because every element of $\langle\sigma\rangle$ is identity on i, and only the trivial element of $\langle\tau\rangle$ is identity on i). Thus $\langle\sigma\rangle \triangleleft G$ and $\langle\tau\rangle$ satisfy the criterion for being an internal semidirect product of G, so $\boxed{G \simeq \langle\sigma\rangle \rtimes_\phi \langle\tau\rangle \simeq \mathbb{Z}/8\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}}$ (the latter being an external semidirect product[§]), also known as the dihedral group D_{16} of order 16 (see lecture 10/22/21 from last quarter) — EDIT 3/29/22: apparently it is not the dihedral group; instead some other weird semi-direct product.

Remarks: above we worked in $\mathbb{C}$ for convenience, and at a critical point in the argument used that $i \notin \mathbb{Q}(\sqrt[8]{2})$. Of course, it is possible to construct $\sqrt[8]{2}$ and ξ_8 purely algebraically: in any splitting field K of $f := x^8-2$ over $\mathbb{Q}$, separability $\rightsquigarrow$ 8 distinct roots $\{\alpha_1,\ldots,\alpha_8\}$, where we can define $\sqrt[8]{2} := \alpha_1$; the quotients $\{\frac{\alpha_1}{\alpha_1},\ldots,\frac{\alpha_8}{\alpha_1}\}$ are 8 distinct 8th roots of unity, hence they are exactly the cyclic group μ_8, which has a generator ξ_8. From this we see that $K = \mathbb{Q}(\sqrt[8]{2},\xi_8)$. Moreover with ξ_8, we can define $i := \xi_8^2$, which is an element of order exactly 4, so i is a root of $(x^4-1) = (x^2-1)(x^2+1)$ but not of (x^2-1), meaning i must be a root of (x^2+1). Of course, one can then check that $\frac{\pm1\pm i}{2}$ (all 4 possible sign combinations) are all primitive 8th roots of unity, since $\frac{(\pm1\pm i)^2}{\sqrt{2}^2} = \frac{\pm 2i}{2} = \pm i$, which both have order exactly 4 $\rightsquigarrow$ $\frac{\pm1\pm i}{2}$ has order exactly 8. Hence we again arrive at $K = \mathbb{Q}(\sqrt[8]{2},i)$. This is all fine and dandy, but it is not obvious how to show $i \notin \mathbb{Q}(\sqrt[8]{2})$ in this purely algebraic context, since we can no longer use that $\mathbb{Q}(\sqrt[8]{2}) \subseteq \mathbb{R}$ and $i \notin \mathbb{R}$ like we could when we had access to (the analytically, not algebraically, constructed objects) $\mathbb{R}$ and $\mathbb{C}$.

[§] w.r.t. $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/8\mathbb{Z})$ defined by $0 \mapsto [x \mapsto x]$ and $1 \mapsto [x \mapsto -x]$, which corresponds to the inner semidirect product conjugation map $\phi : \langle\tau\rangle \to \mathrm{Aut}(\langle\sigma\rangle)$ defined by $\phi(\tau^j) = [\sigma^i \mapsto \tau^j\sigma^i\tau^{-j}]$ for $i \in [8]^+$, $j \in [2]^+$.

Problem 7

Let $f \in F[x]$ be an irreducible polynomial over a field F, and let K be a finite field extension of degree relatively prime to $\deg(f)$. We want to prove that f is irreducible over K. We know from 2/7/22 that there is some (finite) field extension L of K that contains a root α of f (e.g. take $L := K[x]/\langle \tilde{f} \rangle$ for some irreducible factor $\tilde{f}$ of f in $K[x]$), so we have a tower of field extensions $L \supseteq K(\alpha) \supseteq K \supseteq F$. We also know from 2/7/22 that $[F(\alpha) : F] = \deg(\mathrm{Irr}(\alpha, F)) = \deg f$ (because α is a root of f, and f is given to be irreducible over F, $f = a \cdot \mathrm{Irr}(\alpha, F)$ for some $a \in F^\times$, namely the leading coefficient of f) and $[K(\alpha) : K] = \deg(\mathrm{Irr}(\alpha, K))$. Moreover because $f = \mathrm{Irr}(\alpha, F) \in F[x] \subseteq K[x]$ has α as a root, the minimality of $\mathrm{Irr}(\alpha, K) \in K[x]$ gives that $\mathrm{Irr}(\alpha, K) \mid f$ in $K[x]$ (again, see 2/7/22 notes). In particular, $[K(\alpha) : K] \leqslant \deg(f) = [F(\alpha) : F]$.

We now prove that $[K(\alpha) : K] = [F(\alpha) : F] \cdot [K : F]$ (this is just a slight variant of Problem 1 from Homework 6). A corollary of the "tower property" from 2/4/22 tells us that the degrees of intermediate field extensions divide the big field extension, meaning both $a := [F(\alpha) : F]$ and $b := [K : F]$ divide (and are $\leqslant$) $[K(\alpha) : F]$. Thus, $[K(\alpha) : F] \geqslant \mathrm{lcm}(a, b)$, which is their product $a \cdot b = [F(\alpha) : F] \cdot [K : F]$ because of relative primality. On the other hand, the tower property gives $[K(\alpha) : F] = [K(\alpha) : K] \cdot [K : F] \leqslant [F(\alpha) : F] \cdot [K : F]$. Thus we indeed have equality, forcing in particular that the inequality $[K(\alpha) : K] \leqslant [F(\alpha) : F]$ is an equality.

But we already pointed out that $[K(\alpha) : K] = \deg(\mathrm{Irr}(\alpha, K))$ and $[F(\alpha) : F] = \deg(\mathrm{Irr}(\alpha, F))$ where $f = a \cdot \mathrm{Irr}(\alpha, F)$, so because $\mathrm{Irr}(\alpha, K) \mid \mathrm{Irr}(\alpha, F)$ (discussed above) and both are monic of the same degree, we must have equality $\mathrm{Irr}(\alpha, K) = \mathrm{Irr}(\alpha, F) \implies f = a \cdot \mathrm{Irr}(\alpha, K)$. By definition $\mathrm{Irr}(\alpha, K)$ is irreducible over K, and $a \in F^\times$ is just a unit, so f is also irreducible over K, as desired.

Problem 8

Let E_1 and E_2 be to normal extensions (implicitly finite — at least as we defined it in class 2/14/22) of (some field) F. Suppose that E_1, E_2 are subfields of some "universal" field U. We show that the intersection $E_1 \cap E_2$ is a normal extension of F. Recall (from 2/14/22) that normality of a (finite) f.e. E of F can be formulates as the condition that every (non-constant) polynomial $f \in F[x]$ with at least one root in E has every root in E splits completely over E.

Letting $f \in F[x]$ be an arbitrary non-constant polynomial with at least one root in $E_1 \cap E_2$, normality of E_1 over F gives that F splits in E_1, so in particular letting $\alpha_1, \ldots, \alpha_n \in E$ be all the roots of f in E_1, the field $L_1 := F(\alpha_1, \ldots, \alpha_n)$ is a splitting field of f over F, contained in $\subseteq E_1 \subseteq U$. Performing the same construction for E_2 yields another splitting field L_2 of f over F, this time contained in $\subseteq E_2 \subseteq U$. But we know from 2/9/22 that if f splits in the field U , U contains a *unique* splitting field of f! Meaning $L_1 = L_2 =: L \implies L \subseteq E_1 \cap E_2$, so (the arbitrarily chosen non-constant polynomial in $F[x]$) f splits in $E_1 \cap E_2$. Thus by the definition of normality stated above, $E_1 \cap E_2$ is normal over F.

Problem 9

Let $f \in F[x]$ be a polynomial over F (of degree say n) and let g be a monic divisor of f over a field extension L of F. We want to prove that the coefficients of g are algebraic over F. We know from 2/9/22 that there is a (finite) field extension K of F in which f splits, say into $a\prod_{i=1}^{n}(x-\alpha_i)$ for $\alpha_i \in K$, $a \in F$. Then, $g \in L[x] \subseteq KL[x]$ (with some $h \in L[x] \subseteq KL[x]$ s.t. $f = gh$), and $(x-\alpha_i) \in K[x] \subseteq KL[x]$, so because $KL[x]$ is a EuD $\implies$ UFD (see 1/3/22 and 1/5/22), factoring g into a product of irreducibles $g_1, \ldots, g_m \in KL[x]$, uniqueness of factorization (up to units) forces $g_j = u_j(x-\beta_j)$ for some unit $u_j \in KL[x]^\times = KL^\times$ (see 1/7/22) and some $\beta_j \in \{\alpha_1, \ldots, \alpha_n\} \implies (x-\beta_j) \in K[x]$.

Therefore, $g = u_1 \cdots u_m \cdot \prod_{j=1}^{m}(x-\beta_j)$, and because g is monic, comparing leading coefficients yields $u_1 \cdots u_m = 1$. I've already pointed out that $(x-\beta_j) \in K[x]$, so $g = \prod_{j=1}^{m}(x-\beta_j) \in K[x]$ as well, and so all coefficients of g are in K. But K is a finite f.e. of F, and we know from 2/7/22 that finite extensions are algebraic, and all elements of an algebraic f.e. of F are algebraic over F, so we are done.

Problem 10

Let Φ_n be the nth cyclotomic polyomial over $\mathbb{Q}$. We are asked to factor the polynomial $\Phi_n(x^2)$ into a product of irreducible polynomials over $\mathbb{Q}$. We know from the lecture (3/2/22) on cyclotomic fields that denoting by $\mathbb{Q}_n$ the splitting field of (the separable polynomial) $x^n - 1$ over $\mathbb{Q}$, by μ_n the (group of) n roots of $x^n - 1$ in $\mathbb{Q}_n$ (so $\mathbb{Q}_n = \mathbb{Q}(\mu_n)$), and by $\hat{\mu}_n$ the set (whose elements I'll generally write as ξ) of primitive/generating elements in the group μ_n, the nth cyclotomic polynomial $\Phi_n := \mathrm{Irr}(\xi, \mathbb{Q})$ equals $\Phi_n = \prod_{\xi \in \hat{\mu}_n}(x-\xi) \implies \deg(\Phi_n) = |\hat{\mu}_n| = \varphi(n)$. In other words, the roots of Φ_n in $\mathbb{Q}_n = \mathbb{Q}(\mu_n)$ are exactly the elements of order n ($\min\{k \in \mathbb{N}^+ : \xi^k = 1\} = n$).

I now claim that $\Phi_n(x^2)$ splits into distinct linear factors in $\mathbb{Q}_{2n} = \mathbb{Q}(\mu_{2n})$. First note that choosing $\alpha \in \hat{\mu_{2n}} \implies \mu_{2n} = \{\alpha^0, \alpha^1, \ldots, \alpha^{2n-1}\}$, the elements $\{\alpha^0, \alpha^2, \ldots, \alpha^{2n-2}\}$ are all order $\leqslant n \implies$ contained in μ_n, but since both sets have size n, we must actually have equality $\mu_n = \{\alpha^0, \alpha^2, \ldots, \alpha^{2n-2}\}$. Then, since $\Phi_n(x^2) = \prod_{\xi \in \hat{\mu}_n}(x^2 - \xi)$, for each $\xi \in \hat{\mu}_n \subseteq \mu_n$ we must have $\xi = \alpha^{2k}$, so $(x^2 - \xi) = (x^2 - \alpha^{2k}) = (x - \alpha^k)(x + \alpha^k)$, meaning $\Phi_n(x^2)$ splits in $\mathbb{Q}(\mu_{2n})$. Moreover, the linear factors are distinct because $-\alpha^k \neq \alpha^k$ (otherwise $\alpha^k = 0$), and the roots of each $(x^2 - \xi_i)$ can't be the roots of some other $(x^2 - \xi_j)$, since their squares ξ_i and ξ_j are distinct. In particular, this shows that Z, the set of roots (zeroes) of $\Phi_n(x^2)$ in $\mathbb{Q}(\mu_{2n})$ has size $|Z| = 2|\hat{\mu}_n| = 2\varphi(n)$.

Now suppose α is any root of $\Phi_n(x^2)$ (in $\mathbb{Q}_{2n} = \mathbb{Q}(\mu_{2n})$) $\iff \alpha^2$ is a root of $\Phi_n(x) \iff \alpha^2$ is an element of order exactly n. We showed in the previous paragraph that α must be in μ_{2n}. While it is not true that every element of μ_{2n} can be such an α, it is true that *primitive* $2n$th roots of unity α are roots of $\Phi_n(x^2)$, since if α has order exactly $2n$, then α^2 has order exactly n. This however may not be a necessary condition: say the order of α is k; then $(\alpha^2)^k = (\alpha^k)^2 = 1 \implies k \geqslant n$ (by definition of order $n = \min\{k \in \mathbb{N}^+ : (\alpha^2)^k = 1\}$), but because $\alpha^{2n} = 1$, we must have $k \mid 2n$, thus leaving 2 possibilities, $k = n$ or $k = 2n$. In summary, we have $\hat{\mu}_{2n} \subseteq Z \subseteq \hat{\mu}_{2n} \cup \hat{\mu}_n$.

We already know that $|Z| = 2\varphi(n)$. On the other hand, $|\hat{\mu}_{2n}| = \varphi(2n)$, and $|\mu_{2n} \cup \hat{\mu}^n| = |\hat{\mu}_{2n}| + |\hat{\mu}_n|$ (because no element has both order n and $2n$) $= \varphi(2n) + \varphi(n)$. We must now understand how $\varphi(2n)$ and $\varphi(n)$ relate: recall that $\varphi(mn) = \varphi(m)\varphi(n)$ for relatively prime $m, n \in \mathbb{N}^+$ (essentially by the Chinese remainder theorem), and $\varphi(p^k) = p^k - p^{k-1}$ (because sharing factors with $p^k \iff$ having p as a factor, and there are $p^{k-1} = |\{1 \cdot p, 2 \cdot p, \ldots, p^{k-1} \cdot p\}|$ multiples of p in $[p^k]^+$), so if n is odd, then $\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$, and if n is even, say $2^k \cdot m$ ($k \in \mathbb{N}^+, 2 \nmid m$), then $\varphi(2n) = \varphi(2^{k+1} \cdot m) = (2^{k+1} - 2^k)\varphi(m) = 2(2^k - 2^{k-1})\varphi(m) = 2\varphi(n)$.

Therefore, if n is odd, then $2\varphi(n) = |Z| \leqslant |\hat{\mu}_{2n} \cup \hat{\mu}_n| = \varphi(2n) + \varphi(n) = 2\varphi(n)$, forcing the containment $Z \subseteq \hat{\mu}_{2n} \cup \hat{\mu}_n$ to be an equality, in which case $\Phi_n(x^2) = \prod_{\alpha \in Z}(x - \alpha) = \prod_{\alpha \in \hat{\mu}_{2n}}(x - \alpha) \cdot \prod_{\xi \in \hat{\mu}_n}(x - \xi) = \Phi_{2n}(x) \cdot \Phi_n(x)$, where Φ_n, Φ_{2n} are irreducible over $\mathbb{Q}$; and if n is even, $2\varphi(n) = \varphi(2n) = |\hat{\mu}_{2n}| \leqslant |Z| = 2\varphi(n)$, forcing the containment $\hat{\mu}_{2n} \subseteq Z$ to be an equality, in which case $\Phi_n(x^2) = \prod_{\alpha \in \hat{\mu}_{2n}}(x - \alpha) = \Phi_{2n}(x)$, which again is irreducible over $\mathbb{Q}$. In summary, the irreducible factorization of $\Phi_n(x^2)$ over $\mathbb{Q}$ is

$$\boxed{\Phi_n(x^2) = \begin{cases} \Phi_{2n}(x) \cdot \Phi_n(x) & \text{if } n \text{ is odd} \\ \Phi_{2n}(x) & \text{if } n \text{ is even} \end{cases}}.$$

210B Homework 7

Daniel Rui - 3/17/21

Problem 1

We are asked to explicitly construct a field with 9 elements, and to write out its addition and multiplication tables. I showed in Problem 4 below that if f is irreducible of degree n over $\mathbb{F}_3 := \mathbb{Z}/3\mathbb{Z}$, then $K := \mathbb{F}_3[x]/f\mathbb{F}_3[x]$ is a field with 3^n elements (in fact $K \simeq \mathbb{F}_{3^n}$, since $\mathbb{F}_{3^n}$ is the only field of 3^n elements up to isomorphism, as we know from 2/11/22). Well, $f := x^2 + 1 \in \mathbb{F}_3[x]$ is irreducible over $\mathbb{F}_3$ (the only way f can factor non-trivially is into linear factors, i.e. have a root in $\mathbb{F}_3$, but modulo 3/in $\mathbb{F}_3$ we have that $0^2 + 1 = 1 \neq 0$ and $1^2 + 1 = 2 \neq 0$ and $2^2 + 1 = 1 \neq 0$, so indeed f has no roots in $\mathbb{F}_3$), and so $K := \mathbb{F}_3[x]/f\mathbb{F}_3[x]$ is a field with 9 elements.

Then we have 9 distinct elements $\{a+bx\}_{a,b\in[3]^+}$ (distinct because $a_1+b_1x = a_2+b_2x \iff (a_1-a_2)+(b_1-b_2)x \in (x^2+1)\mathbb{F}_3[x]$, and by degree considerations the only possibility is that $a_1-a_2 = b_1-b_2 = 0$), hence these are all the elements of K. The addition table is trivial, and the multiplication table is not much more difficult: as an example, $(1+2x)(x+2) = 2x^2+5x+2 = 2(-1)+5x+2 = 5x = 2x$, where we used that $x^2 = -1$ in K. I fill in some values, but rest assured the rest are the result of equally easy computations:

$+$	0	1	2	x	$1+x$	$2+x$	$2x$	$1+2x$	$2+2x$
0	0								
1		2		$1+x$					
2								$2x$	
x							0		
$1+x$									0
$2+x$									
$2x$		$1+2x$				2			
$1+2x$						0			
$2+2x$									$1+x$

$\cdot$	0	1	2	x	$1+x$	$2+x$	$2x$	$1+2x$	$2+2x$
0	0								
1		1		x					
2								$2+x$	
x							1		
$1+x$					$2x$				
$2+x$									
$2x$		$2x$				$x+1$			
$1+2x$						$2x$			
$2+2x$									$2x$

Problem 3

We want to prove that $\mathbb{F}_q$ (a finite field of q elements) is isomorphic to a subfield of $\mathbb{F}_{q'}$ if and only if q' is a power of q. In Problem 10 of Homework 6, I mentioned that there is a proof of the fact that finite subgroups of the group of units of a field are cyclic (which we proved in class 2/11/22), done using the lemma that if a finite group G of order n is s.t. $d \mid n \implies |\{x \in G : x^d = 1\}| \leqslant d$ (true if G is a subgroup of the group of units of some field, by the factor theorem — see Problem 6 of Homework 6 below), then in fact $|\{x \in G : x^d = 1\}| = d$ for all $d \mid n \implies$ there is an order n element $\implies G$ is cyclic. From the "elephant teacup formula" $a^n - b^n = (a-b)(a^{n-1}b^0 + \ldots + a^0b^{n-1})$ (also used in Problem 2 of the Midterm below), we have that $k \mid n \implies (p^k - 1) \mid (p^n - 1)$, and so the aforementioned lemma gives that $|\{x \in \mathbb{F}_{q'} : x^{p^k} = x\}| = |\{0\} \cup \{x \in \mathbb{F}_{q'}^\times : x^{p^k-1} = 1\}| = 1 + p^k - 1 = p^k$. It is easy to check that $\{x \in \mathbb{F}_{q'}^\times : x^{p^k} = x\}$ is a field ("freshman's dream" is used here), and so indeed $\mathbb{F}_q$ is isomorphic to a subfield of any $\mathbb{F}_{q'}$ where $q' = p^n$ is a power of $q = p^k$ ($\iff k \mid n$).[†]

For the other direction, we start with $\mathbb{F}_q$ isomorphic to a subfield of $\mathbb{F}_{q'}$, say $q = p_1^k$ and $q' = p_2^n$. By Lagrange (thinking of each field solely as an additive group), we must have $p_1 \mid p_1^k \mid p_2^n$, and by primality $p_1 \mid p_2 \implies p_1 = p_2 =: p$. For convenience, I will let $\mathbb{F}_q$ denote the relevant subfield of $\mathbb{F}_{q'}$, and also denote by $\mathbb{F}_p$ the isomorphic copy of $\mathbb{Z}/p\mathbb{Z}$ in $\mathbb{F}_q$, so that $\mathbb{F}_p \subseteq \mathbb{F}_q \subseteq \mathbb{F}_{q'}$. From 2/11/22[‡] we know that $|\mathbb{F}_q| = p^{[\mathbb{F}_q : \mathbb{F}_p]}$, so $[\mathbb{F}_q : \mathbb{F}_p] = k$ and $[\mathbb{F}_{q'} : \mathbb{F}_p] = n$. Finally from the "tower property" we know that $[\mathbb{F}_q : \mathbb{F}_p] \cdot [\mathbb{F}_{q'} : \mathbb{F}_q] = [\mathbb{F}_{q'} : \mathbb{F}_p]$, so in particular $k \mid n$, so indeed $q' = p^n$ is a power of $q = p^k$.

Problem 4

Let f be an irreducible polynomial of degree n over a finite field $\mathbb{F}_q$. We want to prove that f divides $x^{q^n} - x$. Note that since $\mathbb{F}_q$ is a field we can assume that f is monic (just multiply by the inverse of the leading coefficient). Then, we know from 2/7/22 that $K := \mathbb{F}_q[x]/f\mathbb{F}_q[x]$ is a field extension of $\mathbb{F}_q$ (or rather the isomorphic copy $\mathbb{F}_q + f\mathbb{F}_q[x]$ of $\mathbb{F}_q$ in K) of degree n containing a root α of f, i.e. K as a vector space over $\mathbb{F}_q$ has a basis $\{x_1, \ldots, x_n\}$, meaning every element of K has a unique representation $\sum_{i=1}^n a_i x_i$ for $a_i \in \mathbb{F}_q$, and so in total $|K| = q^n$ (q choices for each a_i).

We know from 2/11/22 that there is only one field of size q^n (up to isomorphism), namely we have $K \simeq \mathbb{F}_{q^n}$. We also know from 2/11/22 that every element of $\mathbb{F}_{q^n}$ (hence K) is a root of $x^{q^n} - x$. In particular, α is a root. But because f is assumed monic and irreducible, $f = \mathrm{Irr}(\alpha, \mathbb{F}_q)$, and from 2/7/22 we know that it must divide any other polynomial with α as a root, so indeed $f \mid x^{q^n} - x$ in $\mathbb{F}_q[x]$, as desired.

[†] alternatively, one can just use the result that $\mathbb{F}_{q'}^\times$ is cyclic, and the fact from Homework 1 Problem 2(b) that for a cyclic group G of order n, there is exactly one subgroup of order $k \mid n$, all of whose elements satisfy $a^k = 1$. This gives the lower bound $|\{x \in \mathbb{F}_{q'}^\times : x^{p^k} = x\}| \geqslant p^k$, and the other direction comes from the factor theorem, as mentioned above.

[‡] any finite field F must have some positive characteristic, i.e. the only field homomorphism $\varphi : \mathbb{Z} \hookrightarrow F$ (field homomorphism fixed by $0 \mapsto 0$, $1 \mapsto 1$) must have a prime ideal $p\mathbb{Z}$ as kernel (prime because 1st iso. thm. gives $\mathbb{Z}/\ker\varphi$ is isomorphic to a subring of F, which is in particular an integral domain), and we define $\mathrm{char}\, F := p$. Then any finite field of characteristic p has a subfield isomorphic to $\mathbb{Z}/p\mathbb{Z}$, and so $[F : \mathbb{Z}/p\mathbb{Z}]$ is some $n \in \mathbb{N}^+$. Thus F as a vector space over $\mathbb{Z}/p\mathbb{Z}$ has a basis $\{x_1, \ldots, x_n\}$, meaning every element of F has a unique representation $\sum_{i=1}^n a_i x_i$ for $a_i \in \mathbb{Z}/p\mathbb{Z}$, and so in total $|F| = p^n$ (p choices for each a_i).

Problem 10

Let F be a field of characteristic p. We want to show that the rational function field $E := F(x)$ is a normal extension of $K := F(x^p) \subseteq E$ (see the footnote to Homework 6 Problem 4 for an attempt at explaining what exactly $F(x^p)$ "means"). Recall from class 2/14/22 that a finite f.e. E of K is normal (over K) if E is a splitting field of some polynomial $f \in K[t]$. In this case, consider the polynomial $f := t^p - x^p \in K[t] = F(x^p)[t]$. Obviously, $x \in E := F(x)$ is a root of this polynomial, so the degree of the extension $E := F(x) = K(x)$ over K is $\leqslant \deg f = p$ (in particular the extension is finite). Moreover, because f is characteristic p, "freshman's dream" gives that $f := t^p - x^p = (t - x)^p$, where $(t - x) \in E[t] := F(x)[t]$ is a linear factor. In other words, f splits in $E[t]$ (and E is minimal in this regard, because x is a root and hence must be included — see 2/9/22 for more details). Thus, $E := K(x)$ is a splitting field of $f \in K[t]$, and we are done.

210B Midterm

Daniel Rui - 2/20/21

Problem 1

We are asked to find a (single) generator of the ideal $(2, 5+3i) \triangleleft \mathbb{Z}[i]$. We know from class 1/3/22 that $\mathbb{Z}[i]$ is a Euclidean domain with Euclidean function $\varphi(a+bi) = a^2+b^2$. We also proved 1/3/22 that all Euclidean domains (EuD) are principal ideal domains (PID), by showing that given any ideal I of a EuD R, any $a \in I$ s.t. $\varphi(a) = n := \min_{x \in I \setminus \{0\}} \varphi(x)$ generates the entire ideal I. In our case, the ideal $I := (2, 5+3i) \triangleleft \mathbb{Z}[i]$ is the sum of the lattices $2\mathbb{Z}[i]$ and $(5+3i)\mathbb{Z}[i]$. The fact that $\mathbb{Z}[i]$ is a PID tells us the sum of any lattices of $\mathbb{Z}[i]$ is itself a lattice, so finding $\min_{x \in I \setminus \{0\}} \varphi(x)$ is the same as finding the closest (non-zero) lattice point of $2\mathbb{Z}[i] + (5+3i)\mathbb{Z}[i]$ to the origin, or equivalently finding the (square of the) minimum distance between any two points from each respective lattice.

Well, $4+4i \in 2\mathbb{Z}[i]$ is quite close to $5+3i$, namely the (squared) distance between them is $|1-i|^2 = (1-i)(1+i) = 2$. The formula $(1-i)(1+i) = 2$ immediately indicates that $2 \in (1-i)\mathbb{Z}[i]$, i.e. $2\mathbb{Z}[i] \subseteq (1-i)\mathbb{Z}[i]$, and $5+3i = (4+4i) + (1-i) \in 2\mathbb{Z}[i] + (1-i)\mathbb{Z}[i] = (1-i)\mathbb{Z}[i]$, so indeed $I = (2, 5+3i) \subseteq (1-i)\mathbb{Z}[i]$. Again, $1-i = 5+3i-(4+4i) \in I$, so we have equality $I = (i-1)\mathbb{Z}[i]$, and we are done.

Problem 2

We want to prove that the polynomial $x^7+y^7+z^7$ is irreducible in $\mathbb{C}[x,y,z]$. First, let us recall some results from class. On 1/10/22, we showed if R is a UFD, then $R[x]$ is a UFD too (and hence for any $R[x_1, \ldots, x_n]$ too by induction). We also showed (again 1/10/22) that for a UFD R, a non-constant polynomial $f \in R[x]$ is irreducible in $R[x] \iff f$ is primitive and is irreducible in $F[x]$, where $F := .\operatorname{Frac} R$.

In our situation, denote $R := \mathbb{C}[x,y,z] \rightsquigarrow F := \mathbb{C}(x,y)$, so that $f = x^7+y^7+z^7 \in R[z]$. As f is monic in $R[z]$, it is in particular primitive (see lecture 1/7/22). Thus by the aforementioned results, showing $x^7+y^7+z^7$ is irreducible in $R[z]$ is equivalent to showing f is irreducible in $F[z]$. Now recall (again 1/10/22) Eisenstein's criterion, which says that for a UFD R, a polynomial $f = a_n x^n + \ldots + a_0$ and $F := \operatorname{Frac} R$, if some irreducible $\equiv$ prime ("$\equiv$" in any UFD) $p \in R$ satisfies (in R) (1) $p \nmid a_n$, (2) $p \mid a_i$ for $i \in [n-1] = \{0, \ldots, n-1\}$, and (3) $p^2 \nmid a_0$, then f is irreducible in $F[x]$. Therefore, to reach our desired conclusion, it suffices to find a irreducible $\equiv$ prime factor p of x^7+y^7 in $\mathbb{C}[x,y]$ that doesn't divide it twice (since then all three conditions (1) $p \nmid 1$, (2) $p \mid x^7+y^7$, (3) $p^2 \nmid x^7+y^7$ are obviously satisfied). I will call such a desired p an "Eisenstein prime".

We can factor x^7+y^7 in $\mathbb{C}[x,y]$ using the elephant-teacup formula (seems to be a rare name — I heard it from my old teacher Jim Morrow at UW) $a^n-b^n = (a-b)(a^{n-1}+a^{n-2}b+\ldots+ab^{n-2}+b^{n-1})$; taking $a = x$ and $b = -y$ and $n = 7$, we get the factorization $x^7+y^7 = (x+y)(x^6-x^5y+x^4y^2-x^3y^3+x^2y^4-xy^5+y^6)$.

I'm not quite sure how to show the unique factorization of x^7+y^7 in the UFD $\mathbb{C}[x,y]$ only contains one factor of $(x+y)$, so I will just go back to x^7+y^7 and simply prove that an Eisenstein prime merely *exists*, but not construct it (which is good enough for this question anyways). Just submitted to Canvas, but one way to show $(x+y)$ does not divide that $x^6+\ldots$ polynomial is by noticing that if it did, then plugging in any complex number $-c$ in for y would make $+c$ a root of that polynomial (since $x^6+\ldots=(x+y)(\ldots) \implies c$ is a root of $(x+(-c))(\ldots)$), and we can quickly verify that plugging in $y=-c=-1$, the value $c=1$ is *not* a root of $x^6-x^5(-1)+x^4(-1)^2-x^3(-1)^3+x^2(-1)^4-x(-1)^5+(-1)^6=x^6+x^5+x^4+x^3+x^2+x+1$.

Suppose f.s.o.c. that every irreducible $\equiv$ prime factor of x^7+y^7 in the UFD $\mathbb{C}[x,y]$ divides it twice. Then the prime factorization looks like $f=p_1^{k_1}\cdots p_s^{k_s}$ where $k_i\geqslant 2$ for all $i\in[s]^+:=\{1,\ldots,s\}$ and $p_i\in\mathbb{C}[x,y]$. I now claim that taking the formal x derivative, $\partial_x f$ will still be divisible by all the p_i. I will prove this for p_1, and the full claim will follow by symmetry. Observe that $\partial_x f=(\partial_x p_1)\cdot k_1\cdot p_1^{k_1-1}(p_2^{k_2}\cdots p_s^{k_s})+p_1^{k_1}\cdot\partial_x(p_2^{k_2}\cdots p_s^{k_s})$, which is indeed divisible by p_1. In other words, if there does not exist an Eisenstein prime, then $\gcd(f,\partial_x f)\neq 1$ (in fact we've shown that if there is even a *single* prime factor that divides x^7+y^7 twice, then $\gcd(f,\partial_x f)\neq 1$).

However, this is a contradiction because $\partial_x(x^7+y^7)=7x^6$, and $\gcd(x^7+y^7,7x^6)=1$ because any non-constant factor of $7x^6$ is of the form x^k, and if $x^k\mid x^7+y^7$, then of course $x\mid x^7+y^7$, which is not true because if it were, then $xf=x^7+y^7\implies x(f-x^6)=y^7\implies x\mid y^7\implies x\mid y$ (by primality $\equiv$ irreducibility of y in $\mathbb{C}[x,y]$); contradiction. Thus, there does in fact exist an Eisenstein prime, so $z^7+x^7+y^7$ is irreducible in $\mathbb{C}(x,y)[z]$, and hence in $\mathbb{C}[x,y,z]$ as well, and we are done.

Remarks: the same proof works for any x^n+y^m $(n,m\in\mathbb{N}^+)$ over any characteristic zero field k in place of $\mathbb{C}$, and indeed continues to work over any characteristic $p>0$ field as long as at least one of n,m aren't divisible by p (important because we used $\gcd(x^7+y^7,7x^6)=1$ to derive a contradiction, and this wouldn't work if $p\mid n\implies nx^{n-1}=0$) — I specify "at least one of n,m" because even if x doesn't work, we can take the y derivative instead.

Problem 3

Let $R:=\mathbb{Z}[x,y]$ be a polynomial ring and let $I:=(x,y)\triangleleft R$ be the ideal of R generated by x and y. We are asked to construct an exact sequence sequence of R-modules $0\to R\overset{\iota}{\hookrightarrow}R\oplus R\overset{\pi}{\twoheadrightarrow}I\to 0$, and to also determine whether or not I is projective. Let us define $\pi:R\oplus R\to I$ as the map $(f,g)\mapsto xf+yg$, which is indeed surjective because by definition $I:=\{xf+yg:f,g\in R\}$, and has kernel $\ker(\pi):=\{(f,g)\in R\oplus R:xf=-yg\}$. Then, defining $\iota:R\to R\oplus R$ to map $h\mapsto(-yh,xh)$, we see that

- $\mathrm{im}(\iota)\subseteq\ker(\pi)$ because indeed $x(-yh)=-y(xh)$;
- $\mathrm{im}(\iota)\supseteq\ker(\pi)$ because $xf=-yg\implies x\mid yg\implies x\mid g$ (since x is irreducible $\equiv$ prime in the UFD R, and $x\nmid y$) implies $xh_1=g$ for some $h_1\in R$, and similarly $yh_2=f$, so $xyh_2=-xyh_1\implies xy(h_2+h_1)=0\implies -h_2=h_1=:h$ (since R is an integral domain an $xy\neq 0$), i.e.

$(f, g) = (-yh, xh) =: \iota(h)$;

- and ι is injective because $\iota(h_1) = \iota(h_2) \implies xh_1 = xh_2 \implies x(h_1 - h_2) = 0 \implies h_1 = h_2$ (again using that R is an integral domain).

We have now completed the verification that $0 \to R \overset{\iota}{\hookrightarrow} R \oplus R \overset{\pi}{\twoheadrightarrow} I \to 0$ is a short exact sequence. Moving to the projectivity of I, recall that in class 1/14/22 we proved that free modules are projective, and then used this to prove that an R-module P is projective $\iff$ P is a direct summand of a free module; we also proved in class 11/29/21 that given a s.e.s. $0 \to A \overset{\iota}{\hookrightarrow} B \overset{\pi}{\twoheadrightarrow} C \to 0$ in an abelian category (such as R-**Mod**), $B \simeq A \oplus C$ if and only if the s.e.s. splits, and also if C is projective, then any s.e.s. $0 \to A \hookrightarrow B \twoheadrightarrow C \to 0$ splits. Hence, since $R \oplus R = R^2$ is a free R-module, we see that I being projective $\implies$ the s.e.s. we constructed splits $\iff R^2 \simeq I \oplus R \implies I$ is a direct summand of a free module $\implies I$ is projective.

Thus, to conclude that I is *not* projective, it suffices (and is necessary) to show that the s.e.s. we constructed does not split. The aforementioned result from 11/29/21 also tells us in an abelian category the notions of "right split" and "left split" are equivalent, so to show I is not projective as an R-module, we will proceed by showing that there does not exist any splitting of ι, i.e. any R-module homomorphism $k : R \oplus R \to R$ s.t. $k \circ \iota = 1_R \iff k(-yh, xh) = h$ for all $h \in R$.

Well, if such a k existed, then denoting $k(1, 0) =: f_0$ and $k(0, 1) =: g_0$, then by linearity, $1 = k(-y \cdot 1, x \cdot 1) = k(-y, 0) + k(0, x) = -y \cdot k(1, 0) + x \cdot k(0, 1) = -yf_0 + xg_0$, so $xg_0 = 1 + yf_0$. Obviously, x divides the LHS, but it can not possibly divide the RHS, because if it did, then there would be some $f \in R = \mathbb{Z}[x, y]$ s.t. $xf = 1 + yf_0$, but every term/monomial of xf must have an x, whereas the term/monomial 1 on the RHS has no x in it. Thus, any such k is "self-defeating", meaning the s.e.s. we constructed does not split, so in fact I is not projective as an R-module.

Problem 4

Let $a_1, \ldots, a_n$ be elements of a commutative ring R generating the unit ideal in R. We want to show that the submodule M in R^n consisting of all n-tuples $(x_1, \ldots, x_n) \in R^n$ s.t. $a_1x_1 + \ldots + a_nx_n = 0$ is projective. Recall that in class 1/14/22 we proved that free modules are projective, and then used this to prove that an R-module P is projective $\iff$ P is a direct summand of a free module; we also proved in class 11/29/21 that given a s.e.s. $0 \to A \overset{\iota}{\hookrightarrow} B \overset{\pi}{\twoheadrightarrow} C \to 0$ in an abelian category (such as R-**Mod**), $B \simeq A \oplus C$ if and only if the s.e.s. splits.

Now observe that defining ι to simply be the identity map/embedding $\iota : M \hookrightarrow R^n$ (since M is a submodule of R^n), and $\pi : R^n \to R$ to be the map $(x_1, \ldots, x_n) \mapsto a_1x_1 + \ldots + a_nx_n$, the kernel of π is exactly $M = \text{im}(\iota)$ by definition of M, and also π is surjective because $a_1, \ldots, a_n$ generate the unit ideal (i.e. there exist $x_1, \ldots, x_n \in R$ s.t. $a_1x_1 + \ldots + a_nx_n = 1 \implies ra_1x_1 + \ldots + ra_nx_n = r$ for all $r \in R$). In other words, $0 \to M \overset{\iota}{\hookrightarrow} R^n \overset{\pi}{\twoheadrightarrow} R \to 0$ is a short exact sequence. As R^n is a free R-module, it suffices to show that this sequence splits, so that $R^n \simeq M \oplus R \implies M$ is a direct summand of a free module $\iff M$ is projective.

The last step is to recall one last fact from 11/29/21, which is that if C is projective, then any s.e.s. $0 \to A \hookrightarrow B \twoheadrightarrow C \to 0$ splits. Since the proof (essentially by picture) is so short, I will just include it as a nice refresher:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \hookrightarrow & B & \twoheadrightarrow & C & \longrightarrow & 0 \\ & & & & & \nwarrow^{\exists h} & \uparrow{\scriptstyle 1_C} & & \\ & & & & & & C & & \end{array}$$

I already mentioned above that free modules are projective, whence we see in particular that R is projective as an R-module, meaning our s.e.s. $0 \to M \overset{\iota}{\hookrightarrow} R^n \overset{\pi}{\twoheadrightarrow} R \to 0$ does indeed split.

Problem 5

Let M, N, L be finitely generated (f.g.) R-modules over a PID R s.t. $M \oplus L \simeq N \oplus L$. We are asked to determine if the modules M, N are necessarily isomorphic. Recall from class 1/28/22 the statement of the decomposition theorem for f.g. modules over a PID R in invariant factor form: for a f.g. module M over a PID R, we can decompose $M \simeq R^n \oplus M_{\text{tors}}$ where M_{tors} is the (f.g. of course) torsion part of M, which can be decomposed further into $M_{\text{tors}} \simeq {}^{R}\!/_{I_1} \oplus \ldots \oplus {}^{R}\!/_{I_s}$ for some ideals $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_s \lhd R$; moreover, the rank n and the invariant factors $\{I_1, \ldots, I_s\}$ are uniquely determined by M, so two f.g. R-modules are isomorphic $\iff$ they have the same rank n and same set of invariant factors.

However, since we will be considering direct sums $M \oplus P$, $N \oplus P$, "adding" two invariant factor decompositions may not result in an invariant factor decomposition because the two different increasing chains $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_s \lhd R$ may not be compatible. The elementary divisor form of the decomposition theorem does not have this problem, so let me state that form of the theorem: for a f.g. module M over a PID R, we can decompose $M \simeq R^n \oplus M_{\text{tors}}$ where M_{tors} is the (f.g. of course) torsion part of M, which can be decomposed further into $M_{\text{tors}} \simeq \bigoplus_{P \lhd_{\text{pr}} R} \bigoplus_{i=1}^{r_P} {}^{R}\!/_{P^{\alpha_{P,i}}}$, where we are summing over all prime ideals $P \lhd_{\text{pr}} R$, and only finitely many of the $\alpha_{P,i} \in \mathbb{N}$ are non-zero (hence only finitely many r_P are non-zero); moreover, the rank n and the multiset of elementary divisors $\text{ED}(M) := \{P^{\alpha_{P,i}}\}_{P \lhd_{\text{pr}} R}$ are uniquely determined by M, so two f.g. R-modules are isomorphic $\iff$ they have the same rank n and same set of elementary divisors.

Using this theorem, the finitely generated modules M, N, L over the PID R each have elementary divisor decompositions, and the elementary divisor decomposition of the direct sums $M \oplus L$ and $N \oplus L$ just amount to taking the union of the multisets of exponents $\text{ED}(M), \text{ED}(N), \text{ED}(L)$. Thus if the multisets $\text{ED}(M), \text{ED}(N)$ both unioned with $\text{ED}(L)$ give the same multiset $\text{ED}(M \oplus L) = \text{ED}(N \oplus L)$ (again since the multiset of elementary divisors is uniquely determined by the module), then it must be that $\text{ED}(M) = \text{ED}(N)$ as multisets, since the union of multisets (a set S with a counter function $\# : S \to \mathbb{N}$ that keeps track of how many of each element there are) just amounts to adding together the counts, and of course $a+c = b+c \implies a = b$). Finally again using uniqueness, $\text{ED}(M) = \text{ED}(N) \implies M \simeq N$ as R-modules.

210B Homework 6

Daniel Rui - 3/6/21

Problem 1

Let K/F be a field extension and α, β be elements $\in K$. We want to show that if $a := [F(\alpha) : F]$ and $b := [F(\beta) : F]$ are relatively prime, then $[F(\alpha, \beta) : F] = [F(\alpha) : F] \cdot [F(\beta) : F]$. A corollary of the "tower property" from 2/4/22 tells us that the degrees of intermediate field extensions divide the big field extension, meaning both a and b divide (and are $\leqslant$) $[F(\alpha, \beta) : F]$. Thus, $[F(\alpha, \beta) : F] \geqslant \text{lcm}(a, b)$, which is their product $a \cdot b = [F(\alpha) : F] \cdot [F(\beta) : F]$ because of relative primality.

On the other hand, we found (Cor. 3 of the "main theorem" of 2/7/22) that for any algebraic $\alpha_1, \ldots, \alpha_n$ in some field extension (f.e.) K of F, with minimal polynomials $\text{Irr}(\alpha_i, F)$ over F, the degree $[F(\alpha_1, \ldots, \alpha_n) : F] = \prod_{i=1}^n [F(\alpha_1, \ldots, \alpha_i) : F(\alpha_1, \ldots, \alpha_{i-1})] \leqslant \prod_{i=1}^n [F(\alpha_i) : F]$. This provides the other direction inequality as the above paragraph, so we are done.

Remark: as a nice review of the content of 2/7/22, recall the key observation behind the proof of the aforementioned "Cor. 3" is that for any intermediate f.e. $F \subseteq E \subseteq K$, the minimal polynomial $\text{Irr}(\alpha, E)$ of α over E must divide $\text{Irr}(\alpha, F) \in F[x] \subseteq E[x]$ (since both polynomials are in $E[x]$ and have α as a root, but $\text{Irr}(\alpha, E)$ is by definition the minimal such polynomial in $E[x]$), and so $[E(\alpha) : E] = \deg(\text{Irr}(\alpha, E)) \leqslant \deg(\text{Irr}(\alpha, F)) = [F(\alpha) : F]$.

Problem 2

We are asked[†] to determine the minimal polynomial of $\alpha := \sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$. Note that we can use difference of squares to write $(x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3}) = \big((x - \sqrt{2})^2 - 3\big)$, and similarly $(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3}) = \big((x + \sqrt{2})^2 - 3\big)$. Multiplying these together we get

$$\begin{aligned}
\prod \big(x - (\pm\sqrt{2} \pm \sqrt{3})\big) &= \big((x - \sqrt{2})^2 - 3\big)\big((x + \sqrt{2})^2 - 3\big) \\
&= \big((x - \sqrt{2})(x + \sqrt{2})\big)^2 - 3\big((x - \sqrt{2})^2 + (x + \sqrt{2})^2\big) - 3^2 \\
&= (x^2 - 2)^2 - 3\Big[\big((x - \sqrt{2}) + (x + \sqrt{2})\big)^2 - 2(x - \sqrt{2})(x + \sqrt{2})\Big] - 3^2,
\end{aligned}$$

which is clearly in $\mathbb{Q}[x]$ (after using difference of squares to get rid of all the square roots) and has α as a root. Let us call this polynomial f; as we have just found that it is in $\mathbb{Q}[x]$ and has α as a root, it must be some $\mathbb{Q}[x]$-multiple of $\text{Irr}(\alpha, \mathbb{Q})$ (see "main theorem" of 2/7/22). To prove that $f = \text{Irr}(\alpha, \mathbb{Q})$ is exactly the desired minimal polynomial, it suffices (and of course is necessary) to show that $\deg(\text{Irr}(\alpha, \mathbb{Q})) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ is 4 (because we already know $\text{Irr}(\alpha, \mathbb{Q}) \mid f$, and both are monic, so if we knew both their degrees were 4 then the only possibility is equality).

[†]for essentially the same problem with essentially the same solution, see Problem 1 of my 505 Homework 5, to the extent that I can find-replace $17 \mapsto 2$ and $239 \mapsto 3$.

First, we show $\mathbb{Q}(\alpha) := \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$ (this is not a surprise; such a claim is essentially the key behind the primitive element theorem from class 2/18/22). The $\subseteq$ direction is obvious, so we focus on the $\supseteq$ direction. Because $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\alpha)$ and $\mathbb{Q}(\alpha)$ is a field, its inverse $\frac{1}{3^2-2^2}(\sqrt{3}-\sqrt{2})$ must be in $\mathbb{Q}(\alpha)$ as well. We can multiply by (3^2-2^2), giving us that $\sqrt{3}-\sqrt{2} \in \mathbb{Q}(\alpha)$; adding this to or subtracting this from $\sqrt{2}+\sqrt{3}$, it's easy to see that $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\alpha)$, and so indeed $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$.

Now we show that $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$. We know that $\sqrt{2}$ is a root of the monic polynomial x^2-2, which is irreducible by Eisenstein, so $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. The polynomial x^2-3 is in $\mathbb{Q}(\sqrt{2})[x]$, and $\sqrt{3}$ is a root of it, so we do know that $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \leqslant 2$. If it were < 2, i.e. if it were 1, then that would mean that $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, or equivalently $\sqrt{3} = a+b\sqrt{2}$ for some $a, b \in \mathbb{Q}$.

It can't be that $b = 0$, since that would mean that $\sqrt{3} \in \mathbb{Q}$ (which is impossible since by Eisenstein x^2-3 is an irreducible polynomial with $\sqrt{3}$ as a root), and it can't be that $a = 0$, since then $\sqrt{\frac{3}{2}} = b \in \mathbb{Q}$, which is impossible since it is a root of $2x^2-3$, which is again irreducible by Eisenstein. Assuming $a, b \neq 0$, we can square both sides and rearrange, getting $\frac{1}{2ab}(3-a^2-2b^2) = \sqrt{2}$, but the LHS is rational, contradicting the fact that $\sqrt{2}$ is irrational (which we literally just proved, by saying $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$). Thus, it must be $= 2$, and we do indeed get $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$. Thus, f above must in fact be $\mathrm{Irr}(\alpha, \mathbb{Q})$, and we are done.

Problem 3

We are asked to determine the minimal polynomial over $\mathbb{Q}$ of a primitive p^n-th root of unity ξ (p prime, $n \in \mathbb{N}$). By definition, ξ has order exactly p^n (so $\xi^{p^n} = 1$, but $1 \leqslant k < p^n \implies \xi^k \neq 1$). Of course, ξ is a root of $x^{p^n}-1 \in \mathbb{Q}[x]$. But $x^{p^n}-1$ factors as $(x^{p^{n-1}}-1)(x^{p^{n-1}\cdot(p-1)}+x^{p^{n-1}\cdot(p-2)}+\ldots+x^{p^{n-1}\cdot 1}+1)$, and as ξ is not a root of $(x^{p^{n-1}}-1)$, it must be a root of $f := x^{p^{n-1}\cdot(p-1)}+x^{p^{n-1}\cdot(p-2)}+\ldots+x^{p^{n-1}\cdot 1}+1 \in \mathbb{Q}[x]$.

The easiest route now is to appeal to the general theory of cyclotomic polynomials over $\mathbb{Q}$ (from class 3/2/22), which tells us $\deg(\Phi_n) = \varphi(n)$, where Φ_n is the minimal polynomial of any primitive n-th root of unity over $\mathbb{Q}$, and $\varphi(n)$ is the Euler totient function defined as the number of elements in $[n]^+$ relatively prime to n. Since the only numbers not relatively prime to p^n in $[p^n]^+$ are $\{1\cdot p, 2\cdot p, \ldots, p^{n-1}\cdot p\}$, we have that $\varphi(p^n) = p^n - p^{n-1}$, and the f we found above is indeed $\mathrm{Irr}(\xi, \mathbb{Q})$ (it is monic, and has degree equal to that of the minimal polynomial, hence it is exactly the minimal polynomial).

Alternatively, we can show that f is irreducible "manually", by showing (using Eisenstein's criterion — see lecture 1/10/22) that $f(y+1)$ is an irreducible polynomial in $\mathbb{Q}[y]$ (this suffices because if f has a non-trivial factorization in $\mathbb{Q}[x]$, then mapping via the evaluation (ring-)homomorphism $[x \mapsto y+1] : \mathbb{Q}[x] \to \mathbb{Q}[y]$ would produce a non-trivial factorization of $f(y+1)$ in $\mathbb{Q}[y]$). As $\mathbb{Z}$ is a UFD, and the polynomial $f(y+1) \in \mathbb{Z}[y]$ is monic and has p as the constant coefficient (each $(y+1)^{p^n\cdot(p-k)}$ for $k \in [p]^+$ contributes $+1$), Eisenstein will tell us that $f(y+1)$ is irreducible in $\mathbb{Q}[y]$ if we just show that all coefficients (beside that of $y^{p^n\cdot(p-1)}$ of course, which we already said was 1) are divisible by p (as in integer multiples of p, since $f(y+1) \in \mathbb{Z}[y]$). First recall from the definition/construction of f, we have that $f(y+1)\cdot((y+1)^{p^{n-1}}-1) = (y+1)^{p^n}-1$ in $\mathbb{Z}[y]$.

Now applying the "canonical" ring homomorphism $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$ (or rather the induced ring homomorphism $\mathbb{Z}[y] \twoheadrightarrow \mathbb{F}_p[y]$, notated $f \mapsto \overline{f}$), and using "freshman's dream" we get that in $\mathbb{F}_p[y]$,

$$\overline{f(y+1)} \cdot ((y^{p^{n-1}} + 1^{p^{n-1}}) - 1) = ((y^{p^n} + 1^{p^n}) - 1) \implies \overline{f(y+1)} \cdot y^{p^{n-1}} = y^{p^n},$$

and because $\mathbb{F}_p[y]$ is an integral domain, we must have $\overline{f(y+1)} = y^{p^n - p^{n-1}} = y^{p^{n-1} \cdot (p-1)}$ (more explicitly, we rearrange to get $\overline{f(y+1)} \cdot y^{p^{n-1}} - y^{p^n} = 0 \implies y^{p^{n-1}} \cdot (\overline{f(y+1)} - y^{p^n - p^{n-1}}) = 0$, and because $y^{p^{n-1}} \neq 0_{\mathbb{F}_p[y]}$, integral domain-ness forces $\overline{f(y+1)} - y^{p^n - p^{n-1}} = 0_{\mathbb{F}_p[y]}$). In other words, all non-leading coefficients of $\overline{f(y+1)}$ vanish in $\mathbb{F}_p$.

But the only way for a coefficient in $\mathbb{Z}$ to map to $0 \in \mathbb{F}_p$ is if it's a multiple of p in $\mathbb{Z}$! So indeed we have proven that all non-leading coefficients of $f(y+1) \in \mathbb{Z}[y]$ are multiples of p, and as promised, Eisenstein gives that $f(y+1)$ is irreducible in $\mathbb{Q}[y]$, hence $f(x)$ is monic and irreducible in $\mathbb{Q}[x]$ with ξ as a root, meaning exactly that $f = \mathrm{Irr}(\xi, \mathbb{Q})$.

Problem 4

Let t be a variable over a field F, and define $s := \frac{t^2}{t-1}$. We are asked to determine the degree of the extension $[F(t) : F(s)]$[†]. Let us denote $E := F(s)$ for convenience; then $E(t) = F(t)$. We know from the "main theorem " of 2/7/22 that $[E(t) : E] = \deg(\mathrm{Irr}(t, E))$, and moreover the minimal polynomial $\mathrm{Irr}(t, E)$ divides any other $f \in E[x]$ that has t as a root. In particular, t is a root of the polynomial $x^2 - s(x-1) \in E[x]$, so $[E(t) : E] \leqslant 2$.

Recall now Eisenstein's criterion of 1/10/22, which tells us that because $F[s]$ is a UFD (we know from 1/3/22 that it is in fact an Euclidean domain), if we show that s is irreducible in $F[s]$, then $x^2 - sx - s$ will be irreducible in $(\mathrm{Frac}\, F[s])[x]$, where $\mathrm{Frac}\, F[s] =: F(s) =: E$. Well, by degree considerations (see 1/10/22), s is irreducible in $F[s]$ (again thinking of $F[s]$ as just a one-variable polynomial ring over F, without worry of any sort of "conspiracy" between s and t), implying that $\mathrm{Irr}(t, E)$ is indeed $x^2 - sx - s \implies [E(t) : E] = 2$.

[†] we can think of $F[t]$ and $F[s]$ as both polynomial rings over F with one free variable, with fraction fields $F(\bullet) := \mathrm{Frac}(F[\bullet])$ for $\bullet = t, s$ defined using the standard "equivalence classes of pairs" method, where the assertion "$s := \frac{t^2}{t-1}$" can be thought of as the "evaluation" (field-)homomorphism

$$\varphi := \left[\frac{a_n s^n + \ldots + a_0}{b_m s^m + \ldots + b_0} \mapsto \frac{a_n (\frac{t^2}{t-1})^n + \ldots + a_0}{b_m (\frac{t^2}{t-1})^m + \ldots + b_0} = \frac{a_n (t^2)^n + \ldots + a_0 (t-1)^n}{b_m (t^2)^m + \ldots + b_0 (t-1)^n} \cdot \frac{(t-1)^m}{(t-1)^n} \right] : F(s) \to F(t),$$

where it was crucial that any input $b_m s^m + \ldots + b_0 \neq 0 \in F[s]$ ($\iff$ w.l.o.g. $b_m \neq 0$) implies a non-zero denominator $b_m (t^2)^m + \ldots + b_1 (t^2)^1 (t-1)^{m-1} + b_0 (t-1)^m \neq 0 \in F[t]$ (because if $m > 0$,then this has degree $2m > 0$, and if $m = 0$, then the denominator is solely $b_0 \neq 0$), leading to a non-zero total output denominator $[b_m (t^2)^m + \ldots + b_0 (t-1)^m] \cdot (t-1)^n \neq 0$ (since $F[t]$ is an integral domain), thus making φ well-defined. Compare this to a similar-looking situation of replacing the free variable t by some α algebraic over F, in which (I think?) it is possible that $[F(t) : F(\frac{t^2}{t-1})] = 1$. Anyways, since field homomorphisms are always injective, $F(s) \simeq \varphi(F(s)) \subseteq F(t)$, and taking restrictions (to ring homomorphisms) yields $F[s] \simeq \varphi(F[s]) \subseteq F[t]$.

Note: the same argument holds for $s = \frac{f(t)}{g(t)}$ for $\deg f \neq \deg g$, since $b_m f(t)^m + \ldots + b_1 f(t)^1 g(t)^{m-1} + b_0 g(t)^m$ has degree $\max\{\deg f, \deg g\} \cdot m \geqslant 0$; this might not be true if $\deg f = \deg g$, since cancellation could occur.

Problem 5

Let K be a splitting field of the polynomial $f = x^3 - 2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$. We want to find the degree of the field extension $[K : \mathbb{Q}]$ (this question "makes sense" because we proved on 2/9/22 + a tiny bit of 2/11/22 that any two splitting fields of any non-constant polynomial are isomorphic, and hence have the same degree). Recall first from 2/9/22 that for any non-constant $f \in F[x]$, there exists a field extension K of F s.t. f splits in K, and $[K : F] \leqslant (\deg f)!$ — in particular (presented as a *Remark* in the 2/9/22 lecture) we know for sure that $[K : \mathbb{Q}] \leqslant (\deg f)! = 3! = 6$.

One route is to exploit the various analytical properties of $\mathbb{R}$ and $\mathbb{C}$ to show that the unique (again see 2/9/22) splitting field of $f \in \mathbb{Q}[x]$ contained in $\mathbb{C}$ is $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{\pi i/3}, \sqrt[3]{2}e^{2\pi i/3}) = \mathbb{Q}(\sqrt[3]{2}, e^{\pi i/3})$. Namely, the ordering properties of $\mathbb{R}$ tell us that $x^3 - 2 : \mathbb{R} \to \mathbb{R}$ is strictly increasing, and $\to \infty > 0$ as $x \to \infty$ and similarly $\to -\infty < 0$ as $x \to -\infty$, and the analytic properties of $\mathbb{R}$ tell us that it is continuous and so the intermediate value theorem gives exactly 1 zero in $\mathbb{R}$, which we denote by $\sqrt[3]{2}$. Similarly the analytic properties of $\mathbb{C}$ tell us that $e^{\pi i/3}$ is a non-real root of $x^3 - 1$ (non-real because similarly $x^3 - 1$ has exactly 1 real root by the IVT, which is $1 \neq e^{\pi i/3}$), so $[\mathbb{Q}(\sqrt[3]{2}, e^{\pi i/3}) : \mathbb{Q}(\sqrt[3]{2})]$ must be > 1. Note that $e^{\pi i/3}$ is a root of the polynomial $\frac{x^3-1}{x-1} = x^2 + x + 1 \in \mathbb{Q}[x] \subseteq \mathbb{Q}(\sqrt[3]{2})[x]$, meaning $[\mathbb{Q}(\sqrt[3]{2}, e^{\pi i/3}) : \mathbb{Q}(\sqrt[3]{2})] \leqslant 2$, and as the degree is an integer, we must have it $= 2$. For the "lower half" extension $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$, Eisenstein tells us $x^3 - 2$ is an irreducible polynomial over $\mathbb{Q}$, so (by a theorem on 2/7/22) $x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$, and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg(x^3 - 2) = 3$. By the "tower property" of 2/4/22, $[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, e^{\pi i/3}) : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6$.

Another more algebraic way is as follows: we know from 2/16/22 that for any non-constant f in any $F[x]$, it is relatively prime to its (formal) derivative $\gcd(f, f') = 1 \iff$ over *any* field extension K of F, it has no multiple roots (i.e. f is *separable*); in particular if $f \in F[x]$ is irreducible over F, it is separable $\iff f' = 0$. In our case, $f = x^3 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein, and its (formal) derivative $3x^2$ is certainly $\neq 0$, so the 3 roots of f in K are distinct. Now denote by α, β two of these distinct roots. Then, since $\alpha^3 = \beta^3 = 2$, their ratio satisfies $(\frac{\alpha}{\beta})^3 = 1$, and as α, β are distinct, $\xi := \xi_3 := \frac{\alpha}{\beta}$ is a primitive third root of unity in K (primitive meaning the order of ξ is exactly 3; in our case, we know the order must divide 3, i.e. is 3 or 1, and $\alpha \neq \beta \implies \xi^1 := \frac{\alpha}{\beta} \neq 1$).

Again, as before, Eisenstein tells us $x^3 - 2$ is an irreducible polynomial over $\mathbb{Q}$, so (by a theorem on 2/7/22) $x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$, and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg(x^3 - 2) = 3$; and one of our examples from 2/7/22 was that $[\mathbb{Q}(\xi_p) : \mathbb{Q}] = p - 1$ for all primes p (argument was that $\frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \ldots + p + 1$ is irreducible over $\mathbb{Q}$ by variable shift and Eisenstein). But a corollary of the "tower property" from 2/4/22 tells us that the degrees of intermediate field extensions divide the big field extension, meaning both $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and $[\mathbb{Q}(\xi_3) : \mathbb{Q}] = 2$ divide (and are $\leqslant$) $[K : \mathbb{Q}]$. We already established in the first paragraph of this problem that $[K : \mathbb{Q}] \leqslant 6$, which leaves the only possibility $[K : \mathbb{Q}] = 6$.

Remark: I did this before Problem 1, but obviously Problem 1 would have been helpful in the last lines of the above paragraph.

Problem 6

Let ξ be a primitive nth root of unity (in the sense that the order of ξ is exactly n). We want to show that $K := \mathbb{Q}(\xi)$ is a splitting field of the polynomial $x^n - 1$ over $\mathbb{Q}$. As K is a field[†], we know (1/3/22) that $K[x]$ is a Euclidean domain, in which we can do polynomial division, so $f = (x-\alpha)q + r \implies f(\alpha) = r(\alpha)$ (for $q, r \in K[x]$) implies that α is a root of f if and only if $(x-\alpha) \mid f$ in $K[x]$. Then because $K[x]$ is an integral domain, given any root β of f not equal to α, it must also be a root of q (of course any root of q is also a root of f). So by induction, we know that any degree n polynomial in $K[x]$ has $\leqslant n$ roots in K, and taking the product over distinct roots α of f in K, $\prod_\alpha (x-\alpha) \mid f$ in $K[x]$. This fact is known as the *factor theorem*.

Applying to the situation at hand, because $\xi^n = 1$, we have that all ξ^k for $k \in [n-1] := \{0, \dots, n-1\}$ are also roots of $x^n - 1$ (since $(\xi^k)^n = (\xi^n)^k = 1^k = 1$). These are all distinct, because otherwise we would have $\xi^{k_2 - k_1} = 1$ for some $1 \leqslant k_2 - k_1 < n$, contradicting that ξ has order exactly 1. Thus $\prod_{k=0}^{n-1}(x - \xi^k) \mid x^n - 1$, and by degree considerations (and the fact that both LHS and RHS are monic), we must have equality, meaning $x^n - 1$ splits in $K[x]$ (each linear factor $(x - \xi^k) \in K[x]$ as $\xi^k \in K$). Finally, K is "minimal" in the sense that $K := \mathbb{Q}(\xi) = \mathbb{Q}(\xi, \xi^2, \dots, \xi^{n-1})$, so by the definition of splitting field from 2/9/22, $K := \mathbb{Q}(\xi)$ is indeed a splitting field of $x^n - 1$ over $\mathbb{Q}$.

Problem 7

We are asked to find an example of isomorphic fields where one is a non-trivial field extension of the other. Recall from Problem 4 above that for any field F, the "free field generated by one variable" $F(t)$ is a degree 2 extension of $F(\frac{t^2}{t-1})$, i.e. the image of $F(\bullet)$ under the evaluation (field-)homomorphism mapping $\varphi := [\bullet \mapsto \frac{t^2}{t-1}] : F(\bullet) \to F(t)$ (which I showed was well-defined in the footnote to Problem 4 above). Field homomorphisms are automatically injective, so φ is an isomorphism between $F(\bullet) \simeq F(\frac{t^2}{t-1})$. But of course $F(\bullet) \simeq F(t)$, so $F(t) \simeq F(\frac{t^2}{t-1})$ as fields!

Problem 8

Let K be a field extension (f.e.) of F, with $\alpha \in K$. We want to show that if there is non-constant polynomial $f \in F[x]$ s.t. $f(\alpha) \in K$ is algebraic over F, then α is also algebraic over F. By definition of an algebraic element, there is some polynomial $g \in F[x]$ s.t. $g(f(\alpha)) = 0$. But $g \circ f$ is itself a polynomial in $F[x]$ (polynomial operations, i.e. multiplication and addition, applied to a polynomial, result in a polynomial because polynomial rings, or rather rings in general, are closed under those operations)! So α is the root of a polynomial in $F[x]$, which is again exactly what it means for α to be algebraic over F.

[†]since $(x-\alpha)$ is monic, the polynomial division algorithm dividing $f \in R[x]$ by $(x-\alpha)$ (for $\alpha \in R$) works in any ring R, not even needing commutativity; but then the evaluation homomorphism might not even be well-defined without commutativity. In other words, the exact arguments made in this paragraph continue to hold over integral domains, not only fields.

Problem 9

Let K be a f.e. of F, and $\alpha, \beta \in K$. We want to prove that the extension $F(\alpha, \beta)$ of $E := F(\alpha+\beta, \alpha\beta)$ is algebraic. Well, the polynomial[‡] $(x-\alpha)(x-\beta) = x^2 - (\alpha+\beta) + \alpha\beta \in E[x]$ has α, β as roots, so α, β are algebraic over E. Then by Cor. 3 of 2/7/22, $E(\alpha, \beta) = F(\alpha, \beta)$ is an algebraic extension of E.

Problem 10

We are asked to find an example of an infinite algebraic extension. Recall from 2/7/22 that a f.e. K of F is called algebraic if all $\alpha \in K$ are algebraic over F, where $\alpha \in K$ is algebraic over $F \iff [F(\alpha) : F] < \infty$ (Cor. 1 of the "main theorem" of 2/7/22). I claim that **any strictly nested sequence $F := K_0 \subsetneq K_1 \subsetneq \ldots$ of algebraic field extensions of F produces an infinite algebraic f.e. $K := \bigcup_{n=0}^{\infty} K_n$ of F**. First, K is a field because for any $\alpha, \beta \in K$, there is some $n \in \mathbb{N}$ s.t. $\alpha, \beta \in K_n$, and as K_n is a field, all 4 operations can be done on α, β in $K_n \subseteq K$. It is an algebraic f.e. of F because any $\alpha \in K$ is in some K_n, and K_n is an algebraic f.e. of F so $[F(\alpha) : F] < \infty \iff \alpha$ is algebraic over F. Finally, it is infinite because by the tower property, $[K : F] = [K : K_n] \cdot [K_n : F] \geqslant [K_n : F]$ for any $n \in \mathbb{N}$, and iteratively using the tower property yields $[K_n : F] = \prod_{i=1}^{n} [K_i : K_{i-1}] \geqslant 2^n$ (since by "strictly nested", $[K_i : K_{i-1}] \geqslant 2$ for all $i \in \mathbb{N}$), and $2^n \to \infty$ as $n \to \infty$.

As an explicit example, note first that Cor. 2 of the "main theorem" of 2/7/22 tells us any finite f.e. of F is also algebraic over F. Thus one possibility is to consider the characteristic-p fields $K_n := \mathbb{F}_{p^{2^n}}$ over $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ (for some prime p). Recall that there is a proof of the fact that finite subgroups of the group of units of a field are cyclic, done using the lemma that if a finite group G of order n is s.t. $d \mid n \implies |\{x \in G : x^d = 1\}| \leqslant d$, then in fact $|\{x \in G : x^d = 1\}| = d$ for all $d \mid n \implies$ there is an order n element $\implies G$ is cyclic. Anyways for any[§] $k \leqslant n \implies 2^k \mid 2^n \implies (p^{2^k} - 1) \mid (p^{2^n} - 1)$, this lemma gives that $|\{x \in K_n : x^{p^{2^k}} = x\}| = |\{0\} \cup \{x \in K_n^\times : x^{p^{2^k}-1} = 1\}| = 1 + p^{2^k} - 1 = p^{2^k}$. It is easy to check that $\{x \in K_n : x^{p^{2^k}} = x\}$ is a field ("freshman's dream" is used here), so indeed the $K_n := \mathbb{F}_{p^{2^n}}$ can be thought of as a strictly nested sequence of algebraic field extensions of $K_1 := \mathbb{F}_p$.

Another possibility is to start with $F := K_0 := \mathbb{Q}$ and $K_1 := \mathbb{Q}(\sqrt{2})$, and inductively define $K_{n+1} := K_n(\sqrt[[K_n:\mathbb{Q}]+1]{2})$, or perhaps more legibly $\mathbb{Q}(2^{1/([K_n:\mathbb{Q}]+1)})$. Since each K_n is the result of adjoining finitely many algebraic elements (roots of some polynomial $x^N - 2$) to $\mathbb{Q}$, Cor. 3 of the "main theorem" of 2/7/22 tells us that each K_n is an algebraic field extension of $\mathbb{Q}$. They are obviously nested, and in fact strictly so, because we know from the tower property that for any $\alpha \in K$ a f.e. of F, $\deg(\mathrm{Irr}(\alpha, F)) = [F(\alpha) : F] \leqslant [K : F]$, and in our case $\mathrm{Irr}(2^{1/([K_n:\mathbb{Q}]+1)}, \mathbb{Q}) = x^{[K_n:\mathbb{Q}]+1} - 2$ (irreducible over $\mathbb{Q}$ by Eisenstein), so $2^{1/([K_n:\mathbb{Q}]+1)}$ can't possibly be in K_n because if it were, then $[K_n : \mathbb{Q}] + 1 = \deg(x^{[K_n:\mathbb{Q}]+1} - 2) \leqslant [K_n : \mathbb{Q}]$; contradiction.

[‡] the same trick can be used to show that at least one of $\pi + e$ and πe must be transcendental, because if f.s.o.c. both are algebraic over $\mathbb{Q}$, then $(x-\pi)(x-e) = x^2 - (\pi+e)x + \pi e \in K[x]$ where $K := \mathbb{Q}(\pi + e, \pi e)$ is an algebraic extension of $\mathbb{Q}$ (Cor. 3 of 2/7/22), so $K(\pi, e)$ would be an algebraic extension of K, and because being algebraic is a "good property" (see end of 2/7/22 lecture), this would imply $K(\pi, e)$ is an algebraic extension of $\mathbb{Q}$, contradicting that π and e are transcendental (in fact we only needed one of them to be transcendental to establish that $K(\pi, e)$ is not algebraic over $\mathbb{Q}$).

[§] by the "elephant teacup formula" $a^n - b^n = (a-b)(a^{n-1}b^0 + \ldots + a^0 b^{n-1})$ — cf. Problem 2 of the Midterm above.

210B Homework 5

Daniel Rui - 2/20/21

Problem 1

210B Homework 4

Daniel Rui - 2/20/21

Problem 1

Let $a_1, \ldots, a_n$ be elements of a commutative ring R generating the unit ideal in R. We want to show that the submodule M in R^n consisting of all n-tuples $(x_1, \ldots, x_n) \in R^n$ s.t. $a_1x_1 + \ldots + a_nx_n = 0$ is projective. Recall that in class 1/14/22 we proved that free modules are projective, and then used this to prove that an R-module P is projective $\iff$ P is a direct summand of a free module; we also proved in class 11/29/21 that given a s.e.s. $0 \to A \overset{\iota}{\hookrightarrow} B \overset{\pi}{\twoheadrightarrow} C \to 0$ in an abelian category (such as R-**Mod**), $B \simeq A \oplus C$ if and only if the s.e.s. splits.

Now observe that defining ι to simply be the identity map/embedding $\iota : M \hookrightarrow R^n$ (since M is a submodule of R^n), and $\pi : R^n \to R$ to be the map $(x_1, \ldots, x_n) \mapsto a_1x_1 + \ldots + a_nx_n$, the kernel of π is exactly $M = \text{im}(\iota)$ by definition of M, and also π is surjective because $a_1, \ldots, a_n$ generate the unit ideal (i.e. there exist $x_1, \ldots, x_n \in R$ s.t. $a_1x_1 + \ldots + a_nx_n = 1 \implies ra_1x_1 + \ldots + ra_nx_n = r$ for all $r \in R$). In other words, $0 \to M \overset{\iota}{\hookrightarrow} R^n \overset{\pi}{\twoheadrightarrow} R \to 0$ is a short exact sequence. As R^n is a free R-module, it suffices to show that this sequence splits, so that $R^n \simeq M \oplus R \implies M$ is a direct summand of a free module $\iff$ M is projective.

The last step is to recall one last fact from 11/29/21, which is that if C is projective, then any s.e.s. $0 \to A \hookrightarrow B \twoheadrightarrow C \to 0$ splits. Since the proof (essentially by picture) is so short, I will just include it as a nice refresher:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \hookrightarrow & B & \twoheadrightarrow & C & \longrightarrow & 0 \\ & & & & & \nwarrow^{\exists h} & \uparrow{\scriptstyle 1_C} & & \\ & & & & & & C & & \end{array}$$

I already mentioned above that free modules are projective, whence we see in particular that R is projective as an R-module, meaning our s.e.s. $0 \to M \overset{\iota}{\hookrightarrow} R^n \overset{\pi}{\twoheadrightarrow} R \to 0$ does indeed split.

210B Homework 3

Daniel Rui - 1/27/21

Problem 1

Let M be a R-module for a c1-ring R. We define $S^{-1}M$ to be the set of pairs $(m,s) =: \frac{m}{s}$ s.t. $\frac{m_1}{s_1} = \frac{m_2}{s_2} \iff \exists t \in S$ s.t. $t(s_2m_1 - s_1m_2) = 0$, which is an equivalence; the proof is essentially word-for-word identical to the one given during the construction of $S^{-1}R$ in Homework 2 Problem 8. Using again the standard formulas for fraction addition and multiplication, we can equip $S^{-1}M$ with an $S^{-1}R$-module structure $\frac{r}{s} \cdot \frac{m}{t} := \frac{rm}{st}$, which leads to e.g.

$$\frac{r}{s} \cdot \left(\frac{m_1}{t_1} + \frac{m_2}{t_2} \right) = \frac{r}{s} \cdot \left(\frac{t_2m_1 + t_1m_2}{t_1t_2} \right) = \frac{rt_2m_1 + rt_1m_2}{st_1t_2} = \frac{rm_1}{rt_1} + \frac{rm_2}{st_2}.$$

The action of $S^{-1}R$ on $S^{-1}M$ is well defined because given $\frac{r_1}{s_1} = \frac{r_2}{s_2} \iff \exists u \in S : u \cdot (r_1s_2 - r_2s_1) = 0 \iff ur_1s_2 = ur_2s_1$ and $\frac{m_1}{t_1} = \frac{m_2}{t_2} \iff \exists v \in S : v \cdot (t_2m_1 - t_1m_2) = 0 \iff vt_2m_1 = vt_1m_2$. Multiplying these equalities together, we get $uvr_1s_2t_2m_1 - uvr_2s_1t_1m_2 = uv(r_1s_2t_2m_1 - r_2s_1t_1m_2) \iff \frac{r_1m_1}{s_1t_1} = \frac{r_2m_2}{s_2t_2}$.

Furthermore, this correspondence $M \mapsto S^{-1}M$ extends to a functor $\mathsf{L}_S : R\text{-}\mathbf{mod} \to S^{-1}R\text{-}\mathbf{mod}$ (localization at S), where we define $\mathsf{L}_S(f)$ (for a R-module homomorphism $f : M \to N$) to be the map $\frac{m}{s} \mapsto \frac{f(m)}{s}$. Verifying that this map is well defined, a $S^{-1}R$-module homomorphism (i.e. $\mathsf{L}_S(f)(\frac{m_1}{s_1} \cdot \frac{m_2}{s_2}) = \frac{f(m_1)}{s_1} + \frac{f(m_2)}{s_2}$, and $\mathsf{L}_S(f)(\frac{r}{s} \cdot \frac{m}{t}) = \frac{r}{s} \cdot \frac{f(m)}{t}$), and L_S is indeed a functor (i.e. $[\mathsf{L}_S(g) \circ \mathsf{L}_S(f)](\frac{m}{s}) = \mathsf{L}_S(g \circ f)(\frac{m}{s})$ and $\mathsf{L}_S(\mathrm{id}_M)(\frac{m}{s}) = \frac{m}{s} = \mathrm{id}_{S^{-1}M}(\frac{m}{s})$) is a straightforward but tedious symbol-bash.

Problem 2

We are asked to give an example of a non-trivial abelian group A s.t. $A \oplus A \simeq A$. We know from the classification of finitely generated abelian groups (corollary of classification of finitely generated PID-modules) that all finitely generated abelian groups are of the form $G = \mathbb{Z}^r \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/n_k\mathbb{Z}$ where $n_1 \mid \ldots \mid n_k$ are uniquely determined by G. Thus, $G \oplus G$ would have "double the factors" of G, and hence could not possibly be $\simeq G$ (because of the uniqueness part of $G \rightsquigarrow r, n_1, \ldots, n_k$ — I explained this in more detail on Problem 5 of the Midterm above).

Thus, we must consider infinitely generated abelian groups. Let $\mathbb{F}_2 := \mathbb{Z}/2\mathbb{Z}$ be the finite field over 2 elements. Then consider $A := \prod_{i=1}^{\infty} \mathbb{F}_2$, or $\coprod_{i=1}^{\infty} \mathbb{F}_2$ (same as $\prod$, except only finitely many terms in a given tuple are 0; commonly notated $\bigoplus_{i=1}^{\infty} \mathbb{F}_2$). Then, $A \oplus A$ is the set of pairs $((x_1, \ldots), (y_1, \ldots))$ for $x_i, y_i \in \mathbb{F}_2$; we can rearrange by interweaving the x-tuple and y-tuple to get $(x_1, y_1, x_2, y_2, \ldots)$, i.e. exactly the elements of A! This interweaving being an isomorphism of groups thus leads to $A \circ A \simeq A$.

Problem 3

Let A be a non-trivial abelian group A s.t. $A \oplus A \simeq A$ (e.g. the A in Problem 2 above), and let $R := \mathrm{End}(A)$, i.e. the set of homomorphisms $A \to A$, which we can endow with a ring structure of addition and composition, where addition is commutative because A is abelian. We want to show that the free modules R^n and R^m are isomorphic for all $n, m > 0$.

Well, $R^n := \{(f_1, \ldots, f_n) : f \in \mathrm{End}(A)\} = \mathrm{Hom}(\bigoplus_{i=1}^n A, A)$. Taken over finitely many rings, products $\equiv$ coproducts, so we have $\mathrm{Hom}(\bigoplus_{i=1}^n A, A) = \bigoplus_{i=1}^n \mathrm{Hom}(A, A) = \bigoplus_{i=1}^n \mathrm{End}(A) = R^n$. But $\bigoplus_{i=1}^n A \simeq A$ by induction applied to $A \oplus A \simeq A$, so $\mathrm{Hom}(\bigoplus_{i=1}^n A, A) \simeq \mathrm{Hom}(A, A) = \mathrm{End}(A) = R$. Thus indeed $R^n \simeq R$ for all $n \in \mathbb{N}^+$, so $R^n \simeq R^m$ for all $n, m \in \mathbb{N}^+$.

Problem 4

Let I be a two-sided ideal of a ring R, and let M be a left R-module. Let IM be the submodule $\{am : a \in I, m \in M\}$. We want to show that M/IM has a natural left R/I-module structure. We define $(r + I) \bullet (m + IM) := r \bullet m + IM$. We show this is well defined and satisfies the necessary distributivity/multiplicativity properties.

- Well-defined: if $(r_1+I) = (r_2+I) \iff r_1 - r_2 \in I$, and $m_1 + IM = m_2 + IM \iff m_1 - m_2 \in IM$, then
$$r_2 m_2 + IM = r_2 m_2 + \underbrace{(r_1 - r_2)}_{\in I} \cdot \underbrace{m_2}_{\in M} + \underbrace{r_1}_{\in R} \cdot \underbrace{(m_1 - m_2)}_{\in IM} + IM = r_1 m_1 + IM.$$
- Distributivity: inherited from the R-module structure of M, since $(r+I) \bullet (m+IM) := r \bullet m + IM$ is essentially just the action of R on M with an extra "$+IM$" hanging around.
- Multiplication: similarly inherited from the R-module structure on M, in particular $r_1 \cdot (r_2 m) = (r_1 r_2) \cdot m$, and $1 \cdot m = m$, again with a "$+IM$" here or there.

Problem 5

Let F be a free left R-module with basis $(f_\alpha)_{\alpha \in A}$. Let $I \triangleleft R$ be a proper 2-sided ideal. We want to prove that $(f_\alpha + IF)_{\alpha \in A}$ is a basis for the R/I-module F/IF. Well, because any $f \in F$ can be written (uniquely) as $f = \sum_{\alpha \in A} r_\alpha f_\alpha$ for $r_\alpha \in R$, all but finitely many non-zero. Applying the (canonical) projection homomorphism $\pi : F \twoheadrightarrow F/IF$, we get $f + IF = \sum_{\alpha \in A}(r_\alpha f_\alpha + IF)$, which recall from Problem 4 above $= \sum_{\alpha \in A}(r_\alpha + IF) \cdot (f_\alpha + IF)$. Thus the only thing that we still have to proe is that this sum/representation is unique. So suppose we have $\sum_{\alpha \in A}(s_\alpha + I) \cdot (f_\alpha + IM) = \sum_{\alpha \in A}(r_\alpha + I) \cdot (f_\alpha + IM)$. Unraveling definitions gives

$$\left(\sum_{\alpha \in A} s_\alpha f_\alpha\right) + IF = \sum_{\alpha \in A} \left(s_\alpha f_\alpha + IF\right) = \sum_{\alpha \in A} (s_\alpha + I) \cdot (f_\alpha + IF)$$
$$= \sum_{\alpha \in A} (r_\alpha + I) \cdot (f_\alpha + IF) = \left(\sum_{\alpha \in A} r_\alpha f_\alpha\right) + IF,$$

implying that $\sum_{\alpha\in A}(s_\alpha - r_\alpha)f_\alpha = \sum_{\alpha\in A} s_\alpha f_\alpha - \sum_{\alpha\in A} r_\alpha f_\alpha \in IF$. Say it equals some if for $i \in I, f \in F$. Then, f has a basis representation $f = \sum_{\alpha\in A} t_\alpha f_\alpha$, so $if = i\sum_{\alpha\in A} t_\alpha f_\alpha$. By uniqueness of basis representation, we must have $s_\alpha - r_\alpha = it_\alpha \in IR = I$ for all $\alpha \in A$, i.e. $s_\alpha + I = r_\alpha + I$ for all $\alpha \in A$. This is exactly the uniqueness we wanted to show, so we are done.

Problem 6

Let R be a non-zero c1-ring. We want to prove that if the free R-modules R^n and R^m are isomorphic, then $n = m$. As the hint suggests, we first reduce to the case of a field, i.e. $R = F$ is a field and F^n and F^m are vector spaces over F with bases of n and m elements respectively.

The nicest proof of this I know is Lemma 2.21 in Axler's *Linear Algebra Done Right*. A common idea is to note that given a basis, adjoining any other vector makes it linearly dependent, hence not a basis. Therefore, if we had two bases of size m, n resp., with $m < n$, we can try to get a contradiction by somehow replacing m elements of the larger basis with all m elements of the smaller basis. Axler's method of doing this replacement is quite slick: he shows in any linearly dependent (LD) set, one can remove a vector and keep the span the same; then he adds one element of the smaller basis to the larger basis making a LD set, from which he can then remove an element.

To ensure at each step he removes a vector from the original larger basis (otherwise we'd add one vector from the smaller basis, and then immediately remove it, rendering the action useless), he specifies in his removal lemma that one can choose to remove a vector $v_j \in \text{span}\{v_1, \ldots, v_{j-1}\}$, meaning as long as we adjoin the elements of the smaller basis at the front of the list of vectors from the larger basis, the removal lemma will always remove some element of the original larger basis, allowing the smaller basis to eventually complete its infiltration.

We know from class 1/3/22 that by Zorn's lemma, there is a maximal ideal $\mathfrak{m}$ in R, so $R/\mathfrak{m}$ is a field. The proof in Wiki (expanded in Alex Wertheim's Homework 3 Problem 2(b)) works by showing any isomorphism $R^n \xrightarrow{\sim} R^m$ must map $\mathfrak{m}^n = \mathfrak{m}R^n \xrightarrow{\sim} \mathfrak{m}R^m = \mathfrak{m}^m$, and so quotienting we get (using Problem 4 above) isomorphic $R/\mathfrak{m}$-modules $\equiv R/\mathfrak{m}$-vector spaces ${R^n}/{\mathfrak{m}R^n}$ and ${R^m}/{\mathfrak{m}R^m}$, where the size n, m bases of R^n and R^m resp. "push through" the projection to become bases of these quotients (by Problem 5 above), and then finally by the field case, n must equal m.

Another slightly simpler approach (no need to show $R^n \xrightarrow{\sim} R^m$ induces $\mathfrak{m}R^n \xrightarrow{\sim} \mathfrak{m}R^m$) is to simply say if R^n and R^m are isomorphic, then R^n would have two bases of n and m elements resp., say $\{x_i\}_{i=1}^n$ and $\{y_j\}_{j=1}^m$, and projecting down (again using Problem 5) to the quotient ${R^n}/{\mathfrak{m}R^n}$, we would get two bases of this $R/\mathfrak{m}$-module $\equiv$ vector space, namely $\{x_i + \mathfrak{m}R^n\}_{i=1}^n$ and $\{y_j + \mathfrak{m}R^n\}_{j=1}^m$. But we know from the field case that if a vector space has a finite basis, then all bases are that same finite size, so indeed $n = m$.

This article on invariant basis number from B. Badzioch streamlines this by defining a ring R to have the invariant basis number (IBN) property if for any free R-module F, any two bases of F have the same cardinality. Then, the projection fact from Problem 5, and Problem 4, tell us that for any proper

ideal $I \triangleleft R$, if R/I has the IBN property, then R must too (because two bases of differing cardinalities of a free R-module F can always project down to two bases of differing cardinality of the R/I-module F/IF).

Problem 7

Remark: note that $[A \mapsto \mathrm{Hom}_{\mathbb{Z}}(R, A)] : \textbf{AbGroups} \to R\textbf{-Mod}$ also appeared in lecture 1/21/22, during the proof that R-**Mod** has enough injectives (recall we proved the claim first for $R = \mathbb{Z}$, and then used the aforementioned functor to produce a desired injective R-module).

Problem 8

We want to prove that a (left) R-module M generated by one element is isomorphic to R/I, where I is some (left) ideal $\triangleleft R$. Well, let m_0 be the one element generating M, so every $m \in M$ equals $r_m \cdot m_0$ for some $r_m \in R$. Thus the R-module homomorphism $\varphi : R \twoheadrightarrow M$ mapping $r \mapsto r \cdot m_0$ is surjective (trivial to check that this is R-linear), and has kernel $\ker(\varphi) =: I$. The 1st isomorphism theorem for R-modules gives then that the quotient of the R-module R and the R-module I is isomorphic to M. It thus remains to show that this quotient is isomorphism to the quotient ring R/I interpreted as an R-module.

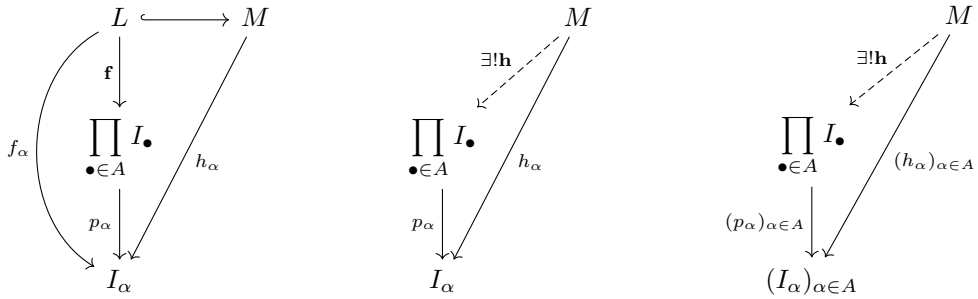
We do this using the the 1st isomorphism theorem again. Define the R-module projection homomorphism $\pi : R \twoheadrightarrow R/I$ by $r \mapsto r + I$ (again trivial to check that this is R-linear). Then $r + I = 0_{R/I} \iff r \in I$, so (the R-module) I is exactly the kernel of π, and the 1st isomorphism theorem indeed finishes things off.

Problem 9

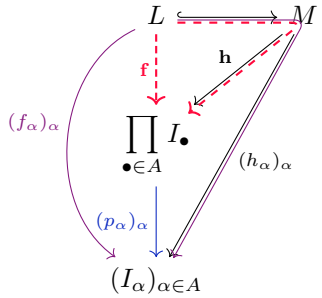
Suppose $\{I_\bullet\}_{\bullet \in A}$ is an arbitrary collection of injective (left) R-modules (or really any injective object in any category). We want to show that the product $\prod_{\bullet \in A} I_\bullet$ of these $I_\bullet$ in R-**mod** is itself an injective (left) R-module — the same result holds for coproducts of projectives, and the argument is essentially exactly the same except the arrows are reversed. In mathematical notation, our goal is to prove that the following commutative diagram on the left holds (for arbitrary "$L \hookrightarrow M$"):



Since we start off with the injectivity of the $I_\bullet$, we have the above-right commutative diagram (one for each $\alpha \in A$), where f_α is exactly $\mathbf{f}$ postcomposed with the projection map $p_\alpha : \prod_{\bullet \in A} I_\bullet \to I_\alpha$. We can represent all this in the below-left commutative diagram:



Recall now from the definition of product that we get a unique map $\mathbf{h} : M \to \prod_{\bullet\in A} I_\bullet$ (independent of α!) s.t. the above-middle diagram commutes. To emphasize that this holds for all $\alpha \in A$, I also use the notation of the above-right diagram. To summarize, we have the following diagram in which all solidly colored paths are known to commute (and also dashed red + blue = purple), and our goal is to show that the (bolded) dashed red paths are the same:



Well, because the purple paths are the same, and the dashed red paths are exactly the induced maps of the purple paths given by the universal property of the product, the *uniqueness* part of the product universal property forces them to be equal!

Problem 10

Let R be a ring. We want to prove that all (left) R-modules are projective if and only if all (left) R-modules are injective. We first prove the following

Lemma: Injectivity (and projectivity) characterized by s.e.s.

An R-module A is injective $\iff$ all short exact sequences (s.e.s.) $0 \to A \hookrightarrow B \twoheadrightarrow C \to 0$ split. Similarly, C is projective $\iff$ all such s.e.s. split.

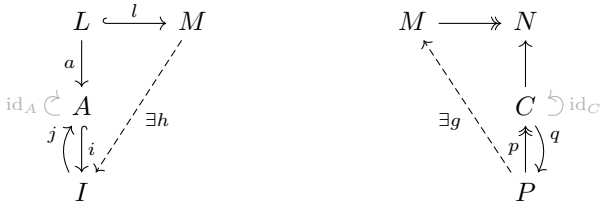
Proof: the ($\implies$) direction was already done in class 11/29/21 (see Problem 4 of the Midterm above for a refresher). Now for ($\impliedby$): recall[¶] from 1/21/22 that all R-modules, such as our given A, can be embedded into an injective module $A \overset{i}{\hookrightarrow} I$; similarly, we know from 1/14/22 that all R-modules are quotients of some free (hence projective) module, so in particular there is some projective R-module P s.t. there's a R-module homomorphism $P \overset{p}{\twoheadrightarrow} C$.

[¶] an alternative approach using "push-outs and pull-ins" (which apparently can be made to work in general abelian categories) can be found in Problem 3 of Homework 2 for my old UW 506 algebra class.

The 1st isomorphism theorem then gives the short exact sequences $0 \to A \overset{i}{\hookrightarrow} I \twoheadrightarrow I/A \to 0$, and $0 \to \ker p \hookrightarrow P \overset{p}{\twoheadrightarrow} C \to 0$. Since we assume these split, the equivalent conditions for splitting in abelian categories (e.g. R-**mod**) discussed in class 11/29/21 all hold, so in particular we have that the following diagrams commute:



Combining this with what injectivity of I and projectivity of P give us, we have the following commutative diagrams:



Adding in the compositions $j \circ h$ and $g \circ q$, we have the following diagrams in which all solidly colored paths are known to commute (and also red + blue = dashed purple for the left diagram and blue + red = dashed purple for the right), and our goal (the injectivity of A and projectivity of C) is to show that the (bolded) dashed purple paths are the same:



Well, because the two red paths (in each diagram) are the same, and the two blue paths (in each diagram) are the same, the dashed purple paths (as their composition/"sum") must also be the same! ■

Back to the original problem: with this lemma in hand, the problem is immediate, since then all (left) R-modules are injective $\iff$ all s.e.s. $0 \to A \hookrightarrow B \twoheadrightarrow C \to 0$ in R-**mod** split $\iff$ all (left) R-modules are projective.

210B Homework 2

Daniel Rui - 1/20/21

Problem 1

Suppose R is a c1-ring s.t. every $a \in R$ is idempotent, i.e. $a^2 = a$. We show that every prime ideal in R is maximal. Let $\mathfrak{p}$ be an arbitrary prime ideal of R, and consider $R/\mathfrak{p}$, which we know to be a integral domain. It suffices (and is necessary) to show that $R/\mathfrak{p}$ is actually a field. The non-zero elements of $R/\mathfrak{p}$ are exactly those (cosets) of the form $\overline{a} := a + \mathfrak{p}$ for $a \in R \setminus \mathfrak{p}$. Because quotients inherit the arithmetic operations from the "parent", we still have $\overline{a} \cdot \overline{a} = \overline{a}$ (idempotence) in $R/\mathfrak{p}$, and as $R/\mathfrak{p}$ is an integral domain, we can use the cancellation property to get $\overline{a} = \overline{1}$. This tells us that all non-zero elements of $R/\mathfrak{p}$ are in fact units, and so $R/\mathfrak{p}$ is a field ($\mathbb{Z}/2\mathbb{Z}$ I think?) as desired.

Problem 2

We want to prove that every non-zero c1-ring R has a minimal (by inclusion) prime ideal. Note that $\{0\}$ is a prime ideal (which would be minimal) if and only if R is an integral domain. As with the proof from class 1/3/22 regarding the existence of maximal ideals, we proceed by Zorn's lemma. Consider the set $\mathcal{S} := \{\mathfrak{p} : \mathfrak{p} \text{ prime ideal of } R\}$, ordered by inclusion (which I'll write as "$\geqslant$", contrary to the more standard notation of "$\leqslant$", since it is more appropriate in this situation). Then suppose we had a chain $(\mathfrak{p}_\alpha)_{\alpha \in A}$ (A totally ordered) in $\mathcal{S}$. To use Zorn's lemma, we need to prove that this chain has an "upper bound". **Claim:** $\mathfrak{P} := \bigcap_{\alpha \in A} \mathfrak{p}_\alpha$ is such a bound, i.e. $\mathfrak{P} \leqslant \mathfrak{p}_\alpha$ for all $\alpha \in A$ (obvious) and $\mathfrak{P} \in \mathcal{S}$.

Suppose f.s.o.c. that $\mathfrak{P}$ is not prime. Then there are $a, b \in R \setminus \mathfrak{P}$ but $ab \in \mathfrak{P}$. Recall that $a \in \mathfrak{P} \iff a \in \mathfrak{p}_\alpha$ for all $\alpha \in A$, so $a, b \notin \mathfrak{P}$ implies that there must be some $\alpha, \beta \in A$ s.t. $a \notin \mathfrak{p}_\alpha, b \notin \mathfrak{p}_\beta$. Say w.l.o.g. that $\beta \geqslant \alpha$, so because the $\mathfrak{p}_\alpha$ are nested $\mathfrak{p}_\beta \leqslant \mathfrak{p}_\alpha$ (!), we have that $a \notin \mathfrak{p}_\alpha \supseteq \mathfrak{p}_\beta$, and so $a, b \notin \mathfrak{p}_\beta$. But $ab \in \mathfrak{P} \subseteq \mathfrak{p}_\beta$, so we get a contradiction to the primality of $\mathfrak{p}_\beta$. We now have an "upper bound" to the chain $(\mathfrak{p}_\alpha)_{\alpha \in A} \geqslant \bigcap_{\alpha \in A} \mathfrak{p}_\alpha$, and as the chain was arbitrary, Zorn's lemma applies and gives the existence of a "maximal element" of $\mathcal{S}$, which by the choice of order on $\mathcal{S}$ is exactly our desired minimal prime ideal.

Problem 3

Define the *spectrum* $\operatorname{Spec}(R)$ of a c1-ring R to be the set of all prime ideals of R (i.e. the set denoted "$\mathcal{S}$" in Problem 2 above). We are asked to determine the spectrum of the subring $R \subseteq \mathbb{Q}$ defined as $R := \{\frac{a}{b} \in \mathbb{Q} : a \in \mathbb{Z}, b \in 1 + 2\mathbb{Z}\}$. Look now at Problem 8, where I provide a brief rundown (and a very good reference — Sharifi's commutative algebra notes) of the basic major properties of localization. This subring R is in fact just the localization $S^{-1}\mathbb{Z}$ for the multiplicatively closed set $S := 1 + 2\mathbb{Z}$! By the results I referenced in Problem 8 below, the prime ideals of $S^{-1}\mathbb{Z}$ are exactly those of form $S^{-1}\mathfrak{p}$ for a prime ideal $\mathfrak{p} \trianglelefteq \mathbb{Z}$ disjoint from S. Well, the prime ideals of $\mathbb{Z}$ are precisely $\{0\}, p\mathbb{Z}$ for p a prime number, and the only such ideals disjoint from $S = 1 + 2\mathbb{Z}$ are $\{0\}, 2\mathbb{Z}$, meaning that $\{0\}$ and $S^{-1}(2\mathbb{Z}) := \{\frac{a}{b} : a \in 2\mathbb{Z}, b \in 1 + 2\mathbb{Z}\}$ are the only prime ideals of $S^{-1}\mathbb{Z} = \mathbb{Z}_{2\mathbb{Z}} = R$.

Problem 4

We are asked to construct a bijection between $\mathrm{Spec}(R \times S)$ and the disjoint union of $\mathrm{Spec}\, R, \mathrm{Spec}\, S$ (for c1-rings R, S). Let us first consider a prime ideal $\mathfrak{P} \trianglelefteq R \times S$. Then $R \times S/\mathfrak{P}$ is an integral domain. Again denoting cosets with the overline notation, we have that $(1,0) \cdot (0,1) = (0,0)$ in $R \times S \implies \overline{(1,0)} \cdot \overline{(0,1)} = \overline{(0,0)}$ in $R \times S/\mathfrak{P}$. In other words, we have two elements multiplying to 0 in an integral domain, meaning one of them must be 0. Well, $\overline{(1,0)} = \overline{(0,0)} \iff (1,0) \in \mathfrak{P} \iff \mathfrak{P} = R \times \mathfrak{p}$ for a prime ideal $\mathfrak{p} \triangleleft S$, and similarly $\overline{(0,1)} = \overline{(0,0)} \iff \mathfrak{P} = \mathfrak{p} \times S$ for a prime ideal $\mathfrak{p} \triangleleft R$. It is trivial that any prime ideal $\mathfrak{p} \triangleleft R, S$ resp. yield prime ideals $\mathfrak{p} \times S, R \times \mathfrak{p}$ in $R \times S$, and so indeed we have shown a one-to-one correspondence between $\mathrm{Spec}(R \times S)$ and the disjoint union of $\mathrm{Spec}(R), \mathrm{Spec}(S)$.

Problem 5

We are asked to construct a bijection between $\mathrm{Spec}(R/I)$ and the set of all prime ideals of R containing I (for R a c1-ring, and $I \trianglelefteq R$ and ideal). Recall from Problem 3 of last week, where I proved that the map sending $S \mapsto S/I$ is a bijection between the set of subrings and ideals of S and of S/I containing I, and I moreover claimed that it remains such a bijection restricting to prime and maximal ideals. All we have to do now is to show that if P is a prime ideal of R, then P/I is a prime ideal of S/I, and if P/I is a prime ideal of S/I, then P must have been a prime ideal of R.

Assuming P is prime, consider $(ab+I) = (a+I)(b+I) \in P/I$. Then because $P/I := \{p+I : p \in P\} \triangleleft R/I$, $ab \in P$, so by primality of P, one the the two elements, w.l.o.g. a is in P. Then $a+I \in P/I$. Conversely, assume P/I is prime and suppose $ab \in P$. Then $ab + I = (a+I)(b+I) \in P/I$, so w.l.o.g. $a + I \in P/I$, meaning $a \in P$. This concludes the proof.

Problem 6

Fermat Christmas theorem: let p be a prime integer $\equiv 1 \pmod 4$. We want to prove that $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. The problem provides the hint to look at $\mathbb{Z}[i]$. Right off the bat, notice that $a^2 + b^2 = (a + bi)(a - bi)$, so the problem is essentially asking us to prove that primes $p \in \mathbb{Z}$ of the form $4k + 1$ are not prime in $\mathbb{Z}[i]$. Suppose f.s.o.c. that p was prime in $\mathbb{Z}[i]$. Then $\mathbb{Z}[i]/(p)$ would be an integral domain. Recall from class 1/3/22, we showed that $\mathbb{Z}[i]$ is a Euclidean domain (with $\varphi(a + bi) := a^2 + b^2$), and hence it is a PID hence UFD, and from class 1/5/22, prime $\equiv$ irreducible in a UFD and irreducible $\equiv$ maximal in a PID. So in fact assuming p prime in $\mathbb{Z}[i] \rightsquigarrow (p)$ a maximal ideal $\iff F := \mathbb{Z}[i]/(p)$ is actually a field (neat, but we will only use that F is a domain).

Observe that $(p) = \{p(a + bi) : a + bi \in \mathbb{Z}[i]\} = (p\mathbb{Z})[i]$, so $F := \mathbb{Z}[i]/(p) = \{a + bi + (p) : a, b \in \{0, \ldots, p-1\}\}$. The subring $\{a + (p) : a \in \{0, \ldots, p-1\}\}$ is actually a subfield $\simeq \mathbb{Z}/p\mathbb{Z}$ (the standard inverse in $\mathbb{Z}/p\mathbb{Z}$ still works when interpreted in F). We will prove soon in class that all finite subgroups of the group of units in a field are cyclic, so in particular the group of units U (which has $p - 1 = 4k$ elements) is $\simeq \mathbb{Z}/4k\mathbb{Z}$. From 210A Homework 1 Problem 2(b), we know that G cyclic $\implies \forall d \mid |G|$ there is exactly one subgroup of G of order d (it will moreover be cyclic). Thus there is a cyclic subgroup of element, hence element of order 4.

In other words we have some element $\alpha \in U$ (so $\alpha = a + (p)$ for some $a \in \{1, \dots, p-1\}$) s.t. $\alpha^4 = 1 \iff \alpha^4 - 1 = 0 \iff (\alpha^2+1)(\alpha^2-1) = 0$. Because α is not order 2, $\alpha^2 - 1 \neq 0$, so then because F is in particular an integral domain, we must have $\alpha^2 + 1 = 0$. Since we are in $\mathbb{Z}[i]$, we can factor further into $(\alpha + i)(\alpha - i) = 0$. But $\alpha = a + (p)$ for some $a \in \{1, \dots, p-1\}$, so neither of $\alpha \pm i$ could possibly equal 0, contradicting that F is an integral domain.

Thus, our initial assumption that p was prime in $\mathbb{Z}[i]$ was incorrect, and indeed we get a factorization $p = (a + bi)(c + di)$, neither of the factors being units in $\mathbb{Z}[i]$. In $\mathbb{C}$, $(a + bi)(c + di) \in \mathbb{R}$, then $a = \lambda c, b = -\lambda d$ for some $\lambda \in \mathbb{R}$. The proof of this rests upon the fact that $(ac - bd) + (ad + bc)i \in \mathbb{R} \implies ad = -bc \implies \frac{a}{c} = -\frac{b}{d} =: \lambda \in \mathbb{R}$. We can replicate this proof in F — the main step was dividing in $\mathbb{R}$, and we can also divide in the field $\mathbb{Z}/(p)$. Thus we get $p = \lambda(a^2 + b^2)$, an at last since p is prime in $\mathbb{Z}$ we must have either $\lambda = 1$, or $a^2 + b^2 = 1 \implies a + bi$ is a unit in $\mathbb{Z}[i]$.

Ending remarks: the most delightful proof of this fact must be Mathologer's video on the topic, detailing a visual proof (using windmill shapes) that the equation $p = x^2 + 4yz$ must have an odd number of solutions ($x, y, z \in \mathbb{N}$) given a prime $p \equiv 1 \pmod 4$, and because y, z can always swap to give another solution unless they are the same, there must be some solution $y = z$, yielding p as a sum of two squares.

Problem 7

We want to show that if a prime p can be written as a sum of two squares, it must be unique. Suppose f.s.o.c. that $p = a^2 + b^2 = c^2 + d^2$, $a, b, c, d \geqslant 1$. Because $\mathbb{Z}[i]$ is a UFD (see refresher in Problem 6 above), primes $\equiv$ irreducibles, and it must be that w.l.o.g. $(a + bi)$ is not irreducible. Then $a + bi = (w + xi)(y + zi)$ where neither $(w + xi)(y + zi)$ are units in $\mathbb{Z}[i]$, and since conjugacy is multiplicative, $a - bi = (w - xi)(y - zi) \implies p = a^2 + b^2 = (a + bi)(a - bi) = (w^2 + x^2)(y^2 + z^2)$, which is the product of two integers. It can't be that $w^2 + x^2 = 1$, because then $w + xi$ would be a unit in $\mathbb{Z}[i]$ (either $\pm 1, \pm i$), so indeed our assumption has lead to the conclusion that p is reducible $\iff$ not prime; contradiction. (where that equivalence is true in PIDs).

Problem 8

Merks defines the *localization* of a c1-ring R at a multiplicative subset $S \subseteq R \setminus 0$ (i.e. S contains 1 and is closed under multiplication) to be $R \times S$ modulo the relation $(r_1, s_1) \sim (r_2, s_2) \iff \exists s \in S$ s.t. $s(r_1 s_2 - r_2 s_1) = 0$. Wiki discusses briefly why S is typically taken to be multiplicatively closed (you can not have that axiom, but the end result of cooking up these fractions is the same if you had just had taken the multiplicative closure). I personally don't like this definition the most; Borcherds has a video in which he defines $S^{-1}R$ first in the case that S has no zero divisors, in which case the $r_1 s_2 = r_2 s_1$ definition works out, and in the case that S has zero divisors, quotient R by $I : \{r \in R : \exists s \in S \text{ s.t. } rs = 0\}$ (i.e. really emphasize that because we can invert elements of S in R, $rs = 0 \implies r = rss^{-1} = 0$, or in other words the possibility that $rs = 0$ for $r \neq 0$ is incompatible with the goal of inverting S).

Anyways, the proof that $\sim$ defined above is an equivalence relation is Lemma 11.1.2 in Sharifi's notes on commutative algebra, and the proof that $S^{-1}R$ is a ring under the standard definitions of fraction addition and multiplication is Theorem 11.1.7 — Sharifi's write-up of these extremely straightforward symbol pushing exercises is as neat, clear, and concise as it's ever going to get, so I'll just leave these to him. Finally although he also proves that $\Phi_S : R \to S^{-1}R$ given by $a \mapsto \frac{a}{1}$ is a ring homomorphism (and more) in Theorem 11.1.10, I'll just do it here as well since it is so short: $\Phi_S(a)\Phi_S(b) = \frac{a}{1} \cdot \frac{b}{1} := \frac{a \cdot b}{1 \cdot 1} = \frac{ab}{1} = \Phi_S(ab)$.

The much more exciting news is the correspondence between the ideals of R and the ideals of $S^{-1}R$. For a ring homomorphism $f : R \to Q$ (R, Q both c1-rings), the *extension* of any ideal $I \trianglelefteq R$ is the ideal $f(I)Q \trianglelefteq Q$, and the *contraction* of an ideal $J \trianglelefteq Q$ is the ideal $f^{-1}(J) \trianglelefteq R$. In the case of $\Phi_S : R \to S^{-1}R$, Prop. 11.1.18 in Sharifi's notes tells us that every ideal of $S^{-1}R$ is the extension $\phi_S(I) = S^{-1}I := \{\frac{r}{s} : r \in I, s \in S\}$ of a (not-necessarily unique) ideal $I \trianglelefteq R$, and moreover, Prop. 11.1.19 says that extension $I \mapsto S^{-1}I$ and contraction $J \mapsto \phi_S^{-1}(J)$ are inverses to each other as maps between the set of {prime $\mathfrak{p} \trianglelefteq R$ disjoint from S}, and the set of {prime ideals of $S^{-1}R$}. In particular, $\Phi_S^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}$, and these two sets are bijective via the bijections extension/contraction.

Problem 9

Again let S be some multiplicative subset of a c1-ring R, and let $\Phi : R \to S^{-1}R$ be again the canonical homomorphism $r \mapsto \frac{r}{1}$. Let $g : R \to T$ be a homomorphism of commutative rings s.t. $g(S) \subseteq T^\times$. We want to show that there is a unique homomorphism $h : S^{-1}R \to T$ s.t. $g = h \circ \Phi$. Suppose such h existed. Then, $h(\frac{r}{1}) = g(r)$. Then, by homomorphism properties, we would have to have $g(r) = h(\frac{r}{s} \cdot \frac{s}{1}) = h(\frac{r}{s})h(\frac{s}{1}) = h(\frac{r}{s})g(s) \implies h(\frac{r}{s}) = \frac{g(r)}{g(s)}$ (can divide because $g(S) \subseteq T^\times$). This shows if h exists, then it is unique/we have determined it's values for all $\frac{r}{s} \in S^{-1}R$, i.e. all elements of $S^{-1}R$.

Lastly, we show the function defined by $h(\frac{r}{s}) := \frac{g(r)}{g(s)}$ is well-defined and a homomorphism.

- Well-defined: if $\frac{r_1}{s_1} = \frac{r_2}{s_2} \implies \exists t \in S$ s.t. $t(s_2r_1 - r_2s_1) = 0$, then $g(t)(g(s_2)g(r_1) - g(r_2)g(s_1)) = 0$, and dividing by $g(t), g(s_1), g(s_2)$ (again using $g(S) \subseteq T^\times$) yields $h(\frac{r_1}{s_1}) = \frac{g(r_1)}{g(s_1)} = \frac{g(r_2)}{g(s_2)} = h(\frac{r_2}{s_2})$.
- Homomorphism: $h(\frac{1}{1}) = \frac{g(1)}{g(1)} = 1$, and addition and multiplication of fractions behave/are defined in the same way in $S^{-1}R$ and T, so indeed h commutes with addition and multiplication.

Problem 10

Recall from class 1/7/22, 1/10/22 that R is a UFD $\iff$ $R[x]$ is a UFD. By definition $R[x, y] := (R[x])[y]$, so the result extends to any finite collection of variables $R[x_1, \ldots, x_n]$. We show now that the result remains true for $R[X]$, where X is any set of variables — recall that $R[X]$ is the set of finite sums of monomials, where a monomial is a scalar ($\in R$) multiple of a finite product of variables taken from the set X, i.e. $R[X] := \bigcup_{F \subseteq X, |F| < \infty} R[F]$ (union taken over all finite subsets F of X). Observe then that any $f \in R[X]$ must be in some $R[F]$, and because $R[F]$ is a UFD (as F is a finite collection of variables), we at least know that f factors into a product $p_1^{k_1} \cdots p_s^{k_s}$ where each p_i is irreducible $\equiv$ prime in $R[F]$. I claim now that **irreducible elements p of $R[F]$ are irreducible in $R[X]$**.

Suppose we have some irreducible $p \in R[F]$ for some finite subset $F \subseteq X$, and suppose we have a factorization $p = fg$ for $fg \in R[X]$. By the construction of $R[X]$, we know that there is some finite subset $\tilde{F} \subseteq X$ s.t. $f, g \in R[\tilde{F}] \subseteq R[F \cup \tilde{F}] = (R[F])[\tilde{F} \setminus F] =: B$. Let us write the ring $R[F]$ as A, and the finite set of variables $\tilde{F} \setminus F := \{x_1, \ldots, x_n\}$, so $f, g \in A[x_1, \ldots, x_n] =: B$. I claim that ${}^{B}/_{pB} \simeq (A/pA)[x_1, \ldots, x_n]$. We prove this with the first isomorphism theorem: let $\pi : B \twoheadrightarrow (A/pA)[x_1, \ldots, x_n]$ be the projection homomorphism mapping monomials with coefficients $a \in A$ to monomials with coefficients $\overline{a} := a + pA \in A/pA$; then the kernel (a polynomial is 0 iff the coefficients of all its monomials are 0) consists exactly of polynomials with monomials with coefficients in pA, i.e. the kernel is exactly $p \cdot A[x_1, \ldots, x_n] = pB$.

Then as p is irreducible $\equiv$ prime in the UFD $R[F] =: A$, the quotient ring (A/pA) is an integral domain, so ${}^{B}/_{pB} \simeq (A/pA)[x_1, \ldots, x_n]$ is an integral domain, so p is prime in B. As B is itself a UFD, and prime $\equiv$ irreducible in UFDs (see 1/5/22), p is irreducible in B. By definition of irreducible, we have w.l.o.g. that f is a unit in B. We know (from 1/8/22) that the units of $R[x]$ are exactly those of R, and by induction the units of $R[\tilde{F} \cup F] =: B$ are exactly those of R. The units of R are certainly also units of $R[X]$, so f is unit of $R[X]$, and as $p = fg$ was an arbitrary factorization of p in $R[X]$, we have shown that indeed p is irreducible in $R[X]$.

With this, we have that the irreducible $\equiv$ prime factorization (I'll henceforth just call them "prime factorizations") of f in $R[F]$ is a prime factorization of f in $R[X]$. It only remains to show that such a factorization in $R[X]$ is unique. A prime factorization by definition consists of finitely many irreducible factors, so given two prime factorizations of f in $R[X]$, we can be sure that is some $R[F]$ contains all of both factorizations' irreducible factors (again F is finite subset of X). Because $R[F]$ is a UFD, these two prime factorizations are equal up to units in $R[F]$, and as noted in the previous paragraphs, the units of $R[F]$ are exactly the units of R, which are definitely units of $R[X]$, so indeed the two prime factorizations are equal up to units in $R[X]$, and we are done.

Meta-mathematical Lessons

In Problem 1, Problem 4, Problem 6, and Problem 10! of this week's homework, which all involved prime ideals, one key step was to quotient by the prime ideal to get an integral domain, and work in there! Amazingly, for each problem, I struggled to think of this step, but now the pattern has been noticed, and it seems like a good first step in any problem involving prime ideals.

210B Homework 1

Daniel Rui - 1/13/21

Problem 1

We want to show that finite integral domains are fields. Suppose R is a finite integral domain with non-zero elements $x_1, \ldots, x_n$. Then the product $x_1 \cdots x_n$ is also in R, say equal to x_a. If $x_a = 1_R$, then indeed for every x_i, by commutativity we see that $\prod_{j \neq i} x_j$ is the inverse of x_i.

Otherwise we may use the cancellation property of integral domains to cancel x_a from both sides, and then get that for all $i \neq a$ in $[n]$, x_i has inverse $\prod_{j \neq i,a} x_j$. Then $x_a^2 \neq x_a$ nor 0 because R is an integral domain and we're assuming $x_a \neq 1, 0$, so $x_a^2 = x_i$ for some $i \neq a$ in $[n]$. This means it has inverse x_i^{-1}, i.e. $x_a(x_a x_i^{-1}) = x_a^2 x_i^{-1} = 1$ so indeed we have found that $x_a(x_a^2)^{-1}$ is the inverse to x_a.

Problem 2

We want to prove that a non-zero matrix $A \in M_n(R)$ (for an integral domain R) is a zero divisor if and only if $\det(A) = 0$. The strategy we use here is to first do the problem in the case that R is a field (allowing us to use the full power of linear algebra!), and then "pullback" the results to the integral domain R (using that integral domains admit fraction fields).

($\implies$): suppose we have a zero divisor $A \in M_n(F)$ and F is a field, where we furthermore suppose f.s.o.c. that $\det(A) \neq 0 \iff A$ is invertible in $M_n(F)$. Then given $AB = 0$, we can multiply on the left by $A^{-1} \in M_n(F)$ to get $B = 0$, contradicting the fact that A is a zero divisor.

Going back to the case with an integral domain R, we can construct the fraction field $F = \mathrm{Frac}(R)$, and since the determinants are calculated in the same way, $\det(A)$ in R is the same as $\det(A)$ in F, and so there is an inverse $A^{-1} \in M_n(F)$. Then given arbitrary $B \in M_n(R)$ s.t. $AB = 0$, we can interpret everything in $M_n(F)$, and then do the above stuff in the field case, and then get that $B = 0$ in $M_n(F)$, which is of course the same as being 0 in $M_n(R)$.

($\impliedby$): we start with $\det(A) = 0$ in $M_n(R)$. Again determinants are calculated the same in $M_n(R)$ and $M_n(F)$, so $\det(A) = 0$ in $M_n(F)$ as well. Then that means the null space is non-trivial, so there is a non-zero vector $v \in F^n$. Pasting n copies of this vector to form the matrix $B \in M_n(F)$, we do indeed get a non-zero B s.t. $AB = 0$ in F. Going back to R, we can multiply B by the product of the denominators in v, denoted $\lambda \in R$ s.t that $\lambda B \in M_n(R)$. Then in $M_n(F)$, $A(\lambda B) = \lambda AB = 0$, and as multiplication calculations are the same in $M_n(R)$ and $M_n(F)$, indeed $A(\lambda B) = 0$ in $M_n(R)$ ($\lambda B \neq 0$ because R is an integral domain implies $\lambda v \neq 0$).

Problem 3

Compare Problem 8 of 210A Homework 2 — there also may be a nicer way using "universal algebra". In the problem, we are given a surjective ring homomorphism $f : R \to S$, but the 1st isomorphism theorem gives that $S \simeq {}^{R}/_{\ker f}$, so we can rephrase the whole problem as being given an ideal $I \trianglelefteq R$, and considering the projection map $\pi : R \to {}^{R}/_{I}$. Following notated with notation of left ideals, but the same exact arguments work with minor notation changes for right ideals and hence two-sided ideals too. We prove that π extended to subrings (defined by $S \mapsto {}^{S}/_{I}$) establishes

(a) a bijection between subrings of R containing I and subrings of ${}^{R}/_{I}$.

- Well-defined: we check that for a subring $S \leqslant R$ containing I, ${}^{S}/_{I}$ is actually a subring of ${}^{R}/_{I}$. Given $s_1 + I, s_2 + I \in {}^{S}/_{I}$, the difference $(s_1 + I) - (s_2 + I) = (s_1 - s_2) + I$ and product $(s_1 + I)(s_2 + I) = (s_1 s_2) + I$ are still in ${}^{S}/_{I}$ because $s_1 - s_2, s_1 s_2 \in S$.
- Inverse: we construct an explicit inverse using the canonical projection $\pi : R \to {}^{R}/_{I}\,(r \mapsto r+I)$, namely we show that π^{-1} is the desired inverse. First, we want to show for a subring $S \leqslant R$ containing I, $\pi^{-1}({}^{S}/_{I}) := \{r \in R : r + I \in {}^{S}/_{I}\} = S$. The $(\supseteq)$ containment is true because $s \in S \implies s + I \in {}^{S}/_{I}$; and the $(\subseteq)$ containment is true because ${}^{S}/_{I} = \{s + I : s \in S\}$ implying that $r + I \in {}^{S}/_{I} \implies r + I = s + I$ for some $s \in S$, i.e. $r = s + i \in S$ since i is some element of $I \subseteq S$.

  Second, we show that for a subring S of ${}^{R}/_{I}$, $\pi^{-1}(S)$ is a subring of R containing I, and $\pi(\pi^{-1}(S)) = S$. We know that inverse images via homomorphisms are subrings, and since S in particular contains $1_{R/I}$, the inverse image $\pi^{-1}(S) \supseteq \pi^{-1}(\{1_{R/I}\}) = \ker(\pi) = I$. Next suppose that $r \in \pi^{-1}(S) \implies \pi(r) = r + I \in S$. This tells us that $\pi(\pi^{-1}(S)) \subseteq S$. Now suppose $r + I \in S$ (i.e. is an arbitrary element of $S \leqslant {}^{R}\big/{}_{I}$ since its elements are all of the form $r + I$ for some $r \in R$). Well, $\pi(r) = r + I \in S \implies r \in \pi^{-1}(S) \implies r + I \in \varphi(\pi^{-1}(S))$, and so $S \subseteq \varphi(\pi^{-1}(S))$, completing the proof.

(b) a bijection between ideals of R containing I and ideals of ${}^{R}/_{I}$.

- Well-defined: we check that for an ideal $S \leqslant R$, ${}^{S}/_{I}$ is actually an ideal of ${}^{R}/_{I}$. In part (a) above, we already verified all the "subring" related claims, so we just need to verify ideal-ness. Let $r + I \in {}^{R}/_{I}$ and $s + I \in {}^{S}/_{I}$ be arbitrary. Then $(r + I)(s + I) = (rs) + I \in {}^{S}/_{I}$ because S ideal $\implies rs \in S$.
- Inverse: we construct an explicit inverse using the canonical projection $\pi : R \to {}^{R}/_{I}\,(r \mapsto r+I)$, namely we show that π^{-1} is the desired inverse. In part (a) above, we already verified all the "subring" related claims, so we just need to verify ideal-ness, namely that the inverse image of an ideal is an ideal. Well if $x \in \pi^{-1}(S)$ for an ideal $S \trianglelefteq RI$, then for any $r \in R$, rx will satisfy $\pi(rx) = \pi(r)\pi(x) \in S$ (since $\pi(x) \in S$ and S is an ideal), so indeed $rx \in \pi^{-1}(S)$.

(c) a bijection between prime/maximal ideals of R containing I and prime/maximal ideals of ${}^{R}/_{I}$. Similar proofs as above.

Problem 4

An element $a \in R$ is called nilpotent if $a^n = 0$ for some $n \in \mathbb{N}$. Let $\mathfrak{N}(R)$ (the nilradical) denote the set of all nipotent elements in R.

(a) We claim if R is a c1-ring, $\mathfrak{N}(R)$ is an ideal, and that $R/\mathfrak{N}(R)$ has no non-zero nilpotent elements (i.e. $\mathfrak{N}(R/\mathfrak{N}(R)) = \{0\}$). We check the addition/multiplication axioms: $a_1, a_2 \in \mathfrak{N}(R) \implies (a_1 + a_2)^{n_1+n_2} = 0$ (binomial theorem) and $(a_1 a_2)^{\max\{n_1,n_2\}} = 0$; and the scalar multiplication axiom: $(ra)^n = r^n a^n = 0$.

Now suppose $r + \mathfrak{N}(R) \in R/\mathfrak{N}(R)$ is nilpotent, i.e. $(r + \mathfrak{N}(R))^m := r^m + \mathfrak{N}(R) = \mathfrak{N}(R) \implies (r^m)^n = r^{mn} = 0 \implies r \in \mathfrak{N}(R) \implies r + \mathfrak{N}(R) = \mathfrak{N}(R) = 0_{R/\mathfrak{N}(R)}$, as desired.

Problem 5

(a) We want to prove that if a is a nilpotent element of a ring R, then $(1 + a)$ is invertible. The intuition behind this is the analytic formula $\frac{1}{1+a} = 1 - a + a^2 - a^3 + \ldots$, which becomes a finite sum if a is nilpotent. Indeed if $a^n = 0$, expanding out $(1+a)(1-a+a^2-a^3+\ldots+(-1)^n a^n)$ and $(1-a+a^2-a^3+\ldots+(-1)^n a^n)(1+a)$ yield 1, i.e. we have found a left/right-inverse to $(1+a)$.

Problem 6

Let R be a ring and $r \in R$. We want to prove that there is a unique ring homomorphism $f : \mathbb{Z}[t] \to R$ s.t. $f(t) = r$, and that $\mathrm{im}(f)$ is the smallest subring of R that contains r. The axioms of a ring homomorphism require that $f(1) = 1_R$ (we notate for all $a \in \mathbb{Z}$, $a \in R$ to mean $1_R + \ldots 1_R$ a times), so for an arbitrary polynomial $p = a_n t^n + \ldots + a_0 \in \mathbb{Z}[t]$ the given restrictions and the axioms of a ring homomorphism force $f(p) = a_n r^n + \ldots + a_1 r + a_0$. This tells us that if there exists a ring homomorphism $f : \mathbb{Z}[t] \to R$ s.t. $f(t) = r$, then it is unique, and exactly as we have specified. To establish existence rigorously, we just check the addition and multiplication axioms: this boils down to the calculations being the same regardless of whether the variable is notated "t" or "r".

Finally the image of any ring homomorphism is a subring in the codomain (because $s_1, s_2 \in \mathrm{im}(f) \implies f(r_i) = s_i$ for $i = 1, 2$ implying $s_1 \pm s_2 = f(r_1 \pm r_2) \in \mathrm{im}(f)$ and $s_1 s_2 = f(r_1 r_2) \in \mathrm{im}(f)$), $\mathrm{im}(f)$ is a subring of R containing R. Because subrings are closed under multiplication and addition, for any subring $S \leqslant R$ containing r, all powers r^n ($n \in \mathbb{N}$) are in S, and all sums $ar^n = r^n + \ldots + r^n$ a times ($a \in \mathbb{Z}$) are in S too, meaning that indeed $\mathrm{im}(f) \subseteq R$ for any such subring S. These two sentences together yield that $\mathrm{im}(f)$ is indeed the smallest subring of R containing r.

Problem 7

Let R be an integral domain s.t. $R[t]$ is a PID. We show that R is actually a field. Consider the case of $\mathbb{Z}[t]$, where for example $(2, t)$ is not a principal ideal. This suggests the examination of $(a, t) = \{af + tg : f, g \in R[t]\}$ for all $0 \neq a \in R$. Suppose $(a, t) = (h_a)$ for some polynomial $h_a \in R[t]$. Because in an integral domain $\deg(fg) = \deg(f) + \deg(g)$, the minimal degree of a non-zero element

of (h_a) would be $\deg(h_a)$. Since we claim that $(h_a) = (a, t)$, which contains $a \neq 0$ which has degree 0, it must be that $\deg(h_a)$ is also 0. We change the notation to c_a, for "constant".

Then for any $f \in (c_a)$, all the coefficients of f will be divisible by c_a. But $t \in (a, t) = (c_a)$, so c_a divides 1_R, i.e. $c_a b = 1_R \iff c_a$ is a unit. If we don't want to use the word divisibility, we can just say that $t \in (c_a) \implies t = c_a f$ for some $f \in R[x]$; comparing degrees yields $\deg(f) = 1 \implies f = b_1 t + b_0$, and comparing coefficients yields $1 = c_a b_1, b_0 = 0$ and again c_a must be a unit. Then, $(a, t) = (c_a) = 1$, so somehow $1 = af + tg$ for $f, g \in R[t]$. Again comparing degrees, we see that $g = 0$, and $f \in R$, giving us a is a unit. As $a \neq 0$ was chosen arbitrarily, we have proven that all non-zero elements of R are invertible, so R is a field.

Problem 8

We want to show that for any non-trivial c1-ring R, $R[t]$ has infinitely many prime ideals. We again use the technique of first considering the case of a field $F[t]$. Recall from class 1/3/22 that $F[t]$ is a Euclidean domain (polynomial division requires inverting coefficient of highest degree term, so F being field is quite important), and hence a PID. From class 1/5/22 we know that in a PID, an element a is prime (i.e. (a) is a prime ideal) $\iff$ a is irreducible $\iff$ (a) is maximal ideal. We prove that $F[t]$ has infinitely many primes using Euclid's proof. Supposing f.s.o.c. that there were only finitely many primes $p_1, \ldots, p_n \in F[t]$, we consider $p_1 \cdots p_n + 1$. Because PID $\implies$ UFD and in a UFD prime $\iff$ irreducible (results from class 1/5/22), we can factor $p_1 \cdots p_n + 1$ into irreducibles. But none of them can be the finitely many primes $\equiv$ irreducibles $p_1, \ldots, p_n$, since then 1 would be multiple of some p_i, i.e. p_i would be a unit; contradiction.

Now with only a non-trivial c1-ring R, we know (Zorn's lemma) that there is a maximal ideal $\mathfrak{m}$. Then $R/\mathfrak{m}$ is a field, so $R/\mathfrak{m}[t]$ has infinitely prime $\equiv$ maximal ideals by the above paragraph. But $R/\mathfrak{m}[t] \simeq {}^{R[t]}\!/_{\mathfrak{m}[t]}$ because of the 1st isomorphism theorem applied to the map $R[t] \to R/\mathfrak{m}[t]$ defined by $a_n t^n + \ldots + a_0 \mapsto \overline{a_n} t^n + \ldots + \overline{a_0}$ where $\overline{a} := a + \mathfrak{m} \in R/\mathfrak{m}$ (the kernel of this map is indeed $\mathfrak{m}[t]$). Thus ${}^{R[t]}\!/_{\mathfrak{m}[t]}$ has infinitely prime $\equiv$ maximal ideals. By the correspondence theorem (Problem 3 above) all these prime/maximal ideals are in bijection with prime/maximal ideals in $R[t]$ containing $\mathfrak{m}[t]$, so indeed there are infinitely many prime ideals in $R[t]$ (and I'm pretty sure the prime ideals containing $\mathfrak{m}[t]$ are in particular also maximal, inherited from above prime $\equiv$ maximal in the PID $R/\mathfrak{m}[t]$?)

Problem 9

We define the *Jacobson radical* $J(R)$ of R to be the intersection of all maximal ideals of R, where R is a c1-ring. We want to prove that for each $x \in R, x \in J(R) \iff 1 - yx$ is invertible for EACH $y \in R$.

($\impliedby$): suppose $x \in R$ s.t. for all $y \in R$, $1 - yx$ is invertible. To show $x \in J(R)$, we want to show that $x \in \mathfrak{m}$ for all ideals $\mathfrak{m} \triangleleft R$. Well, suppose that $x \notin \mathfrak{m}$ for some 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 inverse to get that $1 \in \mathfrak{m}$.

($\implies$): if $x \in J(R)$ and there is $y \in R$ s.t. $1 - yx$ is not invertible, then obviously $1 - yx$ is not a unit of R, and hence there is a maximal ideal $\mathfrak{m}$ containing it (cf. Zorn's lemma proof that maximal ideals exist in non-trivial rings). 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.

Problem 10

As discussed in class 12/1/21, the left adjoint functor of the forgetful functor **CRings** $\to$ **Sets** is the functor taking a set $S \mapsto \mathbb{Z}[S]$, and a set map $f : S \to T$ to $\varphi : \mathbb{Z}[S] \to \mathbb{Z}[T]$ defined by $\sum_{i=1}^{N} n_i s_{i,1}^{e_{i,1}} \cdots s_{i,k_i}^{e_{i,k_i}} \mapsto \sum_{i=1}^{N} n_i f(s_{i,1})^{e_{i,1}} \cdots f(s_{i,k_i})^{e_{i,k_i}}$.