Problems

"... den Samen in den Wind streuend; fasse, wer es fassen kann".
—**Hermann Weyl**

Problem 1

1. Suppose G is a finite group and that $\mathrm{Aut}_{\mathrm{Gr}}(G) = \{1\}$. (Here, $\mathrm{Aut}_{\mathrm{Gr}}(G)$ is the group of all bijections, $G \to G$, which are also group homomorphisms.) Find *all* such groups G.

2. Write $\mathbb{Z}/2\mathbb{Z}$ for the cyclic group of order 2. If $G = \mathbb{Z}/2\mathbb{Z} \prod \cdots \prod \mathbb{Z}/2\mathbb{Z}$, t-times, compute $\#\big(\mathrm{Aut}_{\mathrm{Gr}}(G)\big)$. When $t = 2$, determine the group $\mathrm{Aut}_{\mathrm{Gr}}(G)$. When $t = 3$, determine the structure of the odd prime Sylows. Can you decide whether $\mathrm{Aut}_{\mathrm{Gr}}(G)$ has any normal subgroups in the case $t = 3$?

Problem 2

1. (Poincaré). In an infinite group, prove that the intersection of two subgroups of finite index has finite index itself.

2. Show that if a group, G, has a subgroup of finite index, then it possesses a normal subgroup of finite index. Hence, an infinite simple group has no subgroups of finite index.

3. Sharpen (2) by proving: if $(G : H) = r$, then G possesses a normal subgroup, N, with $(G : N) \leq r!$. Conclude immediately that a group of order 36 cannot be simple.

Problem 3 Let $G = \mathrm{GL}(n, \mathbb{C})$ and Δ_n be the subgroup of matrices with entries only along the diagonal. Describe precisely $N_G(\Delta_n)$ in terms of what the matrices look like.

Problem 4 Say G is a group and $\#(G) = p^r g_0$, where p is a prime and $(p, g_0) = 1$. Assume

$$r > \sum_{j=1}^{g_0-1} \sum_{k>0} [j/p^k]$$

$\big([x] = \text{largest integer} \leq x\big)$. Prove that G is not simple. Show that this governs all groups of order < 60, except for $\#(G) = 30, 40, 56$. We know that $\#(G) = 30 \implies G$ not simple. Show by explicit argument that groups of orders $40, 56$ are not simple. (Here, of course, by simple we mean non-abelian and simple.)

Problem 5 In a p-group, G, we cannot have

$$(G\colon Z(G)) = p.$$

Show that for non-abelian groups of order p^3, $Z(G) \cong \mathbb{Z}/p\mathbb{Z}$ and $G/Z(G) \cong \mathbb{Z}/p\mathbb{Z} \prod \mathbb{Z}/p\mathbb{Z}$.

Problem 6 Let G be the group of automorphisms of a regular polyhedron with v vertices, e edges, and f faces. Show that G has order $g = fs = vr = 2e$, where s is the number of sides to a face and r is the number of edges emanating from a vertex. From topology, one knows Euler's formula

$$v - e + f = 2.$$

Find the only possible values for v, e, f, r, s, g. Make a table.

Problem 7 Let p be a prime number. Find all non-abelian groups of order p^3. Get started with the Burnside basis theorem, but be careful to check that the groups on your list are non-isomorphic. Also make sure your list is exhaustive. Your list should be a description of the generators of your groups and the relations they satisfy.

Problem 8 Let G be a finite group and write $c(G)$ for the number of distinct conjugacy classes in G. This number will increase (in general) as $\#(G) \to \infty$; so, look at

$$\overline{c}(G) = \frac{c(G)}{\#(G)}.$$

The number $\overline{c}(G)$ measures the "average number of conjugacy classes per element of G" and is 1 if G is abelian. Assume G is *non-abelian* from now on. Then $0 < \overline{c}(G) < 1$.

1. Prove that for all such G, we have $\overline{c}(G) \le 5/8$.
2. Suppose p is the smallest prime with $p \,|\, \#(G)$. Prove that

$$\overline{c}(G) \le \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^3}.$$

Is the bound of (1) sharp; that is, does there exist a G with $\overline{c}(G) = 5/8$? How about the bound of (2)?

Problem 9 If G is a finite group and H a normal subgroup of G, write P for a p-Sylow subgroup *of H.*

1. Show that the natural injection
$$N_G(P)/N_H(P) \to G/H$$
(why does it exist, why injective?) is actually an isomorphism.
2. Prove that the Frattini subgroup, $\Phi(G)$, of ANY finite group, G, has property N (cf. Section 1.3, Chapter 1).

Problem 10 We've remarked that $\Phi(G)$ is a kind of "radical" in the group-theoretic setting. In this problem we study various types of radicals.
A *normal* subgroup, H, of G is called *small* iff for every $X \lhd G$, the equality $H \cdot X = G$ implies that $X = G$. (Note: $\{1\}$ is small, $\Phi(G)$ is small; so they exist.) Check that if H and L are small, so is HL, and if H is small and $K \lhd G$, then $K \subseteq H \implies K$ is small.

1. The *small radical* of G, denoted $\mathcal{J}^{**}(G)$, is
$$\mathcal{J}^{**}(G) = \bigl\{x \in G \bigm| \mathrm{Gp}\{\mathrm{Cl}(x)\} \text{ is small}\bigr\}.$$
(Here, $\mathrm{Cl}(x)$ is the conjugacy class of x in G, and $\mathrm{Gp}\{S\}$ is the group generated by S.) Prove that $\mathcal{J}^{**}(G)$ is a subgroup of G.
2. The *Jacobson radical* of G, denoted $\mathcal{J}^{*}(G)$, is the intersection of all maximal, normal subgroups of G; while the *Baer radical* of G, denoted $\mathcal{J}(G)$, is the product (inside G) of *all* the small subgroups of G. Prove
$$\mathcal{J}^{**}(G) \subseteq \mathcal{J}(G) \subseteq \mathcal{J}^{*}(G).$$

3. Prove *Baer's Theorem*: $\mathcal{J}^{**}(G) = \mathcal{J}(G) = \mathcal{J}^*(G)$. (Suggestion: if $x \notin \mathcal{J}^{**}(G)$, find $N \lhd G$ $(\neq G)$ so that $\mathrm{Gp}\{\mathrm{Cl}(x)\}N = G$. Now construct an appropriate maximal normal subgroup not containing x.)

Problem 11 Recall that a *characteristic* subgroup is one taken into itself by *all* automorphisms of the group.

1. Prove that a group possessing no proper characteristic subgroups is isomorphic to a product of isomorphic simple groups. (Hints: Choose $\widetilde{G}$ of smallest possible order (> 1) normal in G. Consider all subgroups, H, for which $H \cong G_1 \prod \cdots \prod G_t$, where each $G_j \lhd G$ and each $G_j \cong \widetilde{G}$. Pick t so that $\#(H)$ is maximal. Prove that H is characteristic. Show $K \lhd G_1$ (say) $\Longrightarrow$ $K \lhd G$.)

2. Prove: In every finite group, G, a minimal normal subgroup, H, is either an elementary abelian p-group or is isomorphic to a product of mutually isomorphic, non-abelian, simple groups.

3. Show that in a solvable group, G, only the first case in (2) occurs.

Problem 12 Let G be a finite p-group and suppose $\varphi \in \mathrm{Aut}(G)$ has order n (i.e., $\varphi\big(\varphi(\cdots(\varphi(x))\cdots)\big) = \mathrm{Id}$, all $x \in G$: we do φ n-times in succession and n is minimal). Suppose $(n, p) = 1$. Now φ induces an automorphism of $G/\Phi(G)$, call it $\overline{\varphi}$, as $\Phi(G)$ is characteristic. Remember that $G/\Phi(G)$ is a vector space over $\mathbb{F}_p$; so, $\overline{\varphi} \in \mathrm{GL}\big(G/\Phi(G)\big)$.

1. Prove $\overline{\varphi} = $ identity $\Longleftrightarrow$ $\varphi = $ identity.

2. Show that if d is the Burnside dimension of G, then
$$\#\big(\mathrm{GL}(G/\Phi(G))\big) = p^{\frac{d(d-1)}{2}} \prod_{k=1}^{d} (p^k - 1),$$
and that if P is a p-Sylow subgroup of $\mathrm{GL}\big(G/\Phi(G)\big)$, then $P \subseteq \mathrm{SL}\big(G/\Phi(G)\big)$; i.e., $\sigma \in P \Longrightarrow \det(\sigma) = 1$.

3. Let $\mathcal{P} = \{\varphi \in \mathrm{Aut}(G) \mid \overline{\varphi} \in P,$ no restriction on the order of $\varphi\}$. Show that $\mathcal{P}$ is a p-subgroup of $\mathrm{Aut}(G)$.

4. Call an element $\sigma \in \mathrm{GL}\big(G/\Phi(G)\big)$ *liftable* iff it is $\overline{\varphi}$ for some $\varphi \in \mathrm{Aut}(G)$. Examine all G of order p, p^2, p^3 to help answer the following: Is every σ liftable? If not, how can you tell (given σ) if σ is liftable?

Problem 13 Let p be a prime number and consider a set, S, of p objects: $S = \{\alpha_1, \ldots, \alpha_p\}$. Assume G is a *transitive* group of permutations of S (i.e., the elements of S form an orbit under G); further assume $(\alpha_1\alpha_2) \in G$ (here $(\alpha_1\alpha_2)$ is the transposition). Prove: $G = \mathfrak{S}_p$. (Suggestion: let $M = \{\alpha_j | (\alpha_1\alpha_j) \in G\}$, show if $\sigma \in \mathfrak{S}_p$ and $\sigma = 1$ outside M then $\sigma \in G$. Now prove $\#(M) | p$.)

Problem 14 A *Fermat prime*, p, is a prime number of the form $2^\alpha + 1$. E.g., $2, 3, 5, 17, 257, \ldots$.

1. Show if $2^\alpha + 1$ is prime then $\alpha = 2^\beta$.

2. Say p is a Fermat prime (they are quite big) and g_0 is an *odd* number with $g_0 < p$. Prove that any group of order $g_0 p$ is isomorphic to a product $G_0 \prod(\mathbb{Z}/p\mathbb{Z})$, where $\#(G_0) = g_0$. Hence, for example, the groups of orders $51 (= 3 \cdot 17)$, $85 (= 5 \cdot 17)$, $119 (= 7 \cdot 17)$, $153 (= 9 \cdot 17)$, $187 (= 11 \cdot 17)$, $221 (= 13 \cdot 17)$, $255 (= 3 \cdot 5 \cdot 17)$ are all abelian. Most we knew already, but $153 = 3^2 \cdot 17$ and $255 = 3 \cdot 5 \cdot 17$ are new.

3. Generalize to any prime, p, and $g_0 < p$, with $p \not\equiv 1 \bmod g_0$. For example, find all groups of order 130.

Problem 15 Recall that a group, G, is *finitely generated* (f.g.) iff $(\exists\, \sigma_1, \ldots, \sigma_n \in G)(G = \mathrm{Gp}\{\sigma_1, \ldots, \sigma_n\})$.

1. If G is an *abelian* f.g. group, prove each of its subgroups is f.g.

2. In an arbitrary group, G, an element $\sigma \in G$ is called *n-torsion* ($n \in \mathbb{N}$) $\Longleftrightarrow$ $\sigma^n = 1$; σ is torsion iff it is n-torsion for some $n \in \mathbb{N}$. The element $\sigma \in G$ is *torsion free* $\Longleftrightarrow$ it is not torsion. Show that in an abelian group, the set
$$t(G) = \{\sigma \in G \mid \sigma \text{ is torsion}\}$$
is a subgroup and that $G/t(G)$ is torsion free (i.e., all its non-identity elements are torsion free).

3. In the solvable group $0 \to \mathbb{Z} \to G \to \mathbb{Z}/2\mathbb{Z} \to 0$ (split extension, non-trivial action) find two elements x, y satisfying: $x^2 = y^2 = 1$ and xy is torsion free. Can you construct a group, $\widetilde{G}$, possessing elements x, y of order 2, so that xy has order n, where n is predetermined in $\mathbb{N}$? Can you construct $\widetilde{G}$ solvable with these properties?

4. Back to the abelian case. If G is abelian and finitely generated show that $t(G)$ is a finite group.

5. Say G is abelian, f.g., and torsion-free. Write d for the minimal number of generators of G. Prove that G is isomorphic to a product of d copies of $\mathbb{Z}$.

6. If G is abelian and f.g., prove that
$$G \cong t(G) \prod \big(G/t(G)\big).$$

Problem 16 Let (P) be a property of groups. We say a group, G, is *locally (P)* $\Longleftrightarrow$ each f.g. subgroup of G has (P). Usually, one says a locally cyclic group is a *rank one group*.

1. Prove that a rank one group is abelian.

2. Show that the additive group of rational numbers, $\mathbb{Q}^+$, is a rank one group.

3. Show that every torsion-free, rank one group is isomorphic to a subgroup of $\mathbb{Q}^+$.

Problem 17 Fix a group, G, and consider the set, $\mathcal{M}_n(G)$, of $n \times n$ matrices with entries from G or so that $\alpha_{ij} = 0$ (i.e., entries are 0 or from G). Assume for each row and each column there is one and only one non-zero entry. These matrices form a group under ordinary "matrix multiplication" if we define $0 \cdot \text{group element} = \text{group element} \cdot 0 = 0$. Establish an isomorphism of this group with the wreath product $G^n \wr \mathfrak{S}_n$. As an application, for the subgroup of $\mathrm{GL}(n,\mathbb{C})$ consisting of diagonal matrices, call it Δ_n, show that
$$N_G(\Delta_n) \cong \mathbb{C}^n \wr \mathfrak{S}_n, \quad \text{here } G = \mathrm{GL}(n,\mathbb{C}).$$

Problem 18

1. Say G is a simple group of order n and say p is a prime number dividing n. If $\sigma_1, \dots, \sigma_t$ is a listing of the elements of G of exact order p, prove that $G = \mathrm{Gp}\{\sigma_1, \dots, \sigma_t\}$.

2. Suppose G is any finite group of order n and that d is a positive integer relatively prime to n. Show that every element of G is a dth power.

Problem 19 We know that when G is a (finite) cyclic group, and A is any G-module, we have an isomorphism
$$A^G/\mathcal{N}(A) \xrightarrow{\sim} H^2(G,A).$$
This problem is designed to lead to a proof. There are other proofs which you might dig out of books (after some effort), but do *this* proof.

1. Suppose G is any group and A, B, C are G-modules. Suppose further, we are given a *G-pairing of* $A\prod B \to C$ i.e., a map
$$\theta : A\prod B \to C$$
which is bi-additive and "G-linear":
$$\sigma\theta(a,b) = \theta(\sigma a, \sigma b).$$
If f, g are r-, s-cochains of G with values in A, B (respectively), we can define an $(r+s)$-cochain of G with values in C *via* the formula:
$$(f \smile_\theta g)(\sigma_1, \ldots, \sigma_r, \sigma_{r+1}, \ldots, \sigma_{r+s}) = \theta\big(f(\sigma_1,\ldots,\sigma_r), \sigma_1\ldots\sigma_r g(\sigma_{r+1},\ldots,\sigma_{r+s})\big).$$
Prove that $\delta(f \smile_\theta g) = \delta f \smile_\theta g + (-1)^r f \smile_\theta \delta g$. Show how you conclude from this that we have a pairing of abelian groups
$$\smile_\theta\colon H^r(G,A)\prod H^s(G,B) \to H^{r+s}(G,C).$$
(Notation and nomenclature: $\alpha \smile_\theta \beta$, *cup-product.*)

2. Again G is any group, this time finite. Let $\mathbb{Z}$ and $\mathbb{Q}/\mathbb{Z}$ be G-modules with trivial action. Consider the abelian group $\mathrm{Hom}_{\mathrm{gr}}(G, \mathbb{Q}/\mathbb{Z}) = \widetilde{G}$, where addition in $\widetilde{G}$ is by pointwise operation on functions. If $\chi \in \widetilde{G}$, then $\chi(\sigma) \in \mathbb{Q}/\mathbb{Z}$, all $\sigma \in G$. Show that the function
$$f_\chi(\sigma,\tau) = \delta\chi(\sigma,\tau) = \sigma\chi(\tau) - \chi(\sigma\tau) + \chi(\sigma)$$
has values in $\mathbb{Z}$ and actually is a 2-cocycle with values in $\mathbb{Z}$. (This is an example of the principle: If it looks like a coboundary, it is certainly a cocycle.) The map
$$\chi \in \widetilde{G} \mapsto \text{cohomology class of } f_\chi(\sigma,\tau) \tag{$\dagger$}$$
gives a homomorphism $\widetilde{G} \to H^2(G,\mathbb{Z})$.
Now *any* 2-cocycle $g(\sigma,\tau)$ with values in $\mathbb{Z}$ can be regarded as a 2-cocycle with values in $\mathbb{Q}$ (corresponding to the injection $\mathbb{Z} \hookrightarrow \mathbb{Q}$). Show that *as a 2-cocycle in* $\mathbb{Q}$ it is a coboundary (of some $h(\sigma)$, *values in* $\mathbb{Q}$). So, $g(\sigma,\tau) = \delta h(\sigma,\tau)$, some h. Use this construction to prove:

   For any finite group, G, the map ($\dagger$) above gives an *isomorphism* of $\widetilde{G}$ with $H^2(G,\mathbb{Z})$.

3. Now let G be finite, A be any G-module, and $\mathbb{Z}$ have the trivial G-action. We have an obvious G-pairing $\mathbb{Z}\prod A \to A$, namely $(n,a) \mapsto na$, hence by (1) and (2) we obtain a pairing
$$\widetilde{G}(= H^2(G,\mathbb{Z}))\prod A^G \to H^2(G,A).$$
Show that if $\xi = \mathcal{N}\alpha$, for $\alpha \in A$, then (χ,ξ) goes to 0 in $H^2(G,A)$; hence, we obtain a pairing:
$$\widetilde{G}\prod (A^G/\mathcal{N}A) \to H^2(G,A).$$
(Hint: If $f(\sigma,\tau)$ is a 2-cocycle of G in A, consider the 1-cochain $u_f(\tau) = \sum_{\sigma\in G} f(\sigma,\tau)$. Using the cocycle condition and suitable choices of the variables, show the values of u_f are in A^G and that u_f is related to $\mathcal{N}f$, i.e., $\mathcal{N}f(\tau,\rho) = \sum_\sigma \sigma f(\tau,\rho)$ can be expressed by u_f.)

4. Finally, when G is cyclic, we pick a generator σ_0. There exists a distinguished element, χ_0, of $\widetilde{G}$ corresponding to σ_0, namely χ_0 is that homomorphism $G \to \mathbb{Q}/\mathbb{Z}$ whose value at σ_0 is $\frac{1}{n} \bmod \mathbb{Z}$, where $n = \#(G)$. Show that the map
$$A^G/\mathcal{N}A \to H^2(G,A)$$
via
$$\alpha \mapsto (\chi_0, \alpha) \mapsto \delta\chi_0 \smile \alpha \in H^2(G,A)$$
is the required isomorphism. For surjectivity, I suggest you consider the construction of u_f in part (3) above.

Problem 20 Let $G = \mathrm{SL}(2,\mathbb{Z})$ be the group of all 2×2 integral matrices of determinant 1; pick a prime, p, and write U for the set of 2×2 integral matrices having determinant p. G acts on U *via* $u(\in U) \mapsto \sigma u$, where $\sigma \in G$.

1. Show that the orbit space has $p+1$ elements: $0, 1, \ldots, p-1, \infty$, where j corresponds to the matrix

$$w_j = \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}$$

and ∞ corresponds to the matrix $w_\infty = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$.

2. If $\tau \in G$ and $r \in S = \{0, 1, \ldots, p-1, \infty\} = G\backslash U$, show there exists a unique $r' \in S$ with $w_r\tau^{-1}$ in the orbit of $w_{r'}$. Write $\tau \cdot r = r'$ and prove this gives an action of G on S. Hence, we have a group homomorphism $P : G \to \mathrm{Aut}(S) = \mathfrak{S}_{p+1}$.

3. If $N = \ker P$, prove that G/N is isomorphic to the group $\mathrm{PSL}(2, \mathbb{F}_p)$ consisting of all "fractional linear transformations"

$$x \mapsto x' = \frac{ax+b}{cx+d}, \quad a, b, c, d \in \mathbb{F}_p,\ ad - bc = 1.$$

Show further that

i. $$\#\big(\mathrm{PSL}(2,\mathbb{F}_p)\big) = \begin{cases} \dfrac{p(p+1)(p-1)}{2} & \text{if } p \neq 2 \\ 6 & \text{if } p = 2 \end{cases}$$

and

ii. $\mathrm{PSL}(2,\mathbb{F}_p)$ acts transitively on S under the action of (2).

4. Now prove: $\mathrm{PSL}(2,\mathbb{F}_p)$ is simple if $p \geq 5$. (Note: $\mathrm{PSL}(2,\mathbb{F}_3)$ is A_4, $\mathrm{PSL}(2,\mathbb{F}_5)$ is A_5, but $\mathrm{PSL}(2,\mathbb{F}_p)$ is not A_n if $p \geq 7$. So, you now have a second infinite collection of simple finite groups—these are finite group analogs of the Lie groups $\mathrm{PSL}(2,\mathbb{C})$).

Problem 21 We write $\mathrm{PSL}(2,\mathbb{Z})$ for the group $\mathrm{SL}(2,\mathbb{Z})/(\pm I)$.

(1) Let ξ be a chosen generator for $\mathbb{Z}/3\mathbb{Z}$ and η the generator of $\mathbb{Z}/2\mathbb{Z}$. Map $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$ to $\mathrm{PSL}(2,\mathbb{Z})$ *via*

$$\varphi(\xi) = x = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} (\mathrm{mod}\ \pm I)$$

and

$$\psi(\eta) = y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} (\mathrm{mod}\ \pm I)$$

Then we obtain a map

$$\varphi \amalg \psi \colon \mathbb{Z}/3\mathbb{Z} \amalg \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{PSL}(2,\mathbb{Z})$$

(here, the coproduct is in the category Grp). What is the image of $\varphi \amalg \psi$? What is the kernel?

(2) If

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad \text{in } \mathrm{PSL}(2,\mathbb{Z})$$

express x and y above (in $\mathrm{SL}(2,\mathbb{Z})$) in terms of a and b and show that $\mathrm{SL}(2,\mathbb{Z}) = \mathrm{Grp}\{a, b\}$. Can you express a and b in terms of x and y?

(3) For any odd prime number, p, the element

$$\sigma(p) = \begin{pmatrix} 1 & \frac{p-1}{2} \\ 0 & 1 \end{pmatrix}$$

is equal to $a^{(p-1)/2}$. For any $\sigma \in \mathrm{SL}(2, \mathbb{Z})$, we define the *weight of σ with respect to a and b* by

$$\mathrm{wt}(\sigma) = \inf(\text{length of all words in } a, b, a^{-1}, b^{-1}, \text{ which words equal } \sigma)$$

By deep theorems of Selberg, Margulis and others (in geometry and analysis) one knows that

$$\mathrm{wt}(\sigma(p)) = O(\log p) \qquad \text{as } p \to \infty.$$

(Our expression for $\sigma(p)$ as a power of a shows that we have a word of size $O(p)$ for $\sigma(p)$, yet no explicit word of size $O(\log p)$ is known as of now (Fall, 2005) and the role of b in this is very mysterious.) Now the *Cayley graph* of a group, G, generated by the elements $g_1, \ldots, g_t$ is that graph whose vertices are the elements of G and whose edges emanating from a vertex $\tau \in G$ are the ones connecting τ and $\tau g_1, \ldots, \tau g_t$. Show that the diameter of the Cayley graph of the group $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$ with respect to the generators $\overline{a}$ and $\overline{b}$ is $O(\log p)$.

Problem 22 Let G be a finite group in this problem.

1. Classify all group extensions

$$0 \to \mathbb{Q} \to \mathcal{G} \to G \to 0. \qquad (E)$$

Your answer should be in terms of the collection of all subgroups of G, say H, with $(G : H) \leq 2$, plus, perhaps, other data.

2. Same question as (1) for group extensions

$$0 \to \mathbb{Z} \to \mathcal{G} \to G \to 0, \qquad (E)$$

same kind of answer.

3. Write V for the “four-group” $\mathbb{Z}/2\mathbb{Z} \prod \mathbb{Z}/2\mathbb{Z}$. There are two actions of $\mathbb{Z}/2\mathbb{Z}$ on V: Flip the factors, take each element to its inverse. Are these the only actions? Find all group extensions

$$0 \to V \to \mathcal{G} \to \mathbb{Z}/p\mathbb{Z} \to 0. \qquad (E)$$

The group $\mathcal{G}$ is a group of order 8; compare your results with what you know from Problems 1–6.

4. Say H is any other group, G need no longer be finite and A, B are abelian groups. Suppose $\varphi : H \to G$ is a homomorphism and we are given a group extension

$$0 \to A \to \mathcal{G} \to G \to 0. \qquad (E)$$

Show that, in a canonical way, we can make a group extension

$$0 \to A \to \widetilde{\mathcal{G}} \to H \to 0. \qquad (\varphi^* E)$$

(Note: your answer has to be in terms of G, H, $\mathcal{G}$ and any homomorphisms between them as these are the only “variables” present. You’ll get the idea if you view an extension as a fibre space.)

Now say $\psi : A \to B$ is a group homomorphism and we are given an extension

$$0 \to A \to \mathcal{G} \to G \to 0. \qquad (E)$$

Construct, in a canonical way, an extension

$$0 \to B \to \widetilde{\mathcal{G}} \to G \to 0. \qquad (\psi_* E)$$

5. Explain, carefully, the relevance of these two constructions to parts (1) and (2) of this problem.

Problem 23 Say A is any abelian group, and write G for the *wreath product* $A^n \wr \mathfrak{S}_n$. Show:

1. $[G, G] \neq G$
2. $\big(G : [G, G]\big) = \infty \iff A$ is infinite
3. If $n \geq 2$, then $[G, G] \neq \{1\}$.
4. Give a restriction on n which prevents G from being solvable.

Problem 24 If $\{G_\alpha\}_{\alpha \in \Lambda}$ is a family of *abelian* groups, write $\coprod\limits_{\alpha} G_\alpha$ for

$$\coprod_{\alpha} G_\alpha = \Big\{(\xi_\alpha) \in \prod_{\alpha} G_\alpha \mid \text{ for all but finitely many } \alpha, \text{ we have } \xi_\alpha = 0\Big\}.$$

Then $\coprod_\alpha G_\alpha$ is the *coproduct* of the G_α in $\mathcal{A}$b. Write as well

$$(\mathbb{Q}/\mathbb{Z})_p = \{\xi \in \mathbb{Q}/\mathbb{Z} \mid p^r\xi = 0, \text{ some } r > 0\};$$

here, p is a prime. Further, call an *abelian* group, A, *divisible* iff

$$(\forall\, n)(A \xrightarrow{n} A \to 0 \text{ is exact}).$$

Prove: Theorem Every divisible (abelian) group is a coproduct of copies of $\mathbb{Q}$ and $(\mathbb{Q}/\mathbb{Z})_p$ for various primes p. The group is torsion iff no copies of $\mathbb{Q}$ appear, it is torsion-free iff no copies of $(\mathbb{Q}/\mathbb{Z})_p$ appear (any p). Every torsion-free, divisible, abelian group is naturally a vector space over $\mathbb{Q}$.

Problem 25

1. If G is a group of order n, show that $G \wr \operatorname{Aut}(G)$ is isomorphic to a subgroup of $\mathfrak{S}_n$.
2. Consider the cycle $(1, 2, \ldots, n) \in \mathfrak{S}_n$; let H be the subgroup (of $\mathfrak{S}_n$) generated by the cycle. Prove that
$$\mathcal{N}_{\mathfrak{S}_n}(H) \cong (\mathbb{Z}/n\mathbb{Z}) \wr \operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}).$$

Problem 26 Let TOP denote the category of topological spaces.

1. Show that TOP possesses finite fibred products and finite fibred coproducts.
2. Is (1) true without the word "finite"?
3. Write T2TOP for the full subcategory of TOP consisting of Hausdorff topological spaces. Are (1) and (2) true in T2TOP? If you decide the answer is "no", give reasonable conditions under which a positive result holds. What relation is there between the product (coproduct) you constructed in (1) (or (2)) and the corresponding objects in this part of the problem?

Problem 27 Let R be a ring (not necessarily commutative) and write $\mathcal{M}$od(R) for the category of (left) R-modules; i.e., the action of R on a module, M, is on the left. We know $\mathcal{M}$od(R) has finite products and finite fibred products.

1. What is the situation for infinite products and infinite fibred products?
2. What is the situation for coproducts (finite or infinite) and for fibred coproducts (both finite and infinite)?

Problem 28 As usual, write $\mathcal{G}\mathrm{r}$ for the category of groups. Say G and G' are groups and $\varphi : G \to G'$ is a homomorphism. Then $(G, \varphi) \in \mathcal{G}\mathrm{r}_{G'}$, the comma category of "groups over G'". The group $\{1\}$ possess a canonical morphism to G', namely the inclusion, i. Thus, $\big(\{1\}, i\big) \in \mathcal{G}\mathrm{r}_{G'}$, as well. We form their product in $\mathcal{G}\mathrm{r}_{G'}$, i.e., we form the fibred product $G \prod\limits_{G'} \{1\}$. Prove that there exists a canonical *monomorphism*

$$G \prod_{G'} \{1\} \to G.$$

Identify its image in G.
Now consider the "dual" situation: G' maps to G, so $G \in \mathcal{G}\mathrm{r}^{G'}$ (*via* φ) the "groups co-over G'". We also have the canonical map $G' \to \{1\}$, killing all the elements of G'; so, as above, we can form the fibred coproduct of G and $\{1\}$: $G \overset{G'}{\amalg} \{1\}$. Prove that there exists a canonical epimorphism

$$G \to G \overset{G'}{\amalg} \{1\},$$

identify its kernel in G.

Problem 29 Write CR for the category of commutative rings with unity and RNG for the category of rings with unity.

1. Consider the following two functors from CR to $\mathcal{S}$ets:

   (a) $|\mathcal{M}_{pq}| : A \rightsquigarrow$ underlying set of $p \times q$ matrices with entries from A

   (b) $|\mathrm{GL}_n| : A \rightsquigarrow$ underlying set of all invertible $n \times n$ matrices with entries from A.

   Prove the these two functors are representable.

2. A slight modification of (b) above yields a functor from CR to $\mathcal{G}\mathrm{r}$: namely,

   $$\mathrm{GL}_n : A \rightsquigarrow \textit{group} \text{ of all invertible } n \times n \text{ matrices with entries from } A.$$

   When $n = 1$, we can extend this to a functor from RNG to $\mathcal{G}\mathrm{r}$. That is we get the functor

   $$\mathbb{G}_m : A \rightsquigarrow \text{group of all invertible elements of } A.$$

   Prove that the functor $\mathbb{G}_m$ has a left adjoint, let's temporarily call it (†); that is: There is a functor (†) from $\mathcal{G}\mathrm{r}$ to RNG, so that

   $$(\forall\, G \in \mathcal{G}\mathrm{r})(\forall\, R \in \mathrm{RNG})(\mathrm{Hom}_{\mathrm{RNG}}((\dagger)(G), R) \cong \mathrm{Hom}_{\mathcal{G}\mathrm{r}}(G, \mathbb{G}_m(R))),$$

   via a functorial isomorphism.

3. Show that without knowing what ring $(\dagger)(G)$ is, namely that it exists and that (†) is left adjoint to $\mathbb{G}_m$, we can prove: the category of $(\dagger)(G)$-modules, $\mathcal{M}\mathrm{od}\big((\dagger)(G)\big)$, is equivalent—in fact isomorphic—to the category of G-modules.

4. There is a functor from $\mathcal{G}\mathrm{r}$ to Ab, namely send G to $G^{\mathrm{ab}} = G/[G, G]$. Show this functor has a right adjoint, call it I. Namely, there exists a functor $I : \mathrm{Ab} \to \mathcal{G}\mathrm{r}$, so that

   $$(\forall\, G \in \mathcal{G}\mathrm{r})(\forall\, H \in \mathrm{Ab})(\mathrm{Hom}_{\mathcal{G}\mathrm{r}}(G, I(H)) \cong \mathrm{Hom}_{\mathrm{Ab}}(G^{\mathrm{ab}}, H)).$$

   Does $G \rightsquigarrow G^{\mathrm{ab}}$ have a left adjoint?

Problem 30 (Kaplansky) If A and B are 2×2-matrices with entries in $\mathbb{Z}$, we embed A and B into the 4×4 matrices as follows:

$$\begin{aligned} A^{\mathrm{aug}} &= \begin{pmatrix} 0 & I \\ A & 0 \end{pmatrix} \\ B^{\mathrm{aug}} &= \begin{pmatrix} 0 & I \\ B & 0 \end{pmatrix}. \end{aligned}$$

Is it true that if A^{aug} and B^{aug} are similar over $\mathbb{Z}$, then A and B are similar over $\mathbb{Z}$? Proof or counterexample. What about the case where the entries lie in $\mathbb{Q}$?

Problem 31 We fix a commutative ring with unity, A, and write $\mathcal{M}$ for $\mathcal{M}_{pq}(A)$, the $p \times q$ matrices with entries in A. Choose a $q \times p$ matrix, Γ, and make $\mathcal{M}$ a ring *via*:

Addition: as usual among $p \times q$ matrices
Multiplication: if $R, S \in \mathcal{M}$, set $R * S = R\Gamma S$, where $R\Gamma S$ is the ordinary product of matrices.

Write $\mathcal{M}(\Gamma)$ for $\mathcal{M}$ with these operations, then $\mathcal{M}(\Gamma)$ is an A-algebra (a ring which is an A-module).

1. Suppose that A is a field. Prove that the isomorphism classes of $\mathcal{M}(\Gamma)$'s are finite in number (here p and q are fixed while Γ varies); in fact, are in natural one-to-one correspondence with the integers $0, 1, 2, \ldots, B$ where B is to be determined by you.

2. Given two $q \times p$ matrices Γ and $\widetilde{\Gamma}$ we call them equivalent iff $\widetilde{\Gamma} = W\Gamma Z$, where $W \in \mathrm{GL}(q, A)$ and $Z \in \mathrm{GL}(p, A)$. Prove: each Γ is equivalent to a matrix

$$\begin{pmatrix} I_r & 0 \\ 0 & H \end{pmatrix}$$

where $I_r = r \times r$ identity matrix and the entries of H are non-units of A. Is r uniquely determined by Γ? How about the matrix H?

3. Call the commutative ring, A, a *local ring* provided it possesses exactly one maximal ideal, $\mathfrak{m}_A$. For example, any field is a local ring; the ring $\mathbb{Z}/p^n\mathbb{Z}$ is local if p is a prime; other examples of this large, important class of rings will appear below. We have the descending chain of ideals

$$A \supseteq \mathfrak{m}_A \supseteq \mathfrak{m}_A^2 \supseteq \cdots.$$

For some local rings one knows that $\bigcap\limits_{t \geq 0} \mathfrak{m}_A^t = (0)$; let's call such local rings "good local rings" for temporary nomenclature. If A is a good local ring, we can define a function on A to $\mathbb{Z} \cup \{\infty\}$, call it ord, as follows:

$\mathrm{ord}(\xi) = 0$ if $\xi \notin \mathfrak{m}_A$
$\mathrm{ord}(\xi) = n$ if $\xi \in \mathfrak{m}_A^n$ but $\xi \notin \mathfrak{m}_A^{n+1}$
$\mathrm{ord}(0) = \infty$.

The following properties are simple to prove:

$\mathrm{ord}(\xi \pm \eta) \geq \min\{\mathrm{ord}(\xi), \mathrm{ord}(\eta)\}$
$\mathrm{ord}(\xi\eta) \geq \mathrm{ord}(\xi) + \mathrm{ord}(\eta)$.

Consider the $q \times p$ matrices under equivalence and look at the following three conditions:

(i) Γ is equivalent to $\begin{pmatrix} I_r & 0 \\ 0 & H \end{pmatrix}$, with $H = (0)$

(ii) Γ is equivalent to $\begin{pmatrix} I_r & 0 \\ 0 & H \end{pmatrix}$ with H having non-unit entries and $r \geq 1$

(iii) $(\exists\, Q \in \mathcal{M})(\Gamma Q \Gamma = \Gamma)$.

Of course, i. $\Longrightarrow$ ii. if $\Gamma \neq (0)$, A any ring. Prove: if A is any (commutative) ring then i. $\Longrightarrow$ iii., and if A is good local i. and iii. are equivalent. Show further that if A is good local then $\mathcal{M}(\Gamma)$ possesses a non-trivial idempotent, P, (an element such that $P * P = P$, $P \neq 0, \neq 1$) if and only if Γ has ii.

4. Write $\mathcal{I} = \{U \in \mathcal{M}(\Gamma) \mid \Gamma U \Gamma = 0\}$ and given $P \in \mathcal{M}(\Gamma)$, set
$$B(P) = \{V \in \mathcal{M}(\Gamma) \mid (\exists\, Z \in \mathcal{M}(\Gamma))(V = P * Z * P)\}.$$
If iii. above holds, show there exists $P \in \mathcal{M}(\Gamma)$ so that $P * P = P$ and $\Gamma P \Gamma = \Gamma$. For such a P, prove that $B(P)$ is a subring of $\mathcal{M}(\Gamma)$, that $\mathcal{M}(\Gamma) \cong B(P) \amalg \mathcal{I}$ in the category of A-modules, and that $\mathcal{I}$ is a two-sided ideal of $\mathcal{M}(\Gamma)$ (by exhibiting $\mathcal{I}$ as the kernel of a surjective ring homomorphism whose image you should find). Further show if i. holds, then $B(P)$ is isomorphic to the ring of $r \times r$ matrices with entries from A. When A is a field show $\mathcal{I}$ is a maximal 2-sided ideal of $\mathcal{M}(\Gamma)$, here $\Gamma \neq (0)$. Is $\mathcal{I}$ the unique maximal (2-sided) ideal in this case?

5. Call an idempotent, P, of a ring *maximal* (also called *principal*) iff when L is another idempotent, then $PL = 0 \implies L = 0$. Suppose Γ satisfies condition iii. above, prove that an idempotent, P, of $\mathcal{M}(\Gamma)$ is maximal iff $\Gamma P \Gamma = \Gamma$.

Problem 32 Let A be the field of real numbers $\mathbb{R}$ and conserve the notations of Problem 31. Write X for a $p \times q$ matrix of functions of one variable, t, and consider the Γ-*Riccati Equation*
$$\frac{dX}{dt} = X\Gamma X. \qquad ((*)_\Gamma)$$

1. If $q = p$ and Γ is invertible, show that either the solution, $X(t)$, blows up at some finite t, or else $X(t)$ is equivalent to a matrix
$$\widetilde{X}(t) = \begin{pmatrix} 0 & O(1) & O(t) & \dots & O(t^{p-1}) \\ 0 & 0 & O(1) & \dots & O(t^{p-2}) \\ & & \dots\dots\dots\dots & & \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix},$$
where $O(t^s)$ means a polynomial of degree $\leq s$. Hence, in this case, $X(t)$ must be nilpotent.

2. Suppose $q \neq p$ and Γ has rank r. Let P be an idempotent of $\mathcal{M}(\Gamma)$ with $\Gamma P \Gamma = \Gamma$. If $Z \in \mathcal{M}(\Gamma)$, write $Z^\flat$ for $Z - P * Z * P$; so $Z^\flat \in \mathcal{I}$. Observe that $\mathcal{I}$ has dimension $pq - r^2$ as an $\mathbb{R}$-vector space. Now assume that for a solution, $X(t)$, of $(*)_\Gamma$, we have $X(0) \in \mathcal{I}$. Prove that $X(t)$ exists for all t. Can you give necessary and sufficient conditions for $X(t)$ to exist for all t?

3. Apply the methods of (2) to the case $p = q$ but $r = \operatorname{rank} \Gamma < p$. Give a similar discussion.

Problem 33 A module, M, over a ring, R, is called *indecomposable* iff we *cannot* find two submodules M_1 and M_2 of M so that $M \xrightarrow{\sim} M_1 \amalg M_2$ in the category of R-modules.

1. Every ring is a module over itself. Show that if R is a local ring, then R is indecomposable as an R-module.

2. Every ring, R, with unity admits a homomorphism $\mathbb{Z} \to R$ (i.e., $\mathbb{Z}$ is an *initial object* in the category RNG). The kernel of $\mathbb{Z} \to R$ is the principal ideal $n\mathbb{Z}$ for some $n \geq 0$; this n is the *characteristic of* R. Show that the characteristic of a local ring must be 0 or a prime power. Show by example that every possibility occurs as a characteristic of some local ring.

3. Pick a point in $\mathbb{R}$ or $\mathbb{C}$; without loss of generality, we may assume this point is 0. If f is a function we say f is locally defined at 0 iff f has a domain containing some (small) open set, U, about 0 (in either $\mathbb{R}$ or $\mathbb{C}$). Here, f is $\mathbb{R}$- or $\mathbb{C}$-valued, independent of where its domain is. When f and g are locally defined at 0, say f makes sense on U and g on V, we'll call f and g *equivalent at* 0 $\iff$ there exists open W, $0 \in W$, $W \subseteq U \cap V$ and $f \restriction W = g \restriction W$. A *germ of a function at* 0 is an equivalence class of a function. If we consider germs of functions that are at least continuous near 0, then when they form a ring they form a local ring.
   Consider the case $\mathbb{C}$ and complex valued germs of holomorphic functions at 0. This is a local ring. Show it is a good local ring.
   In the case $\mathbb{R}$, consider the germs of real valued C^k functions at 0, for some k with $0 \le k \le \infty$. Again, this is a local ring; however, show it is NOT a good local ring.
   Back to the case $\mathbb{C}$ and the good local ring of germs of complex valued holomorphic functions at 0. Show that this local ring is also a principal ideal *domain*.

   In the case of real valued C^∞ germs at $0 \in \mathbb{R}$, exhibit an infinite set of germs, each in the maximal ideal, no finite subset of which generates the maximal ideal (in the sense of ideals). These germs are NOT to belong to $\mathfrak{m}^2$.

Problem 34 Recall that for every integral domain, A, there is a field, $\mathrm{Frac}(A)$, containing A minimal among all fields containing A. If B is an A-algebra, an element $b \in B$ is *integral over* $A \iff$ there exists a *monic* polynomial, $f(X) \in A[X]$, so that $f(b) = 0$. The domain, A, is *integrally closed in* B iff every $b \in B$ which is integral over A actually comes from A (*via* the map $A \to B$). The domain, A, is *integrally closed* (also called *normal*) iff it is integrally closed in $\mathrm{Frac}(A)$. Prove:

1. A is integrally closed $\iff$ $A[X]/\big(f(X)\big)$ is an integral domain for every MONIC irreducible polynomial, $f(X)$.

2. A is a UFD $\iff$ A possesses the ACC on principal ideals and $A[X]/\big(f(X)\big)$ is an integral domain for every irreducible polynomial $f(X)$. (It follows that every UFD is a normal domain.)

3. If k is a field and the characteristic of k is not 2, show that $A = k[X, Y, Z, W]/(XY - ZW)$ is a normal domain. What happens if $\mathrm{char}(k) = 2$?

Problem 35 Suppose that R is an integral domain and F is its fraction field, $\mathrm{Frac}(R)$. Prove that, as R-module, the field F is "the" injective hull of R. A sufficient condition that F/R be injective is that R be a PID. Is this condition necessary? Proof or counter-example.

Problem 36 If A is a ring, write $\mathrm{End}^*(A)$ for the collection of *surjective* ring endomorphisms of A. Suppose A is commutative and noetherian, prove $\mathrm{End}^*(A) = \mathrm{Aut}(A)$.

Problem 37 Write $M(n, A)$ for the ring of all $n \times n$ matrices with entries from A (A is a ring). Suppose K and k are fields and $K \supseteq k$.

1. Show that if $M, N \in M(n, k)$ and if there is a $P \in \mathrm{GL}(n, K)$ so that $PMP^{-1} = N$, then there is a $Q \in \mathrm{GL}(n, k)$ so that $QMQ^{-1} = N$.

2. Prove that (1) is false for rings $B \supseteq A$ *via* the following counterexample:
   $A = \mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$, $B = \mathbb{C}[X, Y]/(X^2 + Y^2 - 1)$. Find two matrices similar in $M(2, B)$ but NOT similar in $M(2, A)$.

3. Let S^n be the n-sphere and represent $S^n \subseteq \mathbb{R}^{n+1}$ as $\{(z_0, \ldots, z_n) \in \mathbb{R}^{n+1} \mid \sum_{j=0}^n z_j^2 = 1\}$. Show that there is a *natural injection* of $\mathbb{R}[X_0, \ldots, X_n]/(\sum_{j=0}^n X_j^2 - 1)$ into $C(S^n)$, the ring of (real valued) continuous functions on S^n. Prove further that the former ring is an integral domain but $C(S^n)$ is not. Find the group of units in the former ring.

Problem 38 (Rudakov) Say A is a ring and M is a rank 3 free A-module. Write Q for the bilinear form whose matrix (choose some basis for M) is

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

Thus, if $v = (x, y, z)$ and $w = (\xi, \eta, \zeta)$, we have

$$Q(v, w) = (x, y, x) \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \xi \\ \eta \\ \zeta \end{pmatrix}.$$

Prove that $Q(w, v) = Q(v, Bw)$ with $B = I + \text{nilpotent} \iff a^2 + b^2 + c^2 = abc$.

Problem 39 Let M be a Λ-module (Λ is not necessarily commutative) and say N and N' are submodules of M.

1. Suppose $N + N'$ and $N \cap N'$ are f.g. Λ-modules. Prove that both N and N' are then f.g. Λ-modules.
2. Give a generalization to finitely many submodules, $N_1, \ldots, N_t$ of M.
3. Can you push part (2) to an infinite number of N_j?
4. If M is noetherian as a Λ-module, is Λ necessarily noetherian as a ring (left noetherian as M is a left module)? What about $\overline{\Lambda} = \Lambda/\mathrm{Ann}(M)$?

Problem 40 Suppose that V is a not necessarily finite dimensional vector space over a field, k. We assume given a map from *subsets*, S, of V to *subspaces*, $[S]$, of V which map satisfies:

(a) For every S, we have $S \subseteq [S]$

(b) $[\,]$ is monotone; that is, $S \subseteq T$ implies $[S] \subseteq [T]$.

(c) For every S, we have $[S] = [[S]]$

(d) If W is a subspace of V and $W \neq V$, then $[W] \neq V$.

(1) Under conditions (a)—(d), prove that $[S] = \mathrm{Span}\, S$.

(2) Give counter-examples to show that the result is false if we remove either (a) or (d). What about (b) or (c)?

(3) What happens if we replace k by a ring R, consider subsets and submodules and replace $\mathrm{Span}\, S$ by the R-module generated by S?

Problem 41 (Continuation of Problem 34)

1. Consider the ring $A(n) = \mathbb{C}[X_1, \ldots, X_n]/(X_1^2 + \cdots + X_n^2)$. There is a condition on n, call it $C(n)$, so that $A(n)$ is a UFD iff $C(n)$ holds. Find explicitly $C(n)$ and prove the theorem.
2. Consider the ring $B(n) = \mathbb{C}[X_1, \ldots, X_n]/(X_1^2 + X_2^2 + X_3^3 + \cdots + X_n^3)$. There is a condition on n, call it $D(n)$, so that $B(n)$ is a UFD iff $D(n)$ holds. Find explicitly $D(n)$ and prove the theorem.
3. Investigate exactly what you can say if $C(n)$ (respectively $D(n)$) does not hold.
4. Replace $\mathbb{C}$ by $\mathbb{R}$ and answer (1) and (2).

5. Can you formulate a theorem about the ring $A[X,Y]/\bigl(f(X,Y)\bigr)$ of the form $A[X,Y]/\bigl(f(X,Y)\bigr)$ is a UFD provided $f(X,Y)\cdots$? Here, A is a given UFD and f is a polynomial in $A[X,Y]$. Your theorem must be general enough to yield (1) and (2) as easy consequences. (You must prove it too.)

Problem 42 (Exercise on projective modules) In this problem, $A \in \mathcal{O}\mathrm{b}(\mathrm{CR})$.

1. Suppose P and P' are projective A-modules, and M is an A-module. If
$$\begin{aligned} 0 \to K \to &P \to M \to 0 \qquad \text{and} \\ 0 \to K' \to &P' \to M \to 0 \end{aligned}$$
are exact, prove that $K' \amalg P \cong K \amalg P'$.

2. If P is a f.g. projective A-module, write P^D for the A-module $\mathrm{Hom}_A(P, A)$. We have a canonical map $P \to P^{DD}$. Prove this is an isomorphism.

3. Again, P is f.g. projective; suppose we're given an A-linear map $\mu : \mathrm{End}_A(P) \to A$. Prove: there exists a unique element $f \in \mathrm{End}_A(P)$ so that $(\forall\, h \in \mathrm{End}_A(P))(\mu(h) = \mathrm{tr}(hf))$. Here, you must define the trace, tr, for f.g. projectives, P, as a well-defined map, then prove the result.

4. Again, P is f.g. projective; μ is as in (3). Show that $\mu(gh) = \mu(hg) \iff \mu = a\,\mathrm{tr}$ for some $a \in A$.

5. Situation as in (2), then each $f \in \mathrm{End}_A(P)$ gives rise to $f^D \in \mathrm{End}_A(P^D)$. Show that $\mathrm{tr}(f) = \mathrm{tr}(f^D)$.

6. Using categorical principles, reformulate (1) for injective modules and prove your reformulation.

Problem 43 Suppose K is a commutative ring and $a, b \in K$. Write $A = K[T]/(T^2 - a)$; there is an automorphism of A (the identity on K) which sends t to $-t$, where t is the image of T in A. If $\xi \in A$, we write $\overline{\xi}$ for the image of ξ under this automorphism. Let $\mathbb{H}(K; a, b)$ denote the set
$$\mathbb{H}(K; a, b) = \left\{ \begin{pmatrix} \xi & b\eta \\ \overline{\eta} & \overline{\xi} \end{pmatrix} \,\middle|\, \xi, \eta \in A \right\},$$
this is a subring of the 2×2 matrices over A. Observe that $q \in \mathbb{H}(K; a, b)$ is a unit there iff q is a unit of the 2×2 matrices over A.

1. Consider the non-commutative polynomial ring $K\langle X, Y\rangle$. There is a 2-sided ideal, $\mathcal{I}$, in $K\langle X, Y\rangle$ so that $\mathcal{I}$ is symmetrically generated *vis a vis* a and b and $K\langle X, Y\rangle/\mathcal{I}$ is naturally isomorphic to $\mathbb{H}(K; a, b)$. Find the generators of $\mathcal{I}$ and establish the explicit isomorphism.

2. For pairs (a, b) and (α, β) decide exactly when $\mathbb{H}(K; a, b)$ is isomorphic to $\mathbb{H}(K; \alpha, \beta)$ as objects of the comma category RNG^K.

3. Find all isomorphism classes of $\mathbb{H}(K; a, b)$ when $K = \mathbb{R}$ and when $K = \mathbb{C}$. If $K = \mathbb{F}_p$, $p \neq 2$ answer the same question and then so do for $\mathbb{F}_2$.

4. When K is just some field, show $\mathbb{H}(K; a, b)$ is a "division ring" (all non-zero elements are units) $\iff$ the equation $X^2 - aY^2 = b$ has no solution in K (here we assume a is not a square in K). What is the case if a *is* a square in K?

5. What is the center of $\mathbb{H}(K; a, b)$?

6. For the field $K = \mathbb{Q}$, prove that $\mathbb{H}(\mathbb{Q}; a, b)$ is a division ring $\iff$ the surface $aX^2 + bY^2 = Z^2$ has no points whose coordinates are integers except 0.

Problem 44

1. If A is a commutative ring and $f(X) \in A[X]$, suppose $(\exists\, g(X) \neq 0)(g(X) \in A[X]$ and $g(X)f(X) = 0)$. Show: $(\exists\, \alpha \in A)(\alpha \neq 0$ and $\alpha f(X) = 0)$. *Caution*: A may possess non-trivial nilpotent elements.

2. Say K is a field and $A = K[X_{ij},\, 1 \le i, j \le n]$. The matrix
$$M = \begin{pmatrix} X_{11} & \dots & X_{1n} \\ & \cdot\,\cdot\,\cdot\,\cdot\,\cdot & \\ X_{n1} & \dots & X_{nn} \end{pmatrix}$$
has entries in A and $\det(M) \in A$. Prove that $\det(M)$ is an irreducible polynomial of A.

Problem 45 Let A be a commutative noetherian ring and suppose B is a commutative A-algebra which is f.g. as an A-algebra. If $G \subseteq \mathrm{Aut}_{A-\mathrm{alg}}(B)$ is a *finite* subgroup, write
$$B^G = \{b \in B \mid \sigma(b) = b,\ \text{all } \sigma \in G\}.$$
Prove that B^G is also f.g. as an A-algebra; hence B^G is noetherian.

Problem 46 Again, A is a commutative ring. Write $\mathrm{RCF}(A)$ for the ring of $\infty \times \infty$ matrices all of whose rows and all of whose columns possess but finitely many (*not* bounded) non-zero entries. This *is* a ring under ordinary matrix multiplication (as you see easily).

1. Specialize to the case $A = \mathbb{C}$; find a *maximal* two-sided ideal, $\mathcal{E}$, of $\mathrm{RCF}(\mathbb{C})$. Prove it is such and is the only such. You are to find $\mathcal{E}$ explicitly. Write $E(\mathbb{C})$ for the ring $\mathrm{RCF}(\mathbb{C})/\mathcal{E}$.

2. Show that there exists a natural injection of rings M_n ($= n \times n$ complex matrices) $\hookrightarrow \mathrm{RCF}(\mathbb{C})$ so that the composition $M_n \to E(\mathbb{C})$ is *still* injective. Show further that if $p \mid q$ we have a commutative diagram
$$\begin{tikzcd} M_p \arrow[rr, hook] \arrow[dr, hook] & & M_q \arrow[dl, hook] \\ & E(\mathbb{C}) & \end{tikzcd}$$

Problem 47 (Left and right noetherian) For parts (1) and (2), let $A = \mathbb{Z}\langle X, Y\rangle/(YX, Y^2)$—a non-commutative ring.

1. Prove that
$$\mathbb{Z}[X] \hookrightarrow \mathbb{Z}\langle X, Y\rangle \to A$$
is an injection and that $A = \mathbb{Z}[X] \amalg \big(\mathbb{Z}[X]y\big)$ as a left $\mathbb{Z}[X]$-module (y is the image of Y in A); hence A is a left noetherian ring.

2. However, the right ideal generated by $\{X^n y \mid n \ge 0\}$ is NOT f.g. (prove!); so, A is not right noetherian.

3. Another example. Let
$$C = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a \in \mathbb{Z};\, b, c, \in \mathbb{Q} \right\}.$$
Then C is right noetherian but NOT left noetherian (prove!).

Problem 48 If $\{B_\alpha, \varphi_\alpha^\beta\}$ is a right mapping system of Artinian rings and if $B = \varinjlim_\alpha B_\alpha$ and B is noetherian, prove that B is Artinian.

Problem 49 Suppose that A is a commutative noetherian ring and B is a given A-algebra which is flat and finite as an A-module. Define a functor $\mathit{Idem}_{B/A}(-)$ which associates to each A-algebra, T the set $\mathit{Idem}_{B/A}(T) = \mathrm{Idem}(B \otimes_A T)$ consisting of all idempotent elements of the ring $B \otimes_A T$.

(1) Prove the functor $\mathit{Idem}_{B/A}$ is representable.

(2) Show the representing ring, C, is a noetherian A-algebra and that it is *étale* over A.

Problem 50 (Vector bundles) As usual, TOP is the category of topological spaces and k will be either the real or complex numbers. All vector spaces are to be finite dimensional. A *vector space family over* X is an object, V, of TOP_X (call p the map $V \to X$) so that

i. $(\forall\, x \in X)(p^{-1}(x)$ (denoted V_x) is a k-vector space)

ii. The induced topology on V_x is the usual topology it has as a vector space over k.

Example: The trivial family $X \,\Pi\, k^n$ (fixed n).
Vector space families over X form a category, $\mathrm{VF}(X)$, if we define the morphisms to be those morphisms, φ, from TOP_X which satisfy:

$$(\forall\, x \in X)(\varphi_x : V_x \to W_x \text{ is a linear map.})$$

1. Say $Y \xrightarrow{\theta} X$ is a continuous map. Define a functor $\theta^* : \mathrm{VF}(X) \rightsquigarrow \mathrm{VF}(Y)$, called pullback. When Y is a subspace of X, the pullback, $\theta^*(V)$, is called the restriction of V to Y, written $V \restriction Y$.
A vector space family is a *vector bundle* $\iff$ it is *locally trivial*, that is:
$(\forall\, x \in X)(\exists$ open $U)(x \in U)$ (so that $V \restriction U$ is isomorphic (in $\mathrm{VF}(U)$) to $U \,\Pi\, k^n$, some n). Let $\mathrm{Vect}(X)$ denote the *full* subcategory of $\mathrm{VF}(X)$ formed by the objects that are vector bundles.

2. Say X is an r-dimensional vector space considered in TOP. Write $\mathbb{P}(X)$ for the collection of all hyperplanes through $0 \in X$, then $\mathbb{P}(X)$ is a topological space and is covered by opens each isomorphic to an $(r-1)$-dimensional vector space. On $\mathbb{P}(X)$ we make an element of $\mathrm{VF}\big(\mathbb{P}(X)\big)$: W is the set of pairs $(\xi, \nu) \in \mathbb{P}(X) \,\Pi\, X^D$ so that $\xi \subset \ker \nu$. Here, X^D is the dual space of X. Show that W is a line bundle on $\mathbb{P}(X)$.

3. If $V \in \mathrm{Vect}(X)$ and X is connected, then $\dim(V_x)$ is constant on X. This number is the *rank* of V.

4. A *section of* V *over* U is a map $\sigma : U \to V \restriction U$ so that $p \circ \sigma = \mathrm{id}_U$. Write $\Gamma(U, V)$ for the collection of sections of V over U. Show: If $V \in \mathrm{Vect}(X)$, each section of V over U is just a compatible family of locally defined vector valued functions on U. Show further that $\Gamma(U, V)$ is a vector space in a natural way.

5. Say V and W are in $\mathrm{Vect}(X)$, with ranks p and q respectively. Show: $\mathrm{Hom}(V, W)$ is isomorphic to the collection of locally defined "compatible" families of *continuous* functions $U \to \mathrm{Hom}(k^p, k^q)$, *via* the local description
$$\varphi \in \mathrm{Hom}(V, W) \rightsquigarrow \widetilde{\varphi} : U \to \mathrm{Hom}(k^p, k^q),$$
where $\varphi(u, v) = \big(u, \widetilde{\varphi}(u)(v)\big)$. Here, $V \restriction U$ is trivial and $v \in k^p$.

   Now $\mathrm{Iso}(k^p, k^q) = \{\psi \in \mathrm{Hom}(k^p, k^q) \mid \psi \text{ is invertible}\}$ is an open of $\mathrm{Hom}(k^p, k^q)$.

6. Show: $\varphi \in \mathrm{Hom}(V, W)$ is an isomorphism $\iff$ for a covering family of opens, $U (\subseteq X)$, we have $\widetilde{\varphi}(U) \subseteq \mathrm{Iso}(k^p, k^q) \iff (\forall\, x \in X)(\varphi_x : V_x \to W_x$ is an isomorphism).

7. Show $\{x \mid \varphi_x$ is an isomorphism (here, $\varphi \in \mathrm{Hom}(U, V)$)$\}$ is open in X.

8. Show all of (1) to (6) go over when $X \in C^k{-}\mathrm{MAN}$ $(0 \le k \le \infty)$ with appropriate modifications; C^k replacing continuity where it appears.

Problem 51 (Linear algebra for vector bundles). First just look at finite dimensional vector spaces over k (remember k is $\mathbb{R}$ or $\mathbb{C}$) and say F is some functor from vector spaces to vector spaces (F might even be a several variable functor). Call F *continuous* $\iff$ the map $\mathrm{Hom}(V,W) \to \mathrm{Hom}\big(F(V), F(W)\big)$ is continuous. (Same definition for C^k, $1 \le k \le \infty$, ω). If we have such an F, extend it to bundles *via* the following steps:

1. Suppose V is the trivial bundle: $X \ \Pi \ k^p$. As sets, $F(X \ \Pi \ k^p)$, is to be just $X \ \Pi \ F(k^p)$, so we give $F(X \ \Pi \ k^p)$ the product topology. Prove: If $\varphi \in \mathrm{Hom}(V,W)$, then $F(\varphi)$ is continuous, therefore $F(\varphi) \in \mathrm{Hom}\big(F(V), F(U)\big)$. Show, further, φ is an isomorphism $\implies$ $F(\varphi)$ is an isomorphism.

2. Set $F(V) = \bigcup_{x \in X}(x, V_x)$, then the topology on $F(V)$, when V is trivial, appears to depend on the specific trivialization. Show this is not true—it is actually independent of same.

3. If V is any bundle, then $V \restriction U$ is trivial for small open U, so by (1) and (2), $F(V \restriction U)$ is a trivial bundle. Topologize $F(V)$ by calling a set, Z, open iff $Z \cap \big(F(V \restriction U)\big)$ is open in $F(V \restriction U)$ for all U where $V \restriction U$ is trivial. Show that if $Y \subseteq X$, then the topology on $F(V \restriction Y)$ is just that on $F(V) \restriction Y$, that $\varphi : V \to W$ continuous $\implies$ $F(\varphi)$ is continuous and extend all these things to C^k. Finally prove: If $f : Y \to X$ in TOP then $f^*\big(F(V)\big) \cong F\big(f^*(V)\big)$ and similarly in C^k−MAN.

4. If we apply (3) , we get for vector bundles:

   (a) $V \amalg W$, more generally finite coproducts

   (b) V^D, the dual bundle

   (c) $V \otimes W$

   (d) $\mathcal{H}om(V,W)$, the vector bundle of (locally defined) homomorphisms.

   Prove: $\Gamma\big(U, \mathcal{H}om(V,W)\big) \cong \mathrm{Hom}(V \restriction U, W \restriction U)$ for *every* open, U, of X. Is this true for the bundles of (a), (b), (c)?

Problem 52 Recall that if $R \in$ RNG, $J(R)$—the Jacobson radical of R— is just the intersection of all (left) maximal ideals of R. The ideal, $J(R)$, is actually 2-sided.

1. Say $J(R) = (0)$ (e.g., $R = \mathbb{Z}$). Show that no non-projective R-module has a projective cover.

2. Suppose M_i, $i = 1, \dots, t$ are R-modules with projective covers $P_1, \dots, P_t$. Prove that $\coprod_i P_i$ is a projective cover of $\coprod_i M_i$.

3. Say M and N are R-modules and assume M and $M \amalg N$ have projective covers. Show that N has one.

4. In M is an R-module, write (as usual) $M^D = \mathrm{Hom}_R(M,R)$. Then M^D is an R^{op}-module. Prove that if M is finitely generated and projective as an R-module, then M^D has the same properties as an R^{op}-module.

Problem 53 Let $\{M_\alpha\}$ be a given family of R^{op}-modules. Define, for R-modules, two functors:

$$U : N \rightsquigarrow \Big(\Big(\prod_\alpha M_\alpha\Big) \otimes_R N\Big)$$

$$V : N \rightsquigarrow \prod_\alpha (M_\alpha \otimes_R N).$$

1. Show that V is right-exact and is exact iff each M_α is flat over R.

2. Show there exists a morphism of functors $\theta : U \to V$. Prove that $\theta_N : U(N) \to V(N)$ is surjective if N is finitely generated, while θ_N is an isomorphism if N is finitely presented.

Problem 54 (Continuation of Problems 50 and 51). Let V and W be vector bundles and $\varphi\colon V \to W$ a homomorphism. Call φ a *monomorphism* (respectively *epimorphism*) iff
$(\forall\, x \in X)(\varphi_x\colon V_x \to W_x$ is a monomorphism (respectively epimorphism)). Note: φ is a monomorphism iff $\varphi^D\colon W^D \to V^D$ is an epimorphism. A *sub-bundle* of V is a subset which is a vector bundle in the induced structure.

1. Prove: If $\varphi\colon V \to W$ is a monomorphism, then $\varphi(V)$ is a sub-bundle of W. Moreover, locally on X, there exists a vector bundle, G, say on the open $U \subseteq X$, so that $(V \restriction U) \amalg G \cong W \restriction U$ (i.e., every sub-bundle is *locally* part of a coproduct decomposition of W). Prove also: $\{x \mid \varphi_x$ is a monomorphism$\}$ is open in X. (Suggestion: Say $x \in X$, pick a subspace of W_x complementary to $\varphi(V_x)$, call it Z. Form $G = X \amalg Z$. Then there exists a homomorphism $V \amalg G \to W$, look at this homomorphism near the point x.)

2. Say V is a sub-bundle of W, show that $\bigcup_{x\in X}(x, W_x/V_x)$ (with the quotient topology) is actually a vector bundle (not just a vector space family) over X.

3. Now note we took a full subcategory of $\mathrm{VF}(X)$, so for $\varphi \in \mathrm{Hom}(V, W)$ with $V, W \in \mathrm{Vect}(X)$, the dimension of $\ker \varphi_x$ need not be locally constant on X. When it is locally constant, call φ a *bundle homomorphism*. Prove that if φ is a bundle homomorphism from V to W, then

   (i) $\bigcup_x(x, \ker \varphi_x)$ is a sub-bundle of V

   (ii) $\bigcup_x(x, \mathrm{Im}\, \varphi_x)$ is a sub-bundle of W, hence

   (iii) $\bigcup_x(x, \mathrm{coker}\, \varphi_x)$ is a vector bundle (quotient topology).

   We refer to these bundles as $\ker\varphi$, $\mathrm{Im}\,\varphi$ and $\mathrm{coker}\,\varphi$, respectively. Deduce from your argument for (i) that

   (iv) Given $x \in X$, there exists an open U, with $x \in U$, so that $(\forall\, y \in U)(\mathrm{rank}\, \varphi_y \geq \mathrm{rank}\, \varphi_x)$. Of course, this φ is not necessarily a bundle homomorphism.

Problem 55 (Continuation of Problem 54) In this problem, X is *compact Hasudorff*. We use two results from analysis:

A) (Tietze extension theorem). If X is a normal space and Y a closed subspace while V is a real vector space, then every continuous map $Y \to V$ admits an extension to a continuous map $X \to V$. Same result for $X \in C^k-$MAN and C^k maps.

B) (Partitions of unity). Say X is compact Hausdorff and $\{U_\alpha\}$ is a finite open cover of X. There exist continuous maps, f_α, taking X to $\mathbb{R}$ such that

   (i) $f_\alpha \geq 0$, (all α)

   (ii) $\mathrm{supp}(f_\alpha) \subseteq U_\alpha$ (so $f_\alpha \in C^0_0(U_\alpha)$)

   (iii) $(\forall\, x \in X)(\sum_\alpha f_\alpha(x) = 1)$.

   The same is true for C^k-MAN (X compact!) and C^k functions $(1 \leq k \leq \infty)$.

1. Extend Tietze to vector bundles: If X is compact Hausdorff, $Y \subseteq X$ closed and $V \in \mathrm{Vect}(X)$, then every section $\sigma \in \Gamma(Y, V\restriction Y)$ extends to a section in $\Gamma(X, V)$. (Therefore, there exist *plenty* of continuous or C^∞ global sections of V. FALSE for holomorphic sections). Apply this to the bundle $\mathcal{H}om(V, W)$ and prove: If Y is closed in X with X (as usual) compact Hausdorff or compact C^k-manifold and if $\varphi\colon V \restriction Y \to W \restriction Y$ is an isomorphism of vector bundles, then there exists an open, U, with $Y \subseteq U$, so that φ extends to an isomorphism $V \restriction U \to W \restriction U$.

2. Every vector space possesses a metric (take any of the p-norms, or take the 2-norm for simplicity). It's easy to see that metrics then exist on trivial bundles. In fact, use the 2-norm, so we can "bundleize" the notion of Hermitian form (Problem 51) and get the bundle $\mathcal{H}erm(V)$. Then an Hermitian metric on V is a global section of $\mathcal{H}erm(V)$ which is positive definite, at each $x \in X$. Show every bundle possesses an Hermitian metric.

3. If we are given vector bundles and *bundle homomorphisms*, we say the sequence
$$\cdots \to V_j \to V_{j+1} \to V_{j+2} \to \cdots$$
of such is *exact* iff for each $x \in X$, the sequence of vector spaces
$$\cdots \to V_{j,x} \to V_{j+1,x} \to V_{j+2,x} \to \cdots$$
is exact. Prove: If $0 \to V' \to V \to V'' \to 0$ is an exact sequence of vector bundles and bundle homomorphisms, then $V \cong V' \amalg V''$. (This is not true for holomorphic bundles.)

4. Consider a vector bundle, V, and a subspace, Σ, of the vector space $\Gamma(X, V)$. We get the trivial bundle $X \amalg \Sigma$ and a natural homomorphism $X \amalg \Sigma \to V$, *via*
$$(x, \sigma) \to \sigma(x).$$
Prove: If X is compact Hausdorff (or compact C^k−MAN), there exists a *finite dimensional* subspace, Σ, of $\Gamma(X, V)$ so that the map $X \amalg \Sigma \to V$ is *surjective*. Thus there exists a finite dimensional surjective family of C-(respectively C^k-) sections of V. Use (3) to deduce: Under the usual assumption on X, for each vector bundle, V, on X, there exists a vector bundle, W, on X, so that $V \amalg W$ is a trivial bundle.

5. Write $C(X)$ (respectively $C^k(X)$, $1 \le k \le \infty$) for the ring of continuous (respectively C^k) functions (values in our field) on X, where X is compact Hausdorff (respectively a compact manifold). In a natural way (pointwise multiplication), $\Gamma(X, V)$ is an A-module ($A = C(X)$, $C^k(X)$), and Γ gives a functor from vector bundles, V, to $\mathcal{M}\text{od}(A)$. Trivial bundles go to free modules of finite rank over A (why?) Use the results above to prove:

   > Γ gives an equivalence of categories: $\text{Vect}(X)$ (as full subcaregory of $VF(X)$) and the full subcategory of A-modules whose objects are f.g. projective modules.

Problem 56

1. Say M is a f.g. $\mathbb{Z}$-module, $\neq (0)$. Prove there exists a prime p so that $M \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z} \neq (0)$. Deduce: No divisible abelian group [cf. Problem 24] can be f.g.

2. Say M, M'' are $\mathbb{Z}$-modules and M is f.g. while M'' is torsion free. Given $\varphi \in \text{Hom}(M, M'')$ suppose $(\forall\,\text{primes } p)$(the induced map $M \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z} \to M'' \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z}$ *is* a monomorphism). Show that φ is a monomorphism and M is free.

3. If M is a divisible abelian group, prove that M possesses no maximal subgroup. Why does Zorn's Lemma fail?

Problem 57 Given Λ, $\Gamma \in \text{RNG}$ and a ring homomorphism $\Lambda \to \Gamma$ (thus, Γ is a Λ-algebra), if M is a Λ-module, then $M \otimes_\Lambda \Gamma$ has the natural structure of a Γ^{op}-module. Similarly, if Z is both a Λ^{op}-module and a Γ-module, then $Z \otimes_\Lambda M$ is still a Γ-module. Now let N be a Γ-module,

1. Prove there is a *natural* isomorphism
$$\text{Hom}_\Gamma(Z \otimes_\Lambda M, N) \xrightarrow{\sim} \text{Hom}_\Lambda(M, \text{Hom}_\Gamma(Z, N)). \tag{$*$}$$
Prove, in fact, the functors $M \rightsquigarrow M \otimes_\Lambda Z$ and $N \rightsquigarrow \text{Hom}_\Gamma(Z, N)$ are adjoint functors, i.e., $(*)$ is functorial.

2. Establish an analog of $(*)$:
$$\mathrm{Hom}_\Gamma(M, \mathrm{Hom}_\Lambda(Z, N)) \cong \mathrm{Hom}_\Lambda(Z \otimes_\Gamma M, N) \tag{$**$}$$
under appropriate conditions on Z, M and N (what are they?)

3. Show: M projective as a Λ^{op}-module, Z projective as a Γ^{op}-module $\Longrightarrow$ $M \otimes_\Lambda Z$ is projective as a Γ^{op}-module. In particular, M projective as a Λ^{op}-module $\Longrightarrow$ $M \otimes_\Lambda \Gamma$ is projective as a Γ^{op}-module and of course, the same statement (without the op) for $Z \otimes_\Lambda M$ and $\Gamma \otimes_\Lambda M$. Show further that, if N is Λ-injective, then $\mathrm{Hom}_\Lambda(\Gamma, N)$ is Γ-injective.

4. For abelian groups, M, write $M^D = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$. Then, if M is free, M^D is injective as a $\mathbb{Z}$-module (why?). From this deduce: Every abelian group is a subgroup of an injective abelian group.

5. (Eckmann) Use (3) and (4) to prove the Baer Embedding Theorem: For every ring, Γ, each Γ-module is a submodule of an injective Γ-module.

Problem 58 Here, A and B are commutative rings and $\varphi : A \to B$ a ring homomorphism so that B is an A-algebra. Assume B is flat (i.e., as an A-module, it's flat). Define a homomorphism
$$\theta : \mathrm{Hom}_A(M, N) \otimes_A B \to \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B)$$
(functorial in M and N)—how?

1. If M is f.g. as an A-module, θ is injective.

2. If M is f.p. as an A-module, θ is an isomorphism.

3. Assume M is f.p. as an A-module, write $\mathfrak{a}$ for the annihilator of M $(= (M \to (0)))$. Prove that $\mathfrak{a} \otimes_A B$ is the annihilator of $M \otimes_A B$ in B.

Problem 59 Let k be a field and f be a *monic* polynomial of *even* degree in $k[X]$.

1. Prove there exist g, $r \in k[X]$ such that $f = g^2 + r$ and $\deg r < \frac{1}{2} \deg f$. Moreover, g and r are unique.

   Now specialize to the case $k = \mathbb{Q}$, and suppose f has *integer* coefficients. Assume $f(X)$ is *not* the square of a polynomial with rational coefficients.

2. Prove there exist only *finitely* many integers, x, such that the value $f(x)$ is a square, say y^2, where $y \in \mathbb{Z}$. In which ways can you get the square of an integer, y, by adding 1 to third and fourth powers of an integer, x?

3. Show there exists a constant, K_N, depending ONLY on the degree, N, of f so that:

   > If all coefficients of f are bounded in absolute value by C (≥ 1) then whenever $\langle x, y \rangle$ is a solution of $y^2 = f(x)$ (with x, $y \in \mathbb{Z}$) we have $|x| \leq K_N C^N$.

4. What can you say about the number of points $\langle x, y \rangle$ with rational coordinates which lie on the (hyperelliptic) curve $Y^2 = f(X)$?

Problem 60 Consider $\mathcal{M}\mathrm{od}(\mathbb{Z})$ and copies of $\mathbb{Z}$ indexed by $\mathbb{N} = \{1, 2, \ldots\}$. Form the module $\prod_{\mathbb{N}} \mathbb{Z}$. It is a product of $\aleph_0$ projective modules. Show $M = \prod_{\mathbb{N}} \mathbb{Z}$ is *not* projective as a $\mathbb{Z}$-module. (Suggestions: Establish that each submodule of a free module over a PID is again free, therefore we need to show M is not free. Look at
$$K = \{\xi = (\xi_j) \in M \mid (\forall\, n)(\exists\, k = k(n))(2^n \mid \xi_j \text{ if } j > k(n))\}.$$[10]
This is a submodule of M; show $K/2K$ is a vector space over $\mathbb{Z}/2\mathbb{Z}$ of the same dimension as K and finish up. Of course, 2 could be replaced by any prime). So, products of projectives need not be projective.

[10] The condition means that $\lim_{j \mapsto \infty} \xi_j$ is zero in the "2-adic numbers" $\mathbb{Q}_2$.

Problem 61

1. Say $A \xrightarrow{\theta} B$ is a homomorphism of commutative rings and suppose it makes B a faithfully flat A-module. Show that θ is injective.

2. Hypotheses as in (1), but also assume B is finitely presented as an A-algebra (e.g., B is finitely generated and A is noetherian). Show that there exists an A-module, M, so that $B \cong A \amalg M$, as A-modules.

3. Assume A and B are local rings, $\theta : A \to B$ is a ring map (N.B. so that we assume $\theta(\mathfrak{m}_A) \subseteq \mathfrak{m}_B$) and B, as an A-module, is flat. Write $\mathcal{N}(A)$, respectively $\mathcal{N}(B)$, for the nilradicals of A, respectively B. [That is,
$$\mathcal{N}(A) = \big\{\xi \in A \mid (\exists n \in \mathbb{N})(\xi^n = 0)\big\}, \text{ etc.]}$$
Prove:
   (a) If $\mathcal{N}(B) = (0)$, then $\mathcal{N}(A) = (0)$.
   (b) If B is an integral domain, so is A.

   Are the converses of (a), (b) true? Proof or counter-example.

Problem 62 Here, I is an index set and $\mathcal{S}(I)$ is the set of all *finite* subsets of I. Partially order $\mathcal{S}(I)$ by inclusion, then it is directed[11] Also, let $\mathcal{C}$ be a category having *finite* products or *finite* coproducts as the case may be below (e.g., groups, Ω-groups, modules). Say for each $\alpha \in I$ we are given an object $M_\alpha \in \mathcal{C}$. For ease of notation below, write $M_S = \coprod_{\alpha\in S} M_\alpha$ and $M_S^* = \prod_{\alpha\in S} M_\alpha$, where $S \in \mathcal{S}(I)$ is given. Prove:
If $\mathcal{C}$ has right limits and finite coproducts, then $\mathcal{C}$ has arbitrary coproducts; indeed,
$$\varinjlim_{S\in\mathcal{S}(I)} M_S = \coprod_{\alpha\in I} M_\alpha.$$
Prove a similar statement for left limits and products.

Problem 63 Recall that a ring, Λ, is *semi-simple*[12] iff every Λ-module, M, has the property:

(∀ submodules, M', of M)(∃ another submodule, M'', of M)($M \cong M' \amalg M''$).

There is a condition on the positive integer, n, so that n has this condition $\iff$ $\mathbb{Z}/n\mathbb{Z}$ is semi-simple. Find the condition and prove the theorem.

Problem 64 In this problem, $A \in$ CR. If $\alpha_1, \ldots, \alpha_m$ are in A, write $\big(\alpha_1, \ldots, \alpha_n\big)$ for the ideal generated by $\alpha_1, \ldots, \alpha_n$ in A. Recall that $K_0(A)$, the *Grothendieck group* of A, is the quotient of the free abelian group on the (isomorphism classes of) finitely generated A-modules (as generators) by the subgroup generated by the relations: if $0 \to M' \to M \to M'' \to 0$ is exact in $\mathcal{M}\mathrm{od}(A)$, then $[M] - [M'] - [M'']$ is a relation.

1. If $\alpha \in A$, show that in $K_0(A)$ we have
$$\big[((\alpha) \to 0)\big] = \big[A/(\alpha)\big]$$

2. If A is a PID and M is a finite length A-module, show that $[M] = 0$ in $K_0(A)$.

3. Prove: If A is a PID, then for all finitely generated A-modules, M, there exists a unique integer $r = r(M)$, so that $[M] = r[A]$ in $K_0(A)$; hence, $K_0(A)$ is $\mathbb{Z}$. Prove further that $r(M) = \dim(M \otimes_A \mathrm{Frac}(A))$.

[11] One also says $\mathcal{S}(I)$ has the Moore–Smith property.
[12] Cf. also, Problem 145.

Problem 65 Write $\mathcal{LCA}\mathrm{b}$ for the category of locally compact abelian topological groups, the morphisms being continuous homomorphisms. Examples include: Every abelian group with the discrete topology; $\mathbb{R}$; $\mathbb{C}$; $\mathbb{R}/\mathbb{Z} = \mathbb{T}$, etc. If $G \in \mathcal{LCA}\mathrm{b}$, write

$$G^D = \mathrm{Hom}_{\mathrm{cts}}(G, \mathbb{T}),$$

make G^D a group *via* pointwise operations and topologize G^D *via* the compact-open topology; that is, take the sets

$$U(C, \epsilon) = \big\{ f \in G^D \mid \mathrm{Im}(f \restriction C) \subseteq -\epsilon < \arg z < \epsilon \big\}$$

—where C runs over the compact subsets of G containing 0, ϵ is positive and we identify $\mathbb{T}$ with the unit circle in $\mathbb{C}$—as a fundamental system of neighborhoods at 0 in G^D.

1. Suppose G is actually compact. Prove G^D is discrete in this topology. Likewise, prove if G is discrete, then G^D is compact in this topology. Finally prove G^D is locally compact in this topology.

2. If $\{G_\alpha, \varphi_\alpha^\beta\}$ is a right (respectively left) mapping family of *finite* abelian groups, then $\Big\{G_\alpha^D, \big(\varphi_\alpha^\beta\big)^D\Big\}$ becomes a left (respectively right) mapping family, again of *finite* abelian groups (how, why?). Prove that
$$\Big(\varinjlim_{\alpha} G_\alpha\Big)^D \cong \varprojlim_{\alpha} G_\alpha^D$$
and
$$\Big(\varprojlim_{\alpha} G_\alpha\Big)^D \cong \varinjlim_{\alpha} G_\alpha^D$$
as *topological* groups. We call a group *profinite* $\iff$ it is isomorphic, as a *topological* group, to a left limit of finite groups.

3. Prove the following three conditions are equivalent for an abelian topological group, G:
   (a) G is profinite
   (b) G is a compact, Hausdorff, totally disconnected group
   (c) G^D is a discrete torsion group.

4. For this part, $\big\{G_\alpha\big\}$ is a family of *compact* groups, not necessarily abelian, and the index set has Moore–Smith. Assume we are given, for each α, a closed, normal subgroup of G_α, call it S_α, and that $\beta \geq \alpha \implies G_\beta \subseteq G_\alpha$ and $S_\beta \subseteq S_\alpha$. Show that the family $\big\{H_\alpha = G_\alpha/S_\alpha\big\}_\alpha$ can be made into a left mapping family, in a natural way, and that
$$\varprojlim_{\alpha} H_\alpha \cong \bigcap_{\alpha} G_\alpha \Big/ \bigcap_{\alpha} S_\alpha \quad \text{(as topological groups.)}$$

5. If G is a compact topological group, write $\big\{U_\alpha | \alpha \in I\big\}$ for the family of *all open, normal* subgroups of G. Continue (3) by proving:
$$G \text{ is profinite} \iff G \text{ is compact and } \bigcap_{\alpha} U_\alpha = \{1\}.$$

6. Here, G need not be abelian. We define $\mathbb{Z}_p$ as $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ and $\hat{\mathbb{Z}}$ as $\varprojlim_{n} \mathbb{Z}/n\mathbb{Z}$ (Artin ordering for the n's). Quickly use (2) to compute $\mathbb{Z}_p^D$ and $(\hat{\mathbb{Z}})^D$. Now consider the following mathematical statements:
   (a) $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$
   (b) $\mathbb{Q}^* \cong \mathbb{Z}/2\mathbb{Z} \, \Pi \, \prod_p \mathbb{Z}$

(c) $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - 1/p^s}, \quad \text{if Re } s > 1$

(d) A statement you know well and are to fill in here concerning arithmetic in $\mathbb{Z}$.

Show (a)-(d) are mutually equivalent.

Problem 66 Fix an abelian group, A, for what follows. Write $A_n = A$, all $n \in \mathbb{N}$ and give $\mathbb{N}$ the Artin ordering. If $n \preceq m$ (i.e. $n|m$) define $\varphi_n^m : A_n \to A_m$ by $\varphi_n^m(\xi) = \left(\frac{m}{n}\right)\xi$, and define $\psi_m^n : A_m \to A_n$ by $\psi_m^n(\xi) = \left(\frac{m}{n}\right)\xi$, too. Let

$$\tilde{A} = \varinjlim \{A_n, \varphi_n^m\} \quad \text{and} \quad T(A) = \varprojlim \{A_m, \psi_m^n\}.$$

($T(A) =$ *full Tate group of* A).

1. Prove that both $\tilde{A}$ and $T(A)$ are divisible groups.

2. Show that if $A = A_1 \xrightarrow{\varphi} \tilde{A}$ is the canonical map into the direct limit, then $\ker(\varphi) = t(A)$, the torsion subgroup of A. Hence, every torsion free abelian group is a subgroup of a divisible group. Given any abelian group , A, write
$$0 \to K \to F \to A \to 0,$$
for some free abelian group F. Show that A may be embedded in $\tilde{F}/K$; hence deduce anew that every abelian group embeds in a divisible abelian group.

3. If A is a free $\mathbb{Z}$-module, what is $T(A)$?

4. If $A \to B \to 0$ is exact, need $T(A) \to T(B) \to 0$ also be exact? Proof or counterexample.

5. Show that if $T(A) \neq (0)$, then A is not finitely generated.

Problem 67 Again, as in Problem 61, let $\theta : A \to B$ be a homomorphism of commutative rings and assume B is faithfully flat over A *via* θ. If M is an A-module, write M_B for $M \otimes_A B$.

1. Prove: M is finitely generated as an A-module iff M_B is finitely generated as a B-module.

2. Same as (1) but for finite presentation instead of finite generation.

3. Show: M is locally free over A iff M_B is locally free over B.

4. When, if ever, is $S^{-1}A$ faithfully flat over A?

Note, of course, that these are results on faithfully flat descent.

Problem 68 Here, $\Lambda \in$ RNG and assume

$$0 \to M' \to M \to M'' \to 0$$

is an exact sequence of Λ-modules.

1. Assume further, M'' is a flat Λ-module. Prove: For all Λ^{op}-modules, N, the sequence
$$0 \to N \otimes_\Lambda M' \to N \otimes_\Lambda M \to N \otimes_\Lambda M'' \to 0$$
is again exact. (You might look at the special case when M is free first.)

2. Again assume M'' is flat; prove M and M' are flat $\iff$ either is flat. Give an example of Λ, M', M, M'' in which both M and M' are flat but M'' is not flat.

Problem 69 (Topologies, Sheaves and Presheaves). Let X be a topological space. We can make a category, $\mathcal{T}_X$, which is specified by and specifies the topology as follows: $\mathcal{O}\mathrm{b}\,\mathcal{T}_X$ consists of the open sets in X. If $U, V \in \mathcal{O}\mathrm{b}\,\mathcal{T}_X$, we let

$$\mathrm{Hom}(U,V) = \begin{cases} \emptyset & \text{if } U \not\subseteq V, \\ \{\mathrm{incl}\} & \text{if } U \subseteq V, \end{cases}$$

here $\{\mathrm{incl}\}$ is the one element set consisting of the inclusion map $\mathrm{incl} : U \to V$.

1. Show that $U \prod_X V$—the fibred product of U and V (over X) in $\mathcal{T}_X$—is just $U \cap V$. Therefore $\mathcal{T}_X$ has finite fibred products.

2. If $\mathcal{C}$ is a given category (think of $\mathcal{C}$ as $\mathcal{S}$ets, $\mathcal{A}$b, or more generally Λ-$\mathcal{M}$odules) a *presheaf on X with values in $\mathcal{C}$* is a cofunctor from $\mathcal{T}_X$ to $\mathcal{C}$. So, F is a presheaf iff ($\forall$ open $U \subseteq X$)($F(U) \in \mathcal{C}$) and when $U \hookrightarrow V$, we have a map $\rho^U_V : F(V) \to F(U)$ (in $\mathcal{C}$) usually called *restriction from V to U*. Of course, we have $\rho^W_V = \rho^W_U \circ \rho^U_V$. The basic example, from which all the terminology comes, is this:

$$\mathcal{C} = \mathbb{R}\text{-modules } (= \text{vector spaces over } \mathbb{R})$$
$$F(U) = \{\text{continuous real valued functions on the open set } U\}.$$

   Now recall that a category is an *abelian category* iff for each morphism $A \xrightarrow{\varphi} B$ in $\mathcal{C}$, there are two pairs: $(\ker\varphi, i)$ and $(\mathrm{coker}\,\varphi, j)$ with $\ker\varphi$ and $\mathrm{coker}\,\varphi$ objects of $\mathcal{C}$ and $i : \ker\varphi \to A$, $j : B \to \mathrm{coker}\,\varphi$ so that:

   (a) $\mathrm{Hom}_{\mathcal{C}}(A,B)$ is an abelian group, operation denoted $+$
   (b) $\ker\varphi \to A \to B$ is zero in $\mathrm{Hom}_{\mathcal{C}}(\ker\varphi, B)$
   (c) If $C \xrightarrow{u} A \to B$ is zero, there is a unique morphism $C \to \ker\varphi$ so that u is the composition $C \to \ker\varphi \xrightarrow{i} A$
   (d) Similar to (c) for coker, with appropriate changes.

   Define $\mathrm{Im}\,\varphi$ as $\ker(B \xrightarrow{j} \mathrm{coker}\,\varphi)$. Now exact sequences make sense in $\mathcal{C}$ (easy, as you see). Write $\mathcal{P}(X,\mathcal{C})$ for the category of presheaves on X with values in $\mathcal{C}$. If $\mathcal{C}$ is abelian show that $\mathcal{P}(X,\mathcal{C})$ is an abelian category, too, in a natural way.

3. If $A \in \mathcal{O}\mathrm{b}\,\mathcal{C}$, we can make a presheaf $\mathfrak{A}$ by: $\mathfrak{A}(U) = A$, all open U and if $V \hookrightarrow U$ then $\rho^U_V = id_A$. This is the *constant presheaf* with values in A. Generalize it as follows: Fix open U of X, define $\mathfrak{A}_U$ by:

$$\mathfrak{A}_U(W) = \coprod_{\mathrm{Hom}(W,U)} A = \begin{cases} (0) & \text{if } W \not\subseteq U \\ A & \text{if } W \subseteq U. \end{cases}$$

   Show $\mathfrak{A}_U$ is a presheaf and $\mathfrak{A}$ is one of these $\mathfrak{A}_U$; which one? Generalize further: Say $\mathcal{F}$ is a presheaf of sets on X, define $\mathfrak{A}_{\mathcal{F}}$ by:

$$\mathfrak{A}_{\mathcal{F}}(W) = \coprod_{\mathcal{F}(W)} A = \big\{\text{functions} : \mathcal{F}(W) \to A \mid \text{these functions have finite support}\big\}.$$

   Make $\mathfrak{A}_{\mathcal{F}}$ into a presheaf on X; it is a clear generalization of $\mathfrak{A}_U$ and this, in turn, generalizes $\mathfrak{A}$.

4. Just as with the defining example in (2), which is called the *presheaf of germs of continuous functions on* X, so we can define the presheaf of germs of C^k-functions, real-analytic functions, complex holomorphic functions, meromorphic functions when X is a real (resp. complex) manifold. Namely:

$$C^k(U) = \{f : U \to \mathbb{R} \mid f \text{ is } C^k \text{ on } U\} \quad 0 \le k \le \infty$$
$$C^\omega(U) = \{f : U \to \mathbb{R} \mid f \text{ is real analytic on } U\}$$
$$\mathrm{Hol}(U) = \{f : U \to \mathbb{C} \mid f \text{ is holomorphic on } U\}$$
$$\mathrm{Mer}(U) = \{f : U \to \mathbb{C} \mid f \text{ is meromorphic on } U\}.$$

Prove: The collection $\{\mathfrak{Z}_U \mid U \text{ open in } X\}$ is *a set of generators* for $\mathcal{P}(X, \mathcal{A}\mathrm{b})$; that is: For all presheaves $\mathcal{F}$, there is a subcollection of the U's, say $\{U_\alpha \mid \alpha \in \Lambda\}$, so that there is a surjection $\coprod\limits_I \Bigl(\coprod\limits_{\alpha\in\Lambda} \mathfrak{Z}_U\Bigr) \twoheadrightarrow \mathcal{F}$, for some *set* I. (Then it turns out that every presheaf embeds in an injective presheaf.)

5. Now sheaves are special kinds of presheaves. Say $U \in \mathcal{T}_X$ and we have a family of morphisms of $\mathcal{T}_X$: $\{U_\alpha \to U\}_{\alpha\in\Lambda}$ (we'll suppress mention of Λ in what follows). We call this family a *covering family* $\iff \bigcup_\alpha U_\alpha = U$, i.e. the U_α form an open covering of U. Of course, if $\xi \in F(U)$, then $\rho_U^{U_\alpha}(\xi) \in F\bigl(U_\alpha\bigr)$, each α; here, F is a presheaf. Hence we get a map

$$\theta : F(U) \to \prod_\alpha F\bigl(U_\alpha\bigr).$$

Now if $\xi_\alpha \in F\bigl(U_\alpha\bigr)$, for each α, then $\rho_{U_\alpha}^{U_\alpha\cap U_\beta}\bigl(\xi_\alpha\bigr)$ lies in $F\bigl(U_\alpha \cap U_\beta\bigr)$ therefore we get a map

$$p_{1,\alpha} : F\bigl(U_\alpha\bigr) \to \prod_\beta F\bigl(U_\alpha \cap U_\beta\bigr).$$

Take the product of these over α and get a map

$$p_1 : \prod_\alpha F\bigl(U_\alpha\bigr) \to \prod_{\alpha,\beta} F\bigl(U_\alpha \cap U_\beta\bigr).$$

If $\xi_\beta \in F\bigl(U_\beta\bigr)$ then $\rho_{U_\beta}^{U_\alpha\cap U_\beta}\bigl(\xi_\beta\bigr) \in F\bigl(U_\alpha \cap U_\beta\bigr)$ therefore we get a map

$$p_{2,\beta} : F\bigl(U_\beta\bigr) \to \prod_\alpha F\bigl(U_\alpha \cap U_\beta\bigr).$$

Again the product over β gives:

$$p_2 : \prod_\beta F\bigl(U_\beta\bigr) \to \prod_{\alpha,\beta} F\bigl(U_\alpha \cap U_\beta\bigr),$$

hence we get two maps:

$$\prod_\gamma F\bigl(U_\gamma\bigr) \underset{p_2}{\overset{p_1}{\rightrightarrows}} \prod_{\alpha,\beta} F\bigl(U_\alpha \cap U_\beta\bigr).$$

Here is the definition of a *sheaf*: A *sheaf, F, of sets* is a presheaf, F, of sets so that ($\forall$ open U) $\Bigl(\forall \text{ covers } \bigl\{U_\alpha \to U\bigr\}_\alpha\Bigr)$, the sequence

$$F(U) \xrightarrow{\theta} \prod_\gamma F\bigl(U_\gamma\bigr) \underset{p_2}{\overset{p_1}{\rightrightarrows}} \prod_{\alpha,\beta} F\bigl(U_\alpha \cap U_\beta\bigr) \tag{S}$$

is exact in the sense that θ *maps* $F(U)$ *bijectively* to the set $\bigl(\xi_\gamma\bigr) \in \prod\limits_\gamma F\bigl(U_\gamma\bigr)$ for which $p_1\bigl(\bigl(\xi_\gamma\bigr)\bigr) = p_2\bigl(\bigl(\xi_\gamma\bigr)\bigr)$.

Show that the presheaves of germs of continuous, k-fold continuous, differentiable, analytic, holomorphic and meromorphic functions are all sheaves. In so doing understand what exactness of sequence (S) means. Prove, however, that $\mathfrak{A}$ is NOT generally a sheaf. (Note: a sheaf with values in $\mathcal{A}\mathrm{b}$ or RNG or Ω-groups is just a presheaf with these values which forms a sheaf of sets.) For which presheaves, $\mathcal{F}$, is $\mathfrak{A}_{\mathcal{F}}$ a sheaf?

Problem 70 Consider $\mathcal{P}(X)$ and $\mathcal{S}(X)$ the categories of presheaves and sheaves of sets on X (our results will also work for other image categories based on sets, e.g., $\mathcal{A}$b, RNG, TOP, etc.) We have the definition of a sheaf so that

$$F(U) \xrightarrow{\theta} \prod_{\alpha} F(U_\alpha) \underset{p_2}{\overset{p_1}{\rightrightarrows}} \prod_{\beta,\gamma} F(U_\beta \cap U_\gamma) \qquad \text{(S)}$$

is exact for all open covers, $\{U_\alpha \longrightarrow U\}_\alpha$ of any open U.

(1) There are two parts to the exactness of (S): θ is injective and the image of θ is the equalizer of p_1 and p_2. Write that F satisfies $(+)$ if θ is injective. Suppose that F is any presheaf, define

$$F^{(+)} = \varinjlim_{\{U_\alpha \longrightarrow U\}} \operatorname{Ker}\,(\prod_{\alpha} F(U_\alpha) \rightrightarrows \prod_{\beta,\gamma} F(U_\beta \cap U_\gamma))$$

(the limit taken over all open covers, $\{U_\alpha \longrightarrow U\}$, of the open U). Show that $F^{(+)}$ satisfies $(+)$.

(2) If $0 \longrightarrow F' \xrightarrow{\varphi} F$ is exact in $\mathcal{P}(X, \mathcal{A}\text{b})$, set $(\operatorname{Cok}\varphi)(U) = \operatorname{Coker}\varphi(U) = \operatorname{Coker}(F'(U) \longrightarrow F(U))$. Prove that $\operatorname{Cok}\varphi$ satisfies $(+)$.

(3) Suppose that F satisfies $(+)$ show that $F^{(+)}$ satisfies (S), i.e., $F^{(+)}$ is a sheaf. Show further that, if F satisfies $(+)$, then $\operatorname{Ker}\,(F(U) \longrightarrow F^{(+)}(U)) = (0)$, i.e., $F \longrightarrow F^{(+)}$ is an injective map of presheaves. Set $F^{\#} = (F^{(+)})^{(+)}$, for any presheaf F.

(4) We know $\#$ is exact and $i\colon \mathcal{S}(X) \to \mathcal{P}(X)$ is left-exact. Prove that $\#$ is the left adjoint of i, that is

$$\operatorname{Hom}_{\mathcal{S}(X)}(F^{\#}, G) \cong \operatorname{Hom}_{\mathcal{P}(X)}(F, i(G)).$$

(5) For the derived functor $\mathcal{H}^q(F)$ $(= (R^q i)(F))$ of $i\colon \mathcal{S}(X, \mathcal{A}\text{b}) \rightsquigarrow \mathcal{P}(X, \mathcal{A}\text{b})$, prove that

$$(\mathcal{H}^q(F))^{\#} = (0).$$

Problem 71 (Grothendieck) In Problem 69, you proved the collection $\{\mathfrak{Z}_U \mid U \text{ open in } X\}$ is a set of generators for
$\mathcal{P}(X, \mathcal{A}\text{b})$.

(1) Show that the collection $\{\mathfrak{Z}_U\}$ has the following property:

(G): For each presheaf, F, and for each monomorphism $0 \longrightarrow F' \longrightarrow F$ (in $\mathcal{P}(X, \mathcal{A}\text{b})$) with $F' \neq F$, there is an open $U \subseteq X$ and a morphism $\mathfrak{Z}_U \xrightarrow{\varphi} F$, so that φ does not factor through a morphism $\mathfrak{Z}_U \longrightarrow F'$.

Prove moreover that property (G) is equivalent to the fact that $\{\mathfrak{Z}_U \mid U \text{ open in } X\}$ is a family of generators for $\mathcal{P}(X, \mathcal{A}\text{b})$.

(2) Write $\underline{\mathbb{Z}}$ for the coproduct $\coprod_{\text{all } U} \mathfrak{Z}_U$ in $\mathcal{P}(X, \mathcal{A}\text{b})$, then $\underline{\mathbb{Z}}$ is a generator for $\mathcal{P}(X, \mathcal{A}\text{b})$. Show that a presheaf, Q, on X is injective if and only if for each monomorphism $0 \longrightarrow W \longrightarrow \underline{\mathbb{Z}}$, every morphism $\theta\colon W \to Q$ extends to a morphism $\underline{\mathbb{Z}} \longrightarrow Q$.

(3) Imitate the construction for rings R, ideals $\mathfrak{A} \subseteq R$ and R-modules M, of an injective hull for M (with the correspondence $R \longleftrightarrow \underline{\mathbb{Z}}$; $\mathfrak{A} \longleftrightarrow W$; $M \longleftrightarrow$ a presheaf F) to show:

There exists a functor $Q\colon F \rightsquigarrow Q(F)$ and a morphism of functors $\psi\colon \text{id} \to Q$ so that

(a) $(\forall F \in \mathcal{P}(X, \mathcal{A}\text{b}))(\psi_F\colon F \to Q(F) \quad \text{is a monomorphism})$

and

(b) Each $Q(F)$ is an injective presheaf.

This gives the proof that $\mathcal{P}(X, \mathcal{A}\mathrm{b})$ has enough injective objects.

(4) The $\mathbb{Z}_U$ in $\mathcal{S}(X, \mathcal{A}\mathrm{b})$ defined as $\mathfrak{Z}_U^{\#}$ form a set of generators for $\mathcal{S}(X, \mathcal{A}\mathrm{b})$. The same argument as in (3) goes through and we obtain another proof (but similar to the text's proof) that $\mathcal{S}(X, \mathcal{A}\mathrm{b})$ has enough injectives.

Problem 72 (Grothendieck) Let $\mathcal{P}$ stand for the category of abelian presheaves, $\mathcal{P}(X, \mathcal{A}\mathrm{b})$, on the space X.

(1) If U is an open in X and $\{U_\alpha \longrightarrow U\}_\alpha$ is an open covering of U, we have induced a diagram of families of maps

$$\begin{tikzcd} U & \{U_\alpha\} \arrow[l] & \{U_\beta \cap U_\gamma\}_{\beta,\gamma} \arrow[l, shift left] \arrow[l, shift right] & \{U_\delta \cap U_\epsilon \cap U_\eta\}_{\delta,\epsilon,\eta} \arrow[l, shift left=2] \arrow[l] \arrow[l, shift right=2] & \cdots \arrow[l, shift left=3] \arrow[l, shift left=1] \arrow[l, shift right=1] \arrow[l, shift right=3] \end{tikzcd}$$

coming from the various projections (note that $U_\beta \cap U_\gamma = U_\beta \prod U_\gamma$; $U_\delta \cap U_\epsilon \cap U_\eta = U_\delta \prod U_\epsilon \prod U_\eta$; *etc.*). When F is a presheaf, we get a *simplicial diagram*

$$\begin{tikzcd} F(U) \arrow[r] & \prod\limits_{\alpha} F(U_\alpha) \arrow[r, shift left] \arrow[r, shift right] & \prod\limits_{\beta,\gamma} F(U_\beta \cap U_\gamma) \arrow[r, shift left=2] \arrow[r] \arrow[r, shift right=2] & \prod\limits_{\delta,\epsilon,\eta} F(U_\delta \cap U_\epsilon \cap U_\eta) \arrow[r, shift left=3] \arrow[r, shift left=1] \arrow[r, shift right=1] \arrow[r, shift right=3] & \cdots \end{tikzcd}$$

and, by taking the alternating sum of these maps, we make a sequence

$$F(U) \longrightarrow \prod_{\alpha} F(U_\alpha) \xrightarrow{\delta^0} \prod_{\beta,\gamma} F(U_\beta \cap U_\gamma) \xrightarrow{\delta^1} \prod_{\delta,\epsilon,\eta} F(U_\delta \cap U_\epsilon \cap U_\eta) \xrightarrow{\delta^2} \cdots . \qquad (*)$$

For notation, write $C^r(\{U_\alpha \longrightarrow U\}, F) = \prod_{\alpha_0, \ldots, \alpha_r} F(U_{\alpha_0} \cap \cdots \cap U_{\alpha_r})$, so that $(*)$ becomes

$$F(U) \longrightarrow C^0(\{U_\alpha \longrightarrow U\}, F) \xrightarrow{\delta^0} C^1(\{U_\alpha \longrightarrow U\}, F) \xrightarrow{\delta^1} C^2(\{U_\alpha \longrightarrow U\}, F) \xrightarrow{\delta^2} \cdots . \qquad (**)$$

Show that $(**)$ is an augmented complex (of abelian groups). We'll call $(**)$ the *explicit Čech cochain complex of the cover* $\{U_\alpha \longrightarrow U\}$ *with coefficients in* F. Denote by $H^q_{\mathrm{xpl}}(\{U_\alpha \longrightarrow U\}, F)$ its q^{th} cohomology group ($=$ Ker δ^q/Im δ^{q-1}).

(2) We know that $\mathrm{Hom}_{\mathcal{P}}(\mathfrak{Z}_V, F) = F(V)$ for all open V of X, show that

$$\mathfrak{Z}_V = \coprod_{\mathrm{Hom}(U,V)} \mathbb{Z}.$$

(3) Now let F be an injective presheaf from $\mathcal{P}$, show that

$$C^0(\{U_\alpha \longrightarrow U\}, F) \xrightarrow{\delta^0} C^1(\{U_\alpha \longrightarrow U\}, F) \xrightarrow{\delta^1} C^2(\{U_\alpha \longrightarrow U\}, F) \xrightarrow{\delta^2} \cdots \qquad (***)$$

is an *exact* sequence. (Suggestions. Show that the exactness of $(***)$ is equivalent to the exactness of

$$\coprod_{\alpha} \mathfrak{Z}_{U_\alpha} \longleftarrow \coprod_{\beta,\gamma} \mathfrak{Z}_{U_\beta \cap U_\gamma} \longleftarrow \coprod_{\delta,\epsilon,\eta} \mathfrak{Z}_{U_\delta \cap U_\epsilon \cap U_\eta} \longleftarrow \cdots \qquad (\dagger)$$

in the category $\mathcal{P}$ and check the latter exactness by evaluation on any open Y of X. For this, show that the last sequence is induced by the simplicial diagram of indexing sets

$$\begin{tikzcd} \coprod\limits_{\alpha} \mathrm{Hom}(Y, U_\alpha) & \coprod\limits_{\beta,\gamma} \mathrm{Hom}(Y, U_\beta \cap U_\gamma) \arrow[l, shift left] \arrow[l, shift right] & \coprod\limits_{\delta,\epsilon,\eta} \mathrm{Hom}(Y, U_\delta \cap U_\epsilon \cap U_\eta) \arrow[l, shift left=2] \arrow[l] \arrow[l, shift right=2] & \cdots \arrow[l, shift left=3] \arrow[l, shift left=1] \arrow[l, shift right=1] \arrow[l, shift right=3] \end{tikzcd}$$

and we can identify $\coprod_{\beta,\gamma}\mathrm{Hom}(Y, U_\beta \cap U_\gamma)$ with $M\prod M$, where $M = \coprod_\alpha \mathrm{Hom}(Y, U_\alpha)$, *etc*. Thus, that (†) is exact comes down to the exactness of the diagram

$$\begin{tikzcd}
\coprod\limits_{M}\mathbb{Z} & \coprod\limits_{M\prod M}\mathbb{Z} \arrow[l, shift left] \arrow[l, shift right] & \coprod\limits_{M\prod M\prod M}\mathbb{Z} \arrow[l, shift left=2] \arrow[l] \arrow[l, shift right=2] & \cdots\ . \arrow[l, shift left=3] \arrow[l, shift left=1] \arrow[l, shift right=1] \arrow[l, shift right=3]
\end{tikzcd}$$

But, construct a contracting homotopy for this last diagram and so complete proving $(*{*}*)$ is exact.)

(4) Prove that the δ-functor $F \rightsquigarrow H^\bullet_{\mathrm{xpl}}(\{U_\alpha \longrightarrow U\}, F)$ is universal and show that we have an isomorphism

$$H^\bullet(\{U_\alpha \longrightarrow U\}, F) \cong H^\bullet_{\mathrm{xpl}}(\{U_\alpha \longrightarrow U\}, F)$$

(functorial in F). Thus, the complex $(*{*}*)$ gives an explicit method for computing the cohomology groups, $H^\bullet(\{U_\alpha \longrightarrow U\}, -)$, of the covering $\{U_\alpha \longrightarrow U\}_\alpha$.

(5) Pass to the limit over all coverings of X and give an explicit complex to compute the Čech cohomology groups $\check{H}^\bullet(X, -)$.

Problem 73 If F is a sheaf of abelian groups on the space X, let's agree to write F again when we consider F as a presheaf.

(1) Show that there is an exact sequence

$$0 \longrightarrow \check{H}^2(X, F) \longrightarrow H^2(X, F) \longrightarrow \check{H}^1(X, \mathcal{H}^1(F))$$

and that if $\check{H}^3(X, F) = (0)$, then

$$0 \longrightarrow \check{H}^2(X, F) \longrightarrow H^2(X, F) \longrightarrow \check{H}^1(X, \mathcal{H}^1(F)) \longrightarrow 0$$

is exact.

(2) Let $\{U_\alpha \longrightarrow X\}_\alpha$ be an open cover of X and assume that

$$(\forall \alpha, \beta)(H^1(U_\alpha \cap U_\beta, F) = (0)).$$

Deduce that the natural map

$$\check{H}^2(X, F) \longrightarrow H^2(X, F)$$

is an isomorphism. If you assume only that

$$(\forall \alpha)(H^1(U_\alpha, F) = (0))$$

can you still deduce that $\check{H}^2(X, F) \cong H^2(X, F)$? Proof or counter-example.

(3) Can you continue the line of argument of (2) applied to groups such as $H^?(U_\alpha \cap U_\beta \cap U_\gamma, F)$, *etc*. and deduce further isomorphisms between Čech and derived functor cohomology? For example, try $\check{H}^3(X, F) \cong H^3(X, F)$.

(4) In a similar vein to (2) and (3) above, prove the following (known as Cartan's Isomorphism Theorem):

For the space X, let $\mathcal{U}$ be a family of open sets covering X so that

(a) If $U, V \in \mathcal{U}$, then $U \cap V \in \mathcal{U}$

(b) $\mathcal{U}$ contains arbitrarily small opens of X

(c) If $U \in \mathcal{U}$ and $q > 0$, then $\check{H}^q(U, F) = (0)$.

Then, the natural maps

$$\check{H}^q(X, F) \longrightarrow H^q(X, F)$$

are isomorphisms for all $q \geq 0$.

(Suggestions: Use induction on q, but replace X by any of the U of $\mathcal{U}$. Use a spectral sequence at the induction step to get $\check{H}^q(X,F) \cong H^q(X,F)$. Now how do you further deduce $\check{H}^q(U,F) \cong H^q(U,F)$ all $U \in \mathcal{U}$ to complete the induction?)

Remark: Two main uses of Cartan's Theorem are when X is a manifold and $\mathcal{U}$ is the family of all finite intersections of all sufficiently small open balls around each point of X and when X is an algebraic variety (over a field) and $\mathcal{U}$ is the collection of its affine open subvarieties.

Problem 74 Let k be a field, X an indeterminate (or transcendental) over k. Write $A = k[X]$ and consider an ideal, $\mathfrak{a}$, of A. The ideal, $\mathfrak{a}$, determines a topology on $k[X]$—called the $\mathfrak{a}$-*adic topology*—defined by taking as a fundamental system of neighborhoods of 0 the powers $\{\mathfrak{a}^n \mid n \geq 0\}$ of $\mathfrak{a}$. Then a fundamental system of neighborhoods at $\xi \in A$ is just the collection $\{\xi + \mathfrak{a}^n \mid n \geq 0\}$.

1. Show A becomes a topological ring (i.e. addition and multiplication are continuous) in this topology. When is A Hausdorff in this topology?

2. The rings $A/\mathfrak{a}^n = A_n$ form a left mapping system. Write

$$\widehat{A} = \varprojlim_{n} A/\mathfrak{a}^n$$

and call $\widehat{A}$ the $\mathfrak{a}$-*adic completion of* A. There is a map $A \to \widehat{A}$; when is it injective?

3. Consider $\mathfrak{a} = (X) =$ all polynomials with no constant term. The ring $\widehat{A}$ in this case has special notation: $k[[X]]$. Establish an isomorphism of $k[[X]]$ with the *ring of formal power series over* k (in X) i.e. with the ring consisting of sequences $\big(c_n\big)$, $n \geq 0$, $c_n \in k$ with addition and multiplication defined by:

$$\big(c_n\big) + \big(d_n\big) = \big(c_n + d_n\big)$$
$$\big(c_n\big) \cdot \big(d_n\big) = \big(e_n\big), \quad e_n = \sum_{i+j=n} c_i d_j$$

$\Big(\big(c_n\big) \leftrightarrow \sum_{n=0}^{\infty} c_n X^n$ explains the name$\Big)$.

4. Show $k[X] \hookrightarrow k[[X]]$, that $k[[X]]$ is an integral domain and a local ring. What is its maximal ideal? Now $(X) = \mathfrak{a}$ is a prime ideal of $k[X]$, so we can form $k[X]_{(X)}$. Prove that

$$k[X] \subseteq k[X]_{(X)} \subseteq k[[X]].$$

We have the (prime) ideal $(X)^e$ of $k[X]_{(X)}$. Form the completion of $k[X]_{(X)}$ with respect to the $(X)^e$-adic topology. What ring do you get?

Problem 75 If k is any field, write $A = k[[T_1, \ldots, T_n]]$ for the ring of formal power series over k in the indeterminates $T_1, \ldots, T_n$. Denote by $\mathrm{Aut}_k(A)$ the group of all k-automorphisms of A.

(1) Give necessary and sufficient conditions on the n power series $S_1(T_1, \ldots, T_n), \ldots, S_n(T_1, \ldots, T_n)$ in order that the map

$$\sigma \colon T_j \mapsto S_j(T_1, \ldots, T_n)$$

be an element of $\mathrm{Aut}_k(A)$. In so doing, describe the group $\mathrm{Aut}_k(A)$.

(2) If now k is no longer necessarily a field but merely a commutative ring with unity, answer question (1) for this case.

(3) Fix k, a commutative ring with unity, and consider the category, $\mathrm{Alg}(k)$, of k-algebras (say commutative). Define a functor $Aut(k[[T_1, \ldots, T_n]]/k)(-)$ by sending $B \in \mathrm{Alg}(k)$ to $\mathrm{Aut}_B(B[[T_1, \ldots, T_n]]) \in \mathrm{Grp}$. Is this functor representable? How?

Problem 76 Prove that in the category of commutative A-algebras, the tensor product is the coproduct:

$$B \otimes_A C \cong B \coprod_A C.$$

Which A-algebra is the product $B \prod_A C$ (in commutative A-algebras)?

Problem 77 Suppose A is a (commutative) semi-local ring obtained by localizing a f.g. $\mathbb{C}$-algebra with respect to a suitable multiplicative subset. Let J be the Jacobson radical of A and write $\widehat{A}$ for the J-adic completion of A. Is it true that every finitely generated $\widehat{A}$-module, M, has the form $M = M_0 \otimes_A \widehat{A}$ for some finitely generated A-module, M_0? Proof or counter-example.

Problem 78 Here A is a commutative ring and we write $M_n(A)$ for the ring of $n \times n$ matrices over A.

1. Prove: The following are equivalent
   (a) A is noetherian
   (b) For some n, $M_n(A)$ has the ACC on 2-sided ideals
   (c) For all n, $M_n(A)$ has the ACC on 2-sided ideals.
2. Is this still valid if "noetherian" is replaced by "artinian" and "ACC" by "DCC"? Proof or counterexample.
3. Can you make this quantitative? For example, suppose all ideals of A are generated by less than or equal to N elements. What can you say about an upper bound for the number of generators of the ideals of $M_n(A)$? How about the converse?

Problem 79 Refer to Problem 74. Write $k((X))$ for $\mathrm{Frac}(k[[X]])$.

1. Show that
$$k((X)) = \left\{ \sum_{j=-\infty}^{\infty} a_j X^j \mid a_j \in k \text{ and } (\exists\, N)(a_j = 0 \text{ if } j < N) \right\}$$
where on the right hand side we use the obvious addition and multiplication for such expressions. If $\xi \in k((X))$, write $\mathrm{ord}(\xi) = N \iff N =$ largest integer so that $a = 0$ when $j < N$; here, $\xi \neq 0$. If $\xi = 0$, set $\mathrm{ord}(\xi) = \infty$. One sees immediately that $k[[X]] = \big\{\xi \in k((X)) \mid \mathrm{ord}(\xi) \geq 0\big\}$.
2. Write $\mathcal{U}$ for $\mathbb{G}_m\big(k[[X]]\big)$ and $\mathcal{M}$ for $\{\xi \mid \mathrm{ord}(\xi) > 0\}$. Prove that $k((X)) = \mathcal{M}^{-1} \cup \mathcal{U} \cup \mathcal{M}$ (disjointly), where
$$\mathcal{M}^{-1} = \{\xi \mid 1/\xi \in \mathcal{M}\}.$$
Now fix a real number, c, with $0 < c < 1$. Define for $\xi, \eta \in k((X))$,
$$d(\xi, \eta) = c^{\mathrm{ord}(\xi - \eta)},$$
then it should be clear that $k((X))$ becomes a metric space and that addition and multiplication are continuous in the metric topology. Prove that $k((X))$ is complete in this topology (i.e., Cauchy sequences converge), and that the topology is independent of which number c is chosen (with $0 < c < 1$).
3. Suppose $u \in k[[X]]$, $u = \sum_{j=0}^{\infty} a_j X^j$, and $a_0 = 1$. Pick an integer $n \in \mathbb{Z}$ and assume $(n, \mathrm{char}(k)) = 1$. Prove: There exists $w \in k[[X]]$ such that $w^n = u$. There is a condition on k so that $k((X))$ is locally compact. What is it? Give the proof. As an example of limiting operations, prove
$$\frac{1}{1-x} = \sum_{j=0}^{\infty} X^j = \lim_{N\to\infty} (1 + X + \cdots + X^N).$$

4. Given $\displaystyle\sum_{j=-\infty}^{\infty} a_j X^j \in k((X))$, its derivative is defined formally as
$$\sum_{j=-\infty}^{\infty} j a_j X^{j-1} \in k((X)).$$
Assume $\mathrm{ch}(k) = 0$. Check mentally that $\alpha' = 0 \bigl(\alpha \in k((X))\bigr) \implies \alpha \in k$. Is the map $\alpha \mapsto \alpha'$ a *continuous* linear transformation $k((X)) \to k((X))$? Set $\eta = \displaystyle\sum_{j=0}^{\infty} \frac{1}{j!} X^j$, so $\eta \in k((X))$. Prove that X and η are independent transcendentals over k.

5. A topological ring is one where addition and multiplication are continuous and we have a Hausdorff topology. Topological k-algebras (k has the discrete topology) form a category in which the morphisms are *continuous* k-algebra homomorphisms. An element λ in such a ring is *topologically nilpotent* iff $\lim_{n\to\infty} \lambda^n = 0$. Let $\mathcal{N}_{\mathrm{top}}$ denote the functor which associates to each topological k-algebra the set of its topological nilpotent elements. Prove that $\mathcal{N}_{\mathrm{top}}$ is representable. As an application, let
$$s(X) = \sum_{j=0}^{\infty} (-1)^j \frac{X^{2j+1}}{(2j+1)!}, \quad c(X) = \sum_{j=0}^{\infty} (-1)^j \frac{X^{2j}}{(2j)!}.$$
Then $s'(X) = c(X)$ and $c'(X) = -s(X)$, so $c^2(X)+s^2(X)$ lies in k (the constants). Without computing $c^2(X)+s^2(X)$, show it is 1. (You'll need $\mathcal{N}_{\mathrm{top}}$, so be careful.)

6. Show that even though $k(X)$ is dense in $k((X))$, the field $k((X))$ possesses infinitely many independent transcendental elements over $k(X)$. (Suggestion: Look in a number theory book under "Liouville Numbers"; mimic what you find there.)

7. Let $C_k\bigl(k((X))\bigr) = \bigl\{\alpha \in k((X)) \mid \alpha \text{ is algebraic over } k\bigr\}$. Show that $C_k\bigl(k((X))\bigr) = k$.
If $\mathrm{ch}(k) = 0$ and $\mathbb{R} \subseteq k$, write $\displaystyle\binom{m}{j} = \frac{m(m-1)\cdots(m-j+1)}{j(j-1)\cdots 3\cdot 2\cdot 1}$ for $m \in \mathbb{R}$. If $\mathbb{R} \not\subseteq k$, do this only for $m \in \mathbb{Q}$. Set
$$y_m = \sum_{j=0}^{\infty} \binom{m}{j} X^j \in k[[X]].$$
If $m \in \mathbb{Q}$ and $m = r/s$, prove that $y_m^s = (1+x)^r$.
Note that $y_m = 1 + O(X)$ and that $O(X) \in \mathcal{N}_{\mathrm{top}}\bigl(k[[X]]\bigr)$. Let $L(1+X) = \displaystyle\sum_{j=0}^{\infty} (-1)^j \frac{X^{j+1}}{(j+1)}$, and set $f(X)^m = \eta\bigl(m \cdot L(f(X))\bigr)$, where
$$\eta(X) = \sum_{j=0}^{\infty} \frac{1}{j!} X^j \quad \text{and} \quad f(X) = 1 + O(X), \text{ some } O(X)$$
and $m \in \mathbb{R}$ (here, $\mathbb{R} \subseteq k$). Show that
$$(1+X)^m = y_m.$$

Problem 80 Say K is a field, A is a subring of K. Write $k = \mathrm{Frac}\, A$.

1. If K is a finitely generated A-module, prove that $k = A$.

2. Suppose there exist finitely many elements $\alpha_1, \ldots, \alpha_m \in K$ *algebraic over* k such that
$$K = A[\alpha_1, \ldots, \alpha_m].$$

Prove $\big(\exists\, b \in A\big)\big(b \neq 0\big)\big($so that $k = A[1/b]\big)$. Prove, moreover, that b belongs to every maximal ideal of A.

Problem 81 Refer to Problem 69. Look at $\mathcal{P}(X, \mathcal{A}\mathrm{b})$. We know that the functor $F \rightsquigarrow F(U)$ taking $\mathcal{P}(X, \mathcal{A}\mathrm{b})$ to $\mathcal{A}\mathrm{b}$ is representable.

1. Grothendieck realized that when computing algebraic invariants of a "space" (say homology, cohomology, homotopy, K-groups, ...) the sheaf theory one needs to use could be done far more generally and with far more richness if one abstracted the notion of "topology". Here is the generalization:

   (a) Replace $\mathcal{T}_X$ by *any* category $\mathcal{T}$.

   To do sheaves, we need a notion of "covering":

   (b) We isolate for each $U \in \mathcal{O}\mathrm{b}\,\mathcal{T}$ some families of morphisms $\{U_\alpha \to U\}_\alpha$ and call each of these a "covering" of U. So we get a whole collection of families of morphisms called $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ *and we require*

   (i) Any isomorphism $\{V \to U\}$ is in $\mathcal{C}\mathrm{ov}\,\mathcal{T}$

   (ii) If $\{U_\alpha \to U\}_\alpha$ is in $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ and for all α, $\{V_\beta^{(\alpha)} \to U_\alpha\}_\beta$ is in $\mathcal{C}\mathrm{ov}\,\mathcal{T}$, then $\Big\{V_\beta^{(\alpha)} \to U\Big\}_{\alpha,\beta}$ is in $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ (*i.e.*, a covering of a covering is a covering).

   (iii) If $\{U_\alpha \to U\}_\alpha$ is in $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ and $V \to U$ is *arbitrary* then $U_\alpha \prod_U V$ exists in $\mathcal{T}$ *and*

   $$\Big\{U_\alpha \prod_U V \to V\Big\}_\alpha$$

   is in $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ (*i.e.*, the restriction of a covering to V is a covering of V; this allows the relative topology—it is the axiom with teeth).

   Intuition: A morphism $V \to U$ in $\mathcal{T}$ is an "open subset of U". N.B. The same V and U can give more than one "open subset" (vary the morphism) so the theory is very rich. In our original example: $\mathcal{T} = \mathcal{T}_X$; the family $\{U_\alpha \to U\}_\alpha$ is in $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ when and only when $\bigcup_\alpha U_\alpha = U$. Check the axioms (i), (ii) and (iii).
   Now a presheaf is just a cofunctor $\mathcal{T} \to \mathcal{S}\mathrm{ets}$ or $\mathcal{A}\mathrm{b}$, etc. and a sheaf is a presheaf for which

   $$F(U) \to \prod_\gamma F\big(U_\gamma\big) \underset{p_2}{\overset{p_1}{\rightrightarrows}} \prod_{\alpha,\beta} F\Big(U_\alpha \prod_U U_\beta\Big) \tag{S}$$

   is exact for *every* $U \in \mathcal{T}$ and *every* $\{U_\gamma \to U\}_\gamma$ in $\mathcal{C}\mathrm{ov}\,\mathcal{T}$. One calls the category $\mathcal{T}$ and its distinguished families $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ a *site* (topology used to be called "analysis situs").

   Given a category, say $\mathcal{T}$, assume $\mathcal{T}$ has finite fibred products. A family of morphisms $\{U_\alpha \to U\}_\alpha$ in $\mathcal{T}$ is called a family of *universal, effective epimorphisms* iff

   (a) $\forall Z \in \mathcal{O}\mathrm{b}\,\mathcal{T}$

   $$\mathrm{Hom}(U, Z) \to \prod_\gamma \mathrm{Hom}\big(U_\gamma, Z\big) \rightrightarrows \prod_{\alpha,\beta} \mathrm{Hom}\big(U_\alpha \prod_U U_\beta, Z\big)$$

   is exact (in $\mathcal{S}\mathrm{ets}$) AND

   (b) The same for $\Big\{U_\alpha \prod_U V \to V\Big\}_\alpha$ *vis a vis* all Z as in (a). (Condition (b) expresses universality, and (a) expresses effectivity of epimorphisms.)

   Decree that $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ is to consist of families of universal, effective epimorphisms. Show that $\mathcal{T}$ with this $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ is a site—it is called the *canonical site on* $\mathcal{T}$, denoted $\mathcal{T}_{\mathrm{can}}$.

2. For $\mathcal{T}_{\mathrm{can}}$, every representable cofunctor on $\mathcal{T}$ is a sheaf (give the *easy* proof). Note that if $\mathcal{T} \subseteq \widetilde{\mathcal{T}}$ where $\widetilde{\mathcal{T}}$ is a bigger category, and if $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ lies in the universal, effective epimorphisms for $\widetilde{\mathcal{T}}$, then any cofunctor on $\mathcal{T}$, *representable in* $\widetilde{\mathcal{T}}$, is a sheaf on $\mathcal{T}_{\mathrm{can}}$. For example, prove that if $\widetilde{\mathcal{T}}$ is all topological spaces and $\mathcal{T}_X$ is our beginning category of Problem 69, then $\mathcal{T}_X \subseteq \widetilde{\mathcal{T}}$ and prove that open coverings in $\mathcal{T}_X$ (as in Problem 69) *are* universal, effective epimorphisms in $\widetilde{\mathcal{T}}$. Hence, for ANY topological space, Y, $U \rightsquigarrow \mathrm{Hom}_{\mathrm{top.spaces}}(U, Y)$ *is a sheaf* on $\mathcal{T}_X$.

3. Let $\mathcal{T} = \mathcal{S}\mathrm{ets}$ and let $\{U_\alpha \to U\}_\alpha$ be in $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ when $\bigcup_\alpha(\text{Images of } U_\alpha) = U$. Prove that the sheaves on $\mathcal{T}$ with values in $\mathcal{S}\mathrm{ets}$ are exactly the representable cofunctors on $\mathcal{T}$.

4. Generalize (3): If G is a given group, let $\mathcal{T}_G$ be the category of sets with a G-action. Make $(\mathcal{T}_G)_{\mathrm{can}}$ the canonical site on $\mathcal{T}_G$. Prove: Coverings are families $\{U_\alpha \to U\}_\alpha$ so that $\bigcup_\alpha(\mathrm{Im}\ U_\alpha) = U$ (all are G-sets, morphisms are G-morphisms). Once again, prove: The sheaves on $(\mathcal{T}_G)_{\mathrm{can}}$ are exactly the representable cofunctors on $\mathcal{T}_G$. Prove further: The sheaves on $(\mathcal{T}_G)_{\mathrm{can}}$ with values in $\mathcal{A}\mathrm{b}$ form a category equivalent to the category of G-modules; namely the equivalence is given by taking a sheaf to its representing object, a G-module.

Problem 82 Consider the two rings $A = \mathbb{R}[T]$ and $B = \mathbb{C}[T]$. Show that $\mathrm{Max}(B)$ is in one-to-one correspondence with the points of the complex plane while $\mathrm{Max}(A)$ is in one-to-one correspondence with the closed upper half plane: $\{\xi \in \mathbb{C} \mid \mathrm{Im}(\xi) \geq 0\}$. Since A is a PID (so is B) we can characterize an ideal by its generator. In these terms, which ideals of $\mathrm{Max}(A)$ correspond to points in $\mathrm{Im}(\xi) > 0$, which to points on the real line? What about $\mathrm{Spec}\,B$ and $\mathrm{Spec}\,A$?

Problem 83 Suppose that $f(X, Y)$ and $g(X, Y)$ are two irreducible polynomials with complex coefficients. Assume neither is a scalar multiple of the other. Show that the set

$$S = \{(\alpha, \beta) \in \mathbb{C}^2 \mid f(\alpha, \beta) = g(\alpha, \beta) = 0\}$$

is finite. (There are many ways of doing this; try to pick a way that is as elementary as possible.)

Problem 84 When X is compact Hausdorff and $A = \mathbb{C}(X)$, we identified X and $\mathrm{Max}(A)$ in the text *via* $x \mapsto \mathfrak{m}_x$. Now $\mathrm{Max}(A)$ has the induced topology from $\mathrm{Spec}\,A$.

1. Show the induced topology on $\mathrm{Max}(A)$ is compact Hausdorff by proving $x \mapsto \mathfrak{m}_x$ is a homeomorphism.

2. Prove all finitely generated ideals of A are principal but that no maximal ideal is finitely generated.

Problem 85

1. Given $A \to B$ a homomorphism prove that B is faithfully flat over A iff B is flat over A and the map $\mathrm{Spec}\,B \to \mathrm{Spec}\,A$ is surjective.

2. Say $A \to B$ is a homomorphism and B is faithfully flat over A. Assume A is noetherian. Show that the topology on $\mathrm{Spec}\,A$ is the quotient topology from $\mathrm{Spec}\,B$.

Problem 86 Here A is a commutative ring, but *not necessarily with unity.* Let $A^{\#}$ denote $A \prod \mathbb{Z}$ (category of sets) with addition componentwise and multiplication given by

$$\langle a, n\rangle\langle b, q\rangle = \langle ab + nb + qa, nq\rangle.$$

1. Clearly, $A^{\#}$ is a commutative ring with unity $\langle 0, 1\rangle$. A is a subring of $A^{\#}$, even an ideal. Suppose A has the ACC on ideals, prove that $A^{\#}$ does, too. Can you make this quantitative as in Problem 78 part (3)?

2. If you know all the prime ideals of A, can you find all the prime ideals of $A^{\#}$?

Problem 87 Let B, C be commutative A-algebras, where A is also commutative. Write D for the A-algebra $B \otimes_A C$.

1. Give an example to show that $\operatorname{Spec} D$ is not $\operatorname{Spec} B \underset{\operatorname{Spec} A}{\times} \operatorname{Spec} C$ (category of sets over $\operatorname{Spec} A$).
2. We have A-algebra maps $B \to D$ and $C \to D$ and so we get maps $\operatorname{Spec} D \to \operatorname{Spec} B$ and $\operatorname{Spec} D \to \operatorname{Spec} C$ (even maps over $\operatorname{Spec} A$), and these are maps of topological spaces (over $\operatorname{Spec} A$). Hence, we do get a map
$$\theta : \operatorname{Spec} D \to \operatorname{Spec} B \underset{\operatorname{Spec} A}{\Pi} \operatorname{Spec} C \quad \text{(top. spaces)}.$$
Show there are closed sets in $\operatorname{Spec} D$ *not* of the form $\theta^{-1}(Q)$, where Q is a closed set in the product topology of $\operatorname{Spec} B \underset{\operatorname{Spec} A}{\Pi} \operatorname{Spec} C$.

Problem 88 Let $A = \mathbb{Z}[T]$, we are interested in $\operatorname{Spec} A$.

1. If $\mathfrak{p} \in \operatorname{Spec} A$, prove that $\operatorname{ht}(\mathfrak{p}) \leq 2$.
2. If $\{\mathfrak{p}\}$ is closed in $\operatorname{Spec} A$, show that $\operatorname{ht}(\mathfrak{p}) = 2$. Is the converse true?
3. We have the map $\mathbb{Z} \hookrightarrow \mathbb{Z}[T] = A$, hence the continuous map $\operatorname{Spec} A \xrightarrow{\pi} \operatorname{Spec} \mathbb{Z}$. Pick a prime number, say p, of $\mathbb{Z}$. Describe $\pi^{-1}(p)$, is it closed?
4. When exactly is a $\mathfrak{p} \in \operatorname{Spec} A$ the generic point (point whose closure is everything) of $\pi^{-1}(p)$ for some prime number p?
5. Describe exactly those $\mathfrak{p} \in \operatorname{Spec} A$ whose image, $\pi(\mathfrak{p})$, is dense in $\operatorname{Spec} \mathbb{Z}$. What is $\operatorname{ht}(\mathfrak{p})$ in these cases?
6. Is there a $\mathfrak{p} \in \operatorname{Spec} A$ so that the closure of $\{\mathfrak{p}\}$ is all of $\operatorname{Spec} A$? What is $\operatorname{ht}(\mathfrak{p})$?
7. For a general commutative ring, B, if $\mathfrak{p}$ and $\mathfrak{q}$ are elements of $\operatorname{Spec} B$ and if $\mathfrak{q} \in \overline{\{\mathfrak{p}\}}$ show that $\operatorname{ht}(\mathfrak{q}) \geq \operatorname{ht}(\mathfrak{p})$ (assuming finite height). If $\mathfrak{p}$, $\mathfrak{q}$ are as just given and $\operatorname{ht}(\mathfrak{q}) = \operatorname{ht}(\mathfrak{p})$ is $\mathfrak{q}$ necessarily $\mathfrak{p}$? Prove that the following are equivalent:
   (a) $\operatorname{Spec} B$ is *irreducible* (that is, it is *not* the union of two properly contained closed subsets)
   (b) $(\exists\, \mathfrak{p} \in \operatorname{Spec} B)(\text{closure of } \{\mathfrak{p}\} = \operatorname{Spec} B)$
   (c) $(\exists$ *unique* $\mathfrak{p} \in \operatorname{Spec} B)(\text{closure of } \{\mathfrak{p}\} = \operatorname{Spec} B)$
   (d) $\mathcal{N}(B) \in \operatorname{Spec} B$. (Here, $\mathcal{N}(B)$ is the nilradical of B)
8. Draw a picture of $\operatorname{Spec} \mathbb{Z}[T]$ as a kind of plane over the "line" $\operatorname{Spec} \mathbb{Z}$ and exhibit in your picture all the different kinds of $\mathfrak{p} \in \operatorname{Spec} \mathbb{Z}[T]$.

Problem 89 If A is a commutative ring, we can view $f \in A$ as a "function" on the topological space $\operatorname{Spec} A$ as follows: for each $\mathfrak{p}$ in $\operatorname{Spec} A$, as usual write $\kappa(\mathfrak{p})$ for $\operatorname{Frac}(A/\mathfrak{p})$ [note that $\kappa(\mathfrak{p}) = A_{\mathfrak{p}}/$its max. ideal] and set $f(\mathfrak{p}) =$ image of f in $A/\mathfrak{p}$ considered in $\kappa(\mathfrak{p})$. Thus, $f : \operatorname{Spec} A \to \bigcup_{\mathfrak{p} \in \operatorname{Spec} A} \kappa(\mathfrak{p})$. Observe that if $f \in \mathcal{N}(A)$, then $f(\mathfrak{p}) = 0$ all $\mathfrak{p}$, *yet f need not be zero as an element of A.*

1. Let $A = k[X_1, \ldots, X_n]$. There are fields, Ω, containing k so that
   (a) Ω has infinitely many transcendental elements independent of each other and of the X_j over k and
   (b) Ω is algebraically closed, i.e., all polynomials with coefficients in Ω have a root in Ω.

An example of this is when $k = \mathbb{Q}$ or some finite extension of $\mathbb{Q}$ and we take $\Omega = \mathbb{C}$. In any case, fix such an Ω. Establish a set-theoretic map $\Omega^n \to \operatorname{Spec} A$ so that $f \in A = k[X_1, \ldots, X_n]$ viewed in the usual way as a function on Ω^n agrees with f viewed as a function on $\operatorname{Spec} A$. We can topologize Ω^n as follows: Call a subset of Ω^n k-closed iff there are finitely many polynomials $f_1, \ldots, f_p$ from A so that the subset is exactly the set of common zeros of $f_1, \ldots, f_p$. This gives Ω^n the *k-topology* (an honest topology, as one checks). Show that your map $\Omega^n \to \operatorname{Spec} A$ is continuous between these topological spaces. Prove, further, that Ω^n maps *onto* $\operatorname{Spec} A$.

2. Show that Ω^n is irreducible in the k-topology. (Definition in 7(a) of Problem 88)

3. Define an equivalence relation on Ω^n: $\xi \sim \eta \iff$ each point lies in the closure (k-topological) of the other. Prove that $\Omega^n / \sim$ is homeomorphic to $\operatorname{Spec} A$ under your map.

Problem 90 (Continuation of Problem 89) Let A be an integral domain and write K for $\mathrm{Frac}(A)$. For each $\xi \in K$, we set

$$\mathrm{dom}(\xi) = \{\mathfrak{p} \in \operatorname{Spec} A \mid \xi \text{ can be written } \xi = a/b, \text{ with } a, b \in A \text{ and } b(\mathfrak{p}) \neq 0\}.$$

1. Show $\mathrm{dom}(\xi)$ is open in $\operatorname{Spec} A$.

2. If $A = \mathbb{R}[X,Y]/(X^2 + Y^2 - 1)$, set $\xi = (1-y)/x$ (where $x = \overline{X}$ and $y = \overline{Y}$). What is $\mathrm{dom}(\xi)$?

3. Set $A = \mathbb{C}[X,Y]/(Y^2 - X^2 - X^3)$ and let $\xi = y/x$. What is $\mathrm{dom}(\xi)$?

4. Note that as ideals of A (any commutative ring) are A-modules, we can ask if they are free or locally free. Check that the non-zero ideal, $\mathfrak{a}$, of A is free $\iff$ it is principal and $\big(\mathfrak{a} \to (0)\big) = (0)$. The second condition is automatic in a domain. Now look again at $A = \mathbb{R}[X,Y]/(X^2 + Y^2 - 1)$, you should see easily that this is a domain. Characterize as precisely as you can the elements $\mathfrak{m} \in \mathrm{Max}(A)$ which are free as A-modules. If there are other elements of $\mathrm{Max}(A)$, are these locally free? What is the complement of $\mathrm{Max}(A)$ in $\operatorname{Spec} A$? Prove that $A \otimes_{\mathbb{R}} \mathbb{C}$ is a PID.

5. Consider the descent question for PIDs: Given rings S and T with $S \to T$ a homomorphism, suppose A is an S-algebra and T is faithfully flat over S. If $A \otimes_S T$ is a PID, is A necessarily a PID?

6. Do part (5) where PID is replaced by UFD.

Problem 91 Let p be an odd prime number, set $m = 2p - 1$ and write $A = \mathbb{Z}[\sqrt{-m}] \cong \mathbb{Z}[T]/(T^2 + m)$. Assume m is square free.

1. Let $\mathfrak{a}$ be the ideal $(p, 1 + \sqrt{-m})$ of A. Prove that $\mathfrak{a}$ is not principal, yet that $\mathfrak{a}$, as a module, is locally free (necessarily of rank one). Prove further that A is *not* a UFD.

2. For $p = 3$ and 7, find all the ideals, $\mathfrak{a}$, which are not free, yet are locally free.

N.B. By results of the text you have non-free projectives here.

Problem 92 In this problem A is an integral domain and $K = \mathrm{Frac}(A)$.

1. Is it true that if $\mathfrak{p} \in \operatorname{Spec}\big(A[X]\big)$ and if $\mathfrak{p} \cap A = (0)$, then $\mathfrak{p}$ is a principal ideal? Proof or counterexample.

2. Say A is a UFD and $\eta \in K$, with $\eta \neq 0$. Write $\eta = a/b$, where a and b are relatively prime. Prove that $A[\eta] \cong A[X]/(bX - a)$. When is $A[\eta]$ a flat A-module?

3. If k is a field and $\xi \in k(X)$ is a non-constant rational function, write $\xi = f(X)/g(X)$ where f and g are relatively prime polynomials. Of course, $k(\xi)$ is a subfield of $k(X)$, so $k(X)$ is a $k(\xi)$ vector space (and a $k(\xi)$-algebra). Prove that $\dim_{k(\xi)}\big(k(X)\big) < \infty$ and compute this dimension in terms of f and g.

Problem 93 If A is a commutative ring and $B = A[[X_1, \dots, X_n]]$ denotes the ring of formal power series in the variables $X_1, \dots, X_n$ (the case $n = 1$ was discussed in Problem 79) over A:

1. Prove:
$$\begin{aligned} A \text{ is noetherian} &\iff B \text{ is noetherian} \\ A \text{ is an integral domain} &\iff B \text{ is an integral domain} \\ A \text{ is a local ring} &\iff B \text{ is a local ring.} \end{aligned}$$

2. Write $K((X_1, \dots, X_n))$ for $\operatorname{Frac} B$, where $K = \operatorname{Frac} A$ and A is a domain. Say $A = K = \mathbb{C}$, $n = 2$. Is $\mathbb{C}((X, Y))$ equal to $\mathbb{C}((X))((Y))$? If not, does one contain the other; which?

Problem 94 If A is a noetherian ring, write $X = \operatorname{Spec} A$ with the Zariski topology. Prove the following are equivalent:

1. X is T_1
2. X is T_2
3. X is discrete
4. X is finite and T_1.

Problem 95 Call a commutative ring *semi-local* iff it possesses just finitely many maximal ideals.

1. If $\mathfrak{p}_1, \dots, \mathfrak{p}_t \in \operatorname{Spec} A$ and $S = A - \bigcup_{j=1}^{t} \mathfrak{p}_j$, then $S^{-1}A$ is semi-local.
2. Say A is semi-local and $\mathfrak{m}_1, \dots, \mathfrak{m}_t$ are its maximal ideals. Show that the natural map of rings
$$A/\mathcal{J}(A) \to \prod_{i=1}^{t} A/\mathfrak{m}_i$$
is an isomorphism. (Here, $\mathcal{J}(A)$ is the Jacobson radical of A)
3. If A is semi-local, show $\operatorname{Pic}(A) = (0)$.

Problem 96 Let A be a domain. An element $a \in A$, not a unit, is called *irreducible* iff it is *not* the product $a = bc$ in which neither b nor c is a unit. The element a is a *prime* iff the principal ideal, Aa, is a prime ideal. Of course, prime $\Longrightarrow$ irreducible.

1. Assume A is noetherian, show each non-unit of A is a finite product of irreducible elements. (A need not be a domain for this.)
2. Prove that the factorization of (1) is unique (when it exists) iff every irreducible element of A is prime.
3. Say A is a UFD and S a multiplicative subset of A. Show that $S^{-1}A$ is a UFD. If A is locally a UFD is A a UFD?
4. Prove: If A is noetherian then A is a PID $\iff$ A is a UFD *and* $\dim A = 1$.
5. Assume A is just a domain. A *weight function*, w, *on* A is a function $A - \{0\} \to \mathbb{Z}_{\geq 0}$ so that
   (a) $a \mid b \implies w(a) \leq w(b)$, with equality $\iff$ $b \mid a$, too
   (b) If a and $b \in A$ and say $a \nmid b$ and $b \nmid a$, then $\exists\, p, q, r \in A$ so that $r = pa + qb$ and $w(r) < \min\{w(a), w(b)\}$.

   Prove: A domain is a PID $\iff$ it possesses a weight function. Can you characterize the fields among the PIDs by their weight functions?

Problem 97 Prove: A noetherian domain is a UFD iff each height 1 prime is principal.

Problem 98 Examples and Counterexamples:

1. Let $A = k[X, Y]$ with k a field; write $\mathfrak{m} = (X, Y)$. Show that $\mathfrak{q} = (X, Y^2)$ is $\mathfrak{m}$-primary, but $\mathfrak{q}$ is *not* a power of any prime ideal of A. Therefore, primary ideals need not be powers of prime ideals.

2. Let $A = k[X, Y, Z]/(XY - Z^2) = k[x, y, z]$. Write $\mathfrak{p}$ for the ideal (x, z) of A. Prove that $\mathfrak{p} \in \operatorname{Spec} A$, but $\mathfrak{p}^2$ is not primary. Hence, powers of non-maximal prime ideals need not be primary. What is the primary decomposition of $\mathfrak{p}^2$?

3. Say $A = k[X, Y]$ as in part (1) and write $\mathfrak{a} = (X^2, XY)$. Show that $\mathfrak{a}$ is *not* primary yet $\sqrt{\mathfrak{a}}$ is a prime ideal—which one? So, here a non-primary ideal has a prime radical. What is the primary decomposition of $\mathfrak{a}$?

4. If A is a UFD and p is a prime element of A, then $\mathfrak{q} = Ap^n$ is always primary. Conversely, show if $\mathfrak{q}$ is primary and $\sqrt{\mathfrak{q}} = Ap$, then $(\exists\, n \geq 1)(\mathfrak{q} = Ap^n)$. Compare with (3) above.

Problem 99 Assume A is a noetherian integral domain. The argument at the end of Theorem 3.56 shows that height one primes of A are elements of $\operatorname{Pic}(A)$ *if A is normal*.

(1) Use this remark to prove that in a normal (noetherian) domain, each isolated prime of a principal ideal has height one (special case of Krull's principal ideal theorem).

(2) Say A is a noetherian normal domain. Show that A is a UFD iff $\operatorname{Pic}(A) = (0)$.

Problem 100 A Little Number Theory.
Let $\mathbb{Q}$ be the rational numbers, and consider fields $k = \mathbb{Q}[X]/\big(f(X)\big)$ where $f(X)$ is an irreducible polynomial over $\mathbb{Q}$. (Each finite extension of $\mathbb{Q}$ has this form, by Chapter 4, Section 4.6.) Such a k will be called a "number field" and we write $\mathcal{O}_k$ for $\operatorname{Int}_k(\mathbb{Z})$.

1. Show $\mathcal{O}_k$ is a noetherian normal domain with $\dim \mathcal{O}_k = 1$.

2. If $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_k$, then $(\mathcal{O}_k)_{\mathfrak{p}}$ is a PID and $\mathcal{O}_k$ is a UFD iff $\operatorname{Pic}(\mathcal{O}_k) = (0)$ iff $\mathcal{O}_k$ is a PID.

3. Let k be the fields: $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(\zeta)$, where ζ is a primitive 7th root of 1. In each case, find $\mathcal{O}_k$ and compute $\operatorname{Pic}(\mathcal{O}_k)$. Make a table.

4. In $\mathbb{Q}(\sqrt{-3})$, look at $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$. Is $\mathbb{Z}[\sqrt{-3}] = \mathcal{O}_k$? If not, what is $\operatorname{Pic}\big(\mathbb{Z}[\sqrt{-3}]\big)$? Same question for $\mathbb{Z}[\sqrt{-5}]$.

5. Let A be a noetherian, normal domain of dimension 1, write $k = \operatorname{Frac} A$ (e.g., $\mathcal{O}_k = A$ by (1)). We examine submodules (for A) of k. Call one of these, M, a *fractional ideal* iff $(\exists\, b \in A)(b \neq 0)(bM \subseteq A)$. Prove that the following are equivalent for A-submodules of k:

   (a) M is a fractional ideal

   (b) M is a finitely generated A-module

   (c) M is a rank one projective A-module.

6. Under multiplication, MN, the fractional ideals form a group, denote it $\mathcal{I}(A)$. (MN goes over to $M \otimes_A N$ in $\operatorname{Pic}(A)$). Let $\mathcal{C}_A$ be the (localizing) category of finite length modules over A and write $\widetilde{K}(A)$ for the Grothendieck group, $K_0(\mathcal{C}_A)$, of $\mathcal{C}_A$. By the theory of associated primes, each M in $\mathcal{C}_A$ has a composition series
$$M = M_0 \supset M_1 \supset M_2 \supset \cdots \supset M_{n+1} = (0)$$
and
$$M_i/M_{i+1} \cong A/\mathfrak{p}_i \text{ for some } \mathfrak{p}_i \in \operatorname{Max}(A).$$

These $\mathfrak{p}_i$ are unique up to order and we set

$$\chi_A(M) = \prod_{i=0}^{n} \mathfrak{p}_i \in \mathcal{I}(A).$$

Prove that χ_A is an isomorphism (first prove homomorphism) of the abelian groups $\widetilde{K}(A) \xrightarrow{\sim} \mathcal{I}(A)$. What is the kernel of the map $\widetilde{K}(A) \to \operatorname{Pic}(A)$?

7. Lastly, assume A is actually a PID. Say $M = A^n$ is a free A-module of rank n and choose $u \in \operatorname{End}_A M$. Assume $\det(u) \neq 0$ and show
$$\det(u) \cdot A = \chi_A(\operatorname{coker} u).$$

Problem 101 More examples.

1. Let $A = k[X, Y, Z, W]/(XY - ZW)$, where k is a field and $\operatorname{char}(k) \neq 2$. By Problem 34; A is a normal domain. Compute $\operatorname{Pic}(A)$.
2. If $A = \mathbb{C}[t^3, t^7, t^8] \subseteq \mathbb{C}[t]$, compute $\operatorname{Pic}(A)$. If $A = \{f \in \mathbb{C}[T] \mid f'(0) = f''(0) \text{ and } f(1) = f(-1)\}$ compute $\operatorname{Pic}(A)$.
3. If $A = \mathbb{C}[X, Y, Z]/(X^2 + Y^2 + Z^2 - 1)$, show $\operatorname{Pic}(A) \neq (0)$.

Problem 102

1. Write $A = K[X, Y, Z]$, with K a field. Set $\mathfrak{a} = (X, Y)(X, Z)$. Find a primary decomposition of $\mathfrak{a}$.
2. Let $A = K[X, XY, Y^2, Y^3] \subseteq K[X, Y] = B$, here K is a field. Write $\mathfrak{p} = YB \cap A = (XY, Y^2, Y^3)$. Prove that $\mathfrak{p}^2 = (X^2Y^2, XY^3, Y^4, Y^5)$ and is not primary. Find a primary decomposition of $\mathfrak{p}^2$ involving (Y^2, Y^3). All ideals are ideals of A.

Problem 103

1. Say A is an integral domain. Prove
$$A = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} A_{\mathfrak{p}} = \bigcap_{\mathfrak{m} \in \operatorname{Max}(A)} A_{\mathfrak{m}}.$$
2. Now let A be a commutative ring and let $f(T)$ be a polynomial of degree d in $A[T]$. Prove that $A[T]/\big(f(T)\big)$ is an A-projective module of rank d iff the coefficient of T^d in $f(T)$ is a unit of A.

Problem 104 Write A for the polynomial ring $k[T_1, \ldots, T_N]$ in which k is a field and $B = A/\mathfrak{p}$ for some prime ideal, $\mathfrak{p}$, of A. Let the transcendence degree of B over k be d and assume $d \geq 1$. Now let $S_0, S_1, \ldots, S_m$ be further indeterminates independent of the $T_1, \ldots, T_N$, write K for the rational function field $k(S_0, \ldots, S_m)$ and L for $k(S_1, \ldots, S_m)$.

(1) For a polynomial $f \in L \otimes_k A$, write $\mathfrak{P}$ for the ideal of $K \otimes_k A$ generated by $\mathfrak{p}$ and the element $f - S_0$ and prove that $\text{tr.d.}_K (K \otimes_k A)/\mathfrak{P} \leq d - 1$.

(2) Assume further $m \leq N$ and consider the composed map

$$k[T_1, \ldots, T_m] \hookrightarrow A \longrightarrow B.$$

We assume the composed map is *injective* and further that the polynomial $f \in L \otimes_k A$ has the form

$$f = \sum_{j=1}^{m} S_j T_j + g(T_{m+1}, \ldots, T_N).$$

Prove that $\mathrm{tr.d.}_K (K \otimes_k A)/\mathfrak{P} = d - 1$.

(3) Under the hypotheses of (2), assume for each prime ideal, $\mathfrak{B}$, of B, the local ring, $B_{\mathfrak{B}}$, is regular. Write $C = (K \otimes_k A)/\mathfrak{P}$, and let $\mathfrak{q}$ be any element of $\operatorname{Spec} C$. Show that $C_{\mathfrak{q}}$ is regular.

(4) Revisit Problem 83 and give a quick proof.

Problem 105 Suppose k is a field (if necessary, assume $\mathrm{ch}(k) = 0$) and A and C are the following $n \times n$ matrices with entries from k:

$$A = \begin{pmatrix} a_0 & \cdot & \cdots & \cdot & a_{n-1} \\ a_{n-1} & a_0 & \cdots & \cdot & a_{n-2} \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ a_1 & a_2 & \cdots & a_{n-1} & a_0 \end{pmatrix}; \quad C = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Of course, $C^n = I$.

(1) In $\overline{k}$ find all the eigenvalues and eigenvectors of C.

(2) Find a polynomial, $f(X) \in k[X]$, so that $A = f(C)$.

(3) Compute the eigenvalues of A in $\overline{k}$ and show that the corresponding eigenvectors are those of C.

(4) Give a criterion for A to be invertible. Can you give a criterion (in the same spirit) for A to be diagonalizable?

Problem 106 A *discrete valuation*, ν, on a (commutative) ring A, is a function $\nu : A \to \mathbb{Z} \cup \{\infty\}$ satisfying

(a) $\nu(xy) = \nu(x) + \nu(y)$

(b) $\nu(x + y) \ge \min\{\nu(x), \nu(y)\}$, with equality if $\nu(x) \ne \nu(y)$

(c) $\nu(x) = \infty \iff x = 0$.

A pair (A, ν) where A a commutative ring and ν is a discrete valuation is called a *discrete valuation ring* (DVR). Prove the following are equivalent:

(1) A is a DVR

(2) A is a local PID

(3) A is a local, noetherian, normal domain of Krull dimension 1

(4) A is a local, noetherian, normal domain and $(\mathfrak{m}_A \to A)\big(= \{\xi \in \operatorname{Frac} A \mid \xi\mathfrak{m}_A \subseteq A\}\big) \ne A$. Here, $\mathfrak{m}_A$ is the maximal ideal of A.

Problem 107 Let A be a commutative ring with unity and assume A is semi-local (it possesses just finitely many maximal ideals). Write $\mathcal{J}$ for the Jacobson radical of A and give A its $\mathcal{J}$-adic topology.

1. Prove that A is noetherian iff each maximal ideal of A is finitely generated and each ideal is closed in the $\mathcal{J}$-adic topology.
2. Assume A is noetherian, then the map $A \to A_{\mathrm{red}}$ gives A_{red} its $\mathcal{J}$-adic topology. If A_{red} is complete prove that A is complete.

Problem 108

1. Let A be a local ring, give A its $\mathfrak{m}$-adic topology ($\mathfrak{m} = \mathfrak{m}_A$ is the maximal ieal of A) and assume A is complete. Given an A-algebra, B, suppose B is finitely generated as an $\widehat{A}$-module. Prove that B is a finite product of A-algebras each of which is a local ring. Give an example to show that some hypothesis like completness is necessary for the conclusion to be valid.

2. (Hensel) Again A is complete and local, assume $f(X) \in A[X]$ is a monic polynomial. Write $\overline{f(X)}$ for the image of f in $(A/\mathfrak{m})[X]$. If $\overline{f(X)}$ factors as $g(X)h(X)$ where g and h are relatively prime in $(A/\mathfrak{m})[X]$, show that f factors as $G(X)H(X)$ where $\overline{G(X)} = g(X)$; $\overline{H(X)} = h(X)$. What can you say about $\deg G$, $\deg H$ and uniqueness of this factorization? Compare parts (1) and (2).

Problem 109 In this problem, A is an integral domain and $k = \mathrm{Frac}\, A$. If ν and ω are two discrete valuations of k (cf. Problem 106), the functions ν and ω are defined on A and extended to k *via* $\nu(a/b) = \nu(a) - \nu(b)$, *etc.*), let's call ν, ω inequivalent iff one is not a constant multiple of the other. Write $\mathcal{S}$ for a set of *inequivalent* discrete valuations of k and say that A is *adapted to* $\mathcal{S}$ provided

$$A = \big\{x \in k \mid (\forall \nu \in \mathcal{S})(\nu(x) \geq 0)\big\}.$$

1. Prove the following are equivalent:

   (a) A is a Dedekind domain

   (b) ($\forall$ ideals, $\mathfrak{a}$, of A)$(\forall x, x \neq 0, x \in \mathfrak{a})(\exists\, y \in \mathfrak{a})(\mathfrak{a} = (x, y))$.

   (c) There is a family of discrete valuations of k, say $\mathcal{S}$, for which A is adapted to $\mathcal{S}$ and so that the following holds:

   $$(\forall \nu, \omega \in \mathcal{S})\big(\nu \neq \omega \implies (\exists\, a \in A)(\nu(a) \geq 1 \text{ and } \omega(a-1) \geq 1)\big).$$

2. *Vis a vis* part (1), describe a one-to-one correspondence $\mathcal{S} \leftrightarrow \mathrm{Max}(A)$.

3. Take $k = \mathbb{Q}$, consider all prime numbers p with $p \equiv 1 \pmod 4$, write $\mathrm{ord}_p(n)$ for the highest exponent, e, so that $p^e \mid n$. Then ord_p is a discrete valuation of $\mathbb{Q}$, and we set $\mathcal{S} = \big\{\mathrm{ord}_p \mid p \equiv 1 \pmod 4\big\}$. Illustrate (c) in part (1) above with this $\mathcal{S}$. What is A, in concrete terms? It is pretty clear now how to make many Dedekind domains.

4. Say A is a Dedekind domain and $\mathfrak{a}$, $\mathfrak{b}$ are two non-zero ideals of A. Show $\exists\, x \in k(= \mathrm{Frac}\, A)$, so that $\mathfrak{a} + x\mathfrak{b} = A$.

5. Again, let A be a Dedekind domain and let L be a *finite* subset of $\mathrm{Max}(A)$. Write
   $A^L = \bigcap\{A_{\mathfrak{p}} \mid \mathfrak{p} \notin L\}$, then $A \subseteq A^L$ and so $\mathbb{G}_m(A) \subseteq \mathbb{G}_m(A^L)$. Recall, $\mathbb{G}_m(B)$ is the group of units of the ring B. Prove that $\mathrm{Pic}(A)$ is a torsion group $\iff$ $\mathbb{G}_m(A^L)/\mathbb{G}_m(A)$ is a free abelian group of rank $\#(L)$ for every finite set, L, of $\mathrm{Max}(A)$.

Problem 110 (Suggested by A. Auel) Suppose that R is a P.I.D. and consider the functor

$$t\colon R\text{-mod} \rightsquigarrow R\text{-mod}$$

that assigns to each M its torsion submodule. Of course, t is left-exact; what are its right derived functors? If instead, R is just a domain but we assume the $R^p t$ are given as in your answer for the case of a P.I.D., must R be a P.I.D.? Proof or counter-example.

Problem 111 Here, k is a field and $A = k[X_\alpha]_{\alpha \in I}$. The index set, I, may possibly be infinite. Write $\mathfrak{m}$ for the ideal generated by all the X_α, $\alpha \in I$. Set $A_i = A/\mathfrak{m}^{i+1}$, so $A_0 = k$. These A_i form a left mapping system and we set

$$\widehat{A} = \varprojlim A_i$$

and, as usual, call $\widehat{A}$ the *completion of A in the $\mathfrak{m}$-adic topology.* Note that the kernel of $\widehat{A} \to A_j$ is the closure of $\mathfrak{m}^{j+1}$ in $\widehat{A}$.

1. Show that $\widehat{A}$ is canonically isomorphic to the ring of formal power series in the X_α in which only finitely many monomials of each degree occur.

2. Now let $I = \mathbb{N}$ (the counting numbers) and write $\widehat{\mathfrak{m}}$ for the closure of $\mathfrak{m}$ in $\widehat{A}$. By adapting Cantor's diagonal argument, prove that $\widehat{\mathfrak{m}}$ is *not* $\widehat{A}\mathfrak{m}$. Which is bigger?

3. (Bourbaki) Again, I as in (2). Let k be a finite field, prove the

   Lemma. If k is a finite field and $\lambda > 0$, $(\exists\, n_\lambda)(\forall n \geq n_\lambda)$, there is a *homogeneous* polynomial, $F_n \in k[n^2 \text{ variables}]$, so that $\deg F_n = n$ and F_n *cannot* be written as the sum of terms of degree n of *any* polynomial $P_1Q_1 + \cdots + P_\lambda Q_\lambda$, where P_j, Q_j are in $k[n^2 \text{ variables}]$ and have no constant term.

   Use the lemma to prove $(\widehat{m})^2 \neq (\widehat{\mathfrak{m}^2})$.

4. Use (2) and (3) to prove that $\widehat{A}$ is *not* complete in the $\widehat{\mathfrak{m}}$-adic topology.

5. All the pathology exhibited in (2), (3) and (4) arises as I is not finite; indeed, when I is finite, prove:

   (a) $\widehat{\mathfrak{m}}$ is $\widehat{A}\mathfrak{m}$;

   (b) $\widehat{\mathfrak{m}}^2 = (\widehat{\mathfrak{m}^2})$;

   (c) $\widehat{A}$ *is* complete in the $\widehat{\mathfrak{m}}$-adic topology.

Problem 112 Consider the category TOP (topological spaces and continuous maps) and T2TOP the full subcategory of Hausdorff topological spaces.

1. At first, use the ordinary Cartesian product in TOP, with the product topology. Denote this $Y \times Z$. Show that $Y \in \text{T2TOP} \iff$ the diagonal map $\Delta : Y \to Y \times Y$ is closed.

2. For $X, Y \in \text{T2TOP}$, recall that $X \xrightarrow{f} Y$ is called a *proper* map $\iff f^{-1}(\text{compact})$ is compact. (Of course, any map $f : X \to Y$ will be proper if X is compact.) Show that $f : X \to Y$ is proper iff $(\forall T \in \text{T2TOP})(f_T : X \underset{Y}{\times} T \to Y \underset{Y}{\times} T$ is a closed map.)

3. With (1) and (2) as background, look at another subcategory, AFF, of TOP: here A is a commutative ring, AFF consists of the topological spaces $\operatorname{Spec} B$, where B is an A-algebra. Maps in AFF are those coming from homomorphisms of A-algebras, viz: $B \to C$ gives $\operatorname{Spec} C \to \operatorname{Spec} B$. Define

   $$(\operatorname{Spec} B)\ \Pi\ (\operatorname{Spec} C) = \operatorname{Spec}(B \otimes_A C)$$

   and prove that AFF possesses products.

   NB:

   (a) The topology on $\operatorname{Spec} B\ \Pi\ \operatorname{Spec} C$ is *not* the product topology—it is stronger (more opens and closeds)

   (b) $\operatorname{Spec} B\ \Pi\ \operatorname{Spec} C \neq \operatorname{Spec} B \times \operatorname{Spec} C$ as sets.
   (Cf. Problem 87)

   Prove: The diagonal map $\Delta_Y : Y \to Y \underset{\operatorname{Spec} A}{\Pi} Y$ is closed ($Y = \operatorname{Spec} B$). This recaptures (1) in the non-Hausdorff setting of AFF.

4. Given $f : \operatorname{Spec} C \to \operatorname{Spec} B$ (arising from an A-algebra map $B \to C$) call f *proper* $\iff$

   (i) C is a finitely generated B-algebra and

   (ii) $(\forall T = \operatorname{Spec} D)(f_T : \operatorname{Spec} C \underset{\operatorname{Spec} A}{\Pi} \operatorname{Spec} D \to \operatorname{Spec} B \underset{\operatorname{Spec} A}{\Pi} \operatorname{Spec} D$ is a closed map.)

Prove: If C is integral over B, then f is proper. However, prove also, $\mathrm{Spec}\,\big(B[T]\big) \to \mathrm{Spec}\, B$ is *never* proper.

5. Say $A = \mathbb{C}$. For which A-algebras, B, is the map $\mathrm{Spec}\, B \to \mathrm{Spec}\, A$ proper?

Problem 113 Assume A is *noetherian* local, $\mathfrak{m}_A$ is its maximal ideal, and

$$\widehat{A} = \varprojlim_{n} A/\mathfrak{m}^{n+1} = \text{completion of } A \text{ in the } \mathfrak{m}\text{-adic topology.}$$

Let B, $\mathfrak{m}_B$ be another noetherian local ring and its maximal ideal. Assume $f : A \to B$ is a ring homomorphism and we *always assume* $f(\mathfrak{m}_A) \subseteq \mathfrak{m}_B$.

1. Prove: f gives rise to a homomorphism $\widehat{A} \xrightarrow{\widehat{f}} \widehat{B}$ (and $\mathfrak{m}_{\widehat{A}} \to \mathfrak{m}_{\widehat{B}}$).
2. Prove: $\widehat{f}$ is an isomorphism $\iff$
   (a) B is flat over A
   (b) $f(\mathfrak{m}_A) \cdot B = \mathfrak{m}_B$
   (c) $A/\mathfrak{m}_A \to B/\mathfrak{m}_B$ is an isomorphism.
3. Use (2) to give examples of B's that are finite A-modules, non-isomorphic to A, yet $\widehat{A}$ and $\widehat{B}$ are isomorphic.

Problem 114 Suppose that $f \in \mathbb{Z}[X]$ is a non-constant polynomial.

(1) Show there exists an $n \in \mathbb{Z}$ so that $f(n)$ is not a prime number.

(2) Consider the sequence $\{f(n)\}_{n=1}^{\infty}$ and write P for the set of primes dividing at least one term of this sequence. Show P is infinite.

Problem 115 If k is a field and $f \in k[T]$, suppose f has degree n and has n distinct roots $\alpha_1, \ldots, \alpha_n$ in some extension of k. Write $\Omega = k(\alpha_1, \ldots, \alpha_n)$ for the splitting field of f and further take $n+1$ independent indeterminates $X, u_1, \ldots, u_n$ over Ω. Let $\widetilde{k} = k(u_1, \ldots, u_n)$, write $\widetilde{\Omega}$ for $\widetilde{k}(\alpha_1, \ldots, \alpha_n)$ and let $\omega = \alpha_1 u_1 + \cdots + \alpha_n u_n \in \widetilde{\Omega}$. If σ is an *arbitrary permutation* of $\alpha_1, \ldots, \alpha_n$ set

$$\sigma\omega = \sigma(\alpha_1)u_1 + \cdots + \sigma(\alpha_n)u_n,$$

and finally set

$$h(X) = \prod_{\sigma \in \mathcal{S}_n} (X - \sigma\omega).$$

1. Show that $h(X)$ has coefficients in $k[u_1, \ldots, u_n]$.
2. Split $h(X)$ into irreducible factors in $\widetilde{k}[X]$; show all the factors have the same degree, r. (Hint: Natural Irrationalities). Moreover, prove if $\sigma\omega$ is a root of a given factor, the other roots of this factor are exactly the $\tau\sigma\omega$, with $\tau \in \mathfrak{g}(\Omega/k)$. Hence, prove that $r = \#\big(\mathfrak{g}(\Omega/k)\big)$.
3. Using (2), give a procedure for explicitly determining those permutations, $\sigma \in \mathfrak{S}_n$, which belong to $\mathfrak{g}(\Omega/k)$. Illustrate your procedure with the examples: $k = \mathbb{Q}$, $f = T^3 - 2$ and $f = T^4 + T^3 + T^2 + T + 1$.

Problem 116 Here k is a field and Ω is a finite normal extension of k. Prove that there exists a normal tower of fields

$$k = k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_n = \Omega$$

so that

(a) the first r of these extensions are separable and the set $\{\mathfrak{g}(k_i/k_{i-1}) \mid 1 \le i \le r\}$ is exactly the set of composition factors of $\mathfrak{g}(\Omega/k)$, and

(b) The last $n - r$ are each purely inseparable over the previous and k_j arises from k_{j-1} by adjunction of a root of $X^p - a_j$, with $a_j \in k_{j-1}$. (Here, $p = \mathrm{char}(k)$.)

Problem 117 Let $g_1, \dots, g_n$ be polynomials (one variable) with coefficients in $k = k_0, \dots, k_{n-1}$ respectively, and with k_j the splitting field for g_j. In this case, we say k_n *arises from the successive solution of a chain of equations* $g_1 = 0, g_2 = 0, \dots, g_n = 0$. If f is a polynomial, we say $f = 0$ *can be solved by means of an auxiliary chain,* $g_i = 0$*, of equations* $\iff$ k_n contains a splitting field for f. When the $g_i(X)$ have the special form $g_i(X) = X^{m_i} - a_i$, we say $f = 0$ may be solved by radicals.

1. Suppose $f = 0$ may be solved by means of the auxiliary chain $g_1 = 0, \dots, g_n = 0$. Let $\mathfrak{s}(G)$ denote the set of simple constituents (composition factors) of a given finite group, G. Prove that $\mathfrak{s}\big(\mathfrak{g}_k(f)\big) \subseteq \bigcup \mathfrak{s}\big(\mathfrak{g}_{k_{j-1}}(g_j)\big)$.

2. Prove "Galois' Theorem": If k is a field, $f \in k[X]$, and Ω is a splitting field for f over k, assume $\big(\mathrm{char}(k), [\Omega : k]\big) = 1$; then $f = 0$ is solvable by radicals $\iff$ $\mathfrak{g}_k(f)$ is a solvable group.

Problem 118 Here k is a field, α is a root of an irreducible polynomial, $f \in k[X]$.

1. Prove: α lies in a field extension, L, of k obtained by successive solution of a chain of *quadratic* equations $g_1 = 0, \dots, g_n = 0$ $\iff$ the degree of a splitting field for f over k is a power of 2.

2. Given a line in the plane, we conceive of the line as the real line and the plane as $\mathbb{C}$. *But*, no numbers are represented on the line. However, two points are indicated on the line; we take these as 0 and 1 and label them so. We are given a straight edge (*no markings on it*) and a pair of dividers (no scale on it either) which we can set to any length and which will hold that length. But, if we reset the dividers, the original setting cannot be recaptured if not marked on our plane as a pair of points "already constructed." We can use our implements to make any finite number of the following moves:

   (a) Set the dividers to a position corresponding to two points already constructed, make any arc or circle with the dividers where one leg is at a point already constructed. (A point is constructed iff it is the intersection of an arc and a line, an arc and an arc, a line and a line.)

   (b) Given any pair of previously constructed points use the straight edge to draw a line or segment of a line through these points.

   You should be able to see that from 0 and 1 we can construct $p/q \in \mathbb{Q}$ (all p, q) therefore it is legitimate to label $\mathbb{Q}$ on our real axis. Call a point $(x, y) \in \mathbb{C}$ constructible iff its real and imaginary parts are constructible; that is these numbers, constructed as lengths, can be obtained from $\mathbb{Q}$ by a finite number of moves (a) and (b). Show that $\alpha \in \mathbb{C}$ is constructible iff $\mathbb{Q}(\alpha)$ may be obtained from $\mathbb{Q}$ by the successive solution of a chain of quadratic equations.

3. Prove

   (a) The duplication of a cube by straight edge and dividers is impossible.

   (b) The trisection of an angle by straight edge and dividers is impossible (try $\pi/3$).

4. (Gauss) Prove that a regular n-gon is constructible by straight edge and dividers iff $n = 2^r p_1 p_2 \cdots p_t$, where r is non-negative and the p_j are distinct Fermat primes (cf. Problem 14).

Problem 119 What is wrong with the following argument?
Let k be a field, write $f(X) \in k[X]$, $\deg(f) = n$, and suppose f has n distinct roots $\alpha_1, \dots, \alpha_n$, in a suitable extension field L/k. Write Ω for the normal extension $k(\alpha_1, \dots, \alpha_n)$. An element, ω, of Ω has the form $\omega = g(\alpha_1, \dots, \alpha_n)$, where g is a polynomial in n variables with coefficients in k. Let σ be an arbitrary

permutation of the α_i, then σ maps $g(\alpha_1,\dots,\alpha_n)$ to $g(\alpha_1',\dots,\alpha_n')$ where $\alpha_j' = \sigma(\alpha_j)$. If $h(\alpha_1,\dots,\alpha_n)$ is another polynomial with coefficients in k, then $h(\alpha_1,\dots,\alpha_n) \mapsto h(\alpha_1',\dots,\alpha_n')$ by σ and we have

$$\begin{gathered} g(\alpha_1,\dots,\alpha_n) + h(\alpha_1,\dots,\alpha_n) \to g(\alpha_1',\dots,\alpha_n') + h(\alpha_1',\dots,\alpha_n') \\ g(\alpha_1,\dots,\alpha_n)h(\alpha_1,\dots,\alpha_n) \to g(\alpha_1',\dots,\alpha_n')h(\alpha_1',\dots,\alpha_n'). \end{gathered}$$

Thus, we have an automorphism of Ω and the elements of k remain fixed. So, the arbitrary permutation, σ, belongs to the group of k-automorphisms of Ω; hence, the latter group has order greater than or equal to $n!$. By Artin's Theorem, $[\Omega : k] \geq n!$. (Theorem 4.32)

Problem 120 If k is a field, $f \in k[X]$ a separable polynomial and Ω is a splitting field for f over k, write $\mathfrak{g} = \mathfrak{g}(\Omega/k)$ and consider $\mathfrak{g}$ as a subgroup of the permutation group on the roots of f. Show that $\mathfrak{g}$ is a transitive permutation group $\iff$ f is an irreducible polynomial over k. Use this to give a necessary condition that $\sigma \in \mathfrak{S}_n$ actually belongs to $\mathfrak{g}_k(f)$, for f an arbitrary separable polynomial of degree n over k. Illustrate your condition by finding the Galois groups over $\mathbb{Q}$ of the polynomials: $X^5 - 1$, $X^5 + X + 1$.

Problem 121 Here, K is a finite field of q elements and q is odd.

1. Let $\mathrm{sq} : K^* \to K^*$ be the homomorphism given by $\mathrm{sq}(x) = x^2$. Show that $\#\ker \mathrm{sq} = \#\operatorname{coker} \mathrm{sq} = 2$ and $\#\operatorname{Im} \mathrm{sq} = (q-1)/2$.
2. Prove:
$$(\forall x \in K^*)\left(x^{(q-1)/2} = \begin{cases} 1 & \text{if } x \text{ is a square in } K \\ -1 & \text{otherwise} \end{cases} \right)$$
3. If $K = \mathbb{F}_p$, then K contains a square root of -1 iff $p \equiv 1 \bmod 4$.
4. For any finite field, K, every element of K is a sum of squares. Is it true that each element of K is a sum of (at most) two squares?

Problem 122 If k is a field of characteristic zero and $f \in k[X]$ is a monic polynomial, factor f into monic irreducible polynomials in $k[X]$ and set
$$f = g_1 g_2^2 \cdots g_r^r$$
where g_j is the product of the distinct irreducible factors of f which divide f with exact exponent j. Prove that the g.c.d. of f and its, derivative, f', is

$$g_2 g_3^2 \cdots g_r^{r-1}.$$

Assume Euclid's algorithm for finding the g.c.d. of two polynomials. Show that $g_1,\dots,g_r$ may be determined constructively. If n is an integer, illustrate with

$$f(X) = X^n - 1 \in \mathbb{Q}[X].$$

Problem 123 If k is a field and f, g are non-constant polynomials in $k[X]$, with f irreducible, prove that the degree of every irreducible factor of $f\big(g(X)\big)$ in $k[X]$ is divisible by $\deg f$.

Problem 124 If k is a field, X is transcendental over k, and $f(X) \in k[X]$ is irreducible in $k[X]$, write $\alpha_1,\dots,\alpha_n$ for a full set of roots of f in a suitable extension field of k. If $\mathrm{char}(k) = 0$, prove that none of the differences $\alpha_i - \alpha_j$ $(i \neq j)$ can lie in k. Give a counterexample for $\mathrm{char}(k) = p > 0$ (*any* prime p).

Problem 125 Let $k \subseteq K$ be two fields of characteristic zero. Assume the following two statements:

(a) Every $f(X) \in k[X]$ of *odd* degree has a root in k

(b) $(\forall \alpha \in k)(X^2 - \alpha$ has a root in $K)$

1. Prove: Each non-constant polynomial $g \in k[X]$ has a root in K.

2. Assume as well that K/k is normal of finite degree. Prove that K is algebraically closed. (Suggestion: Use induction on ν where $\deg g = 2^\nu n_0$ (n_0 odd). If $r \in \mathbb{Z}$, set $\gamma_{ij}^{(r)} = \alpha_i + \alpha_j + r\alpha_i\alpha_j$, where $\alpha_1, \ldots, \alpha_n$ are the roots of g in some $\Omega \supseteq K$. Fix r, show there is a polynomial $h(X) \in k[X]$, so that the $\gamma_{ij}^{(r)}$ are roots of h; for all i, j. Show some $\gamma_{ij}^{(r)} \in K$; now vary r and find $r_1 \neq r_2$ so that $\gamma_{ij}^{(r_1)} \in K$, $\gamma_{ij}^{(r_2)} \in K$.)

3. Take $k = \mathbb{R}$ and $K = \mathbb{C}$. By elementary analysis, (a) and (b) hold. Deduce $\mathbb{C}$ is algebraically closed (Gauss' first proof).

Problem 126 Let $\mathbb{Q}$ be the rational numbers, $\mathbb{R}$ the real numbers , X a transcendental over $\mathbb{R}$ and suppose $f \in \mathbb{Q}[X]$ is a polynomial of degree 3 irreducible in $\mathbb{Q}[X]$ having three real roots α, β, γ. Show that if

$$k_0 = \mathbb{Q} \subseteq k_1 \subseteq k_2 \subseteq \cdots \subseteq k_m$$

is a finite chain of fields each obtained from the preceding one by adjunction of a *real* radical $\rho_j = \sqrt[n_j]{c_j}$ ($n_j \in \mathbb{Z}, n_j > 0, c_j \in k_{j-1}$), the field k_m *cannot* contain ANY of the roots, α, β, γ of f. (Suggestion: If wrong, show we may assume each n_j is prime, let k_j be the field with maximal j where f is still irreducible. If $\alpha \in k_{j+1}$ show $\rho_{j+1} \in k_j(\alpha)$.) This is the famous "casus irreducibilis" of the cubic equation $f = 0$: if the three roots are real, the equation cannot be solved by real radicals.

Problem 127 Here, f is an irreducible quartic polynomial with coefficients in k; assume f has four distinct roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ in some extension field of k. Write $\beta = \alpha_1\alpha_2 + \alpha_3\alpha_4$, $L = k(\beta)$, and let Ω be $k(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$.

1. Assume $\mathfrak{g}(\Omega/k)$ has full size, i.e., 24, find $\mathfrak{g}(\Omega/L)$.

2. Show that, in any case, β is the root of a cubic polynomial, h, with coefficients in k (Lagrange's "cubic resolvent" for f).

Problem 128 Let k be a field, $\mathrm{char}(k) \neq 2$, write K/k for an extension of degree 2 and L/K for an extension also of degree 2.

1. Show $\exists\, \alpha, \beta$ with $\alpha \in K$, in fact $K = k(\alpha)$, and $\alpha^2 = a \in k$ and $\beta \in L$, $\beta^2 = u + v\alpha$; $u, v \in k$ and $L = K(\beta)$. (All this is very easy).

2. Let Ω be a normal closure of k containing L. Show that $[\Omega : k]$ is 4 or 8. In the case $v = 0$ (part (1)), show $\Omega = k(\alpha, \beta) = L$ and that $\exists\, \sigma, \tau \in \mathfrak{g}(\Omega/k)$ so that $\sigma(\alpha) = -\alpha$, $\sigma(\beta) = \beta$, $\tau(\alpha) = \alpha$, $\tau(\beta) = -\beta$. Determine precisely the group $\mathfrak{g}(\Omega/k)$.

3. When $v \neq 0$, let β_1 be a conjugate, not equal to $\pm\beta$, of β. Prove $\Omega = k(\beta, \beta_1)$ and that $\exists\, \sigma \in \mathfrak{g}(\Omega/k)$ such that $\sigma(\beta) = \beta_1$ and $\sigma(\beta_1)$ is one of β or $-\beta$.

4. Show if $[\Omega : k] = 8$ we may assume in (3) that σ maps β_1 to $-\beta$. Prove σ is an element of order 4 and that $\exists\, \tau \in \mathfrak{g}(\Omega/k)$, of order 2, with $\tau^{-1}\sigma\tau = \sigma^{-1}$. Deduce that $\mathfrak{g}(\Omega/k) = \mathrm{Gp}\{\sigma, \tau\}$; which of the two non-abelian groups of order 8 is it?

5. Illustrate (1)-(4) with a discussion of $X^4 - a$ over $\mathbb{Q}$.

6. With the above notation, show that the normal closure of K is cyclic of degree 4 iff a can be written as the sum of two squares, $b^2 + c^2$, in k. (Hints: if Ω is the field above, show $\mathfrak{g}(\Omega/k)$ is cyclic, order 4, iff Ω contains exactly one subfield of degree 2 over k. Then $u^2 - av^2$ must equal aw^2 for some $w \in k$. Now show a is the sum of two squares. You may need to prove that if -1 is a square then every element of k is a sum of two squares in k; cf. Problem 121.) Investigate, from the above, which primes, $p \in \mathbb{Z}$, are the sum of two squares in $\mathbb{Z}$.

Problem 129 Suppose p is a prime number, let $\mathfrak{S}_p$ denote the symmetric group on p letters and write G for a transitive subgroup of $\mathfrak{S}_p$ (i.e., the p letters form an orbit for G).

(1) If G contains a transposition, we know (Problem 13) that $G = \mathfrak{S}_p$. Use this to show there exist extensions, K, of $\mathbb{Q}$ whose Galois group is $\mathfrak{S}_p$.

(2) Hilbert proved the following theorem:

Hilbert Irreducibility Theorem. If $f \in \mathbb{Q}[T_1, \ldots, T_r, Z_1, \ldots, Z_s]$, where the T's and Z's are all algebraically independent, and if f is irreducible, then there exist integers $a_1, \ldots, a_r$ so that substituting a_j for T_j ($j = 1, \ldots, r$), the resulting polynomial $\widetilde{f} \in \mathbb{Q}[Z_1, \ldots, Z_s]$ is still irreducible. (Actually, there are infinitely many choices for the a_js.)

Use Hilbert's theorem to exhibit $\mathfrak{S}_n$ as a Galois group over $\mathbb{Q}$.

(3) Now A_n is a subgroup of $\mathfrak{S}_n$; can you exhibit A_n as a Galois group over $\mathbb{Q}$? (There is an old open question: Is every finite group, G, the Galois group of some finite normal extension of $\mathbb{Q}$? If G is solvable, this is known (due to Shafarevich) and hard to prove. Many simple groups are known to be Galois groups over $\mathbb{Q}$.)

(4) Write $f(X) = X^5 + aX + 1$ with $a \in \mathbb{Z}$ and let Ω be the splitting field of f over $\mathbb{Q}$. Determine $\mathcal{G}(\Omega/\mathbb{Q})$.

Problem 130 *(Bourbaki)*

1. Say k is a field, $\mathrm{char}(k) = p > 2$; let $K = k(X, Y)$ where X and Y are independent transcendentals over k. Write $L = K(\theta)$, where θ is a root of
$$f(Z) = Z^{2p} + XZ^p + Y \in K[Z].$$
Show that L/K is inseparable yet does not contain any purely inseparable elements over K. (Suggestion: First show f is irreducible and say $\exists\, \beta \in L, \beta^p \in K, \beta \notin K$. Then prove f becomes reducible in $K(\beta)[Z]$ and that then $X^{1/p}$ and $Y^{1/p}$ would lie in L. Prove then that $[L : K] \geq p^2$.)

2. Find the Galois group $\mathfrak{g}(\Omega/K)$ where Ω is a normal closure of L/K.

3. Now just assume $\mathrm{char}(k) \neq 2$, write $K = k(X)$ in this case. Let σ, τ be the 2-torsion k-automorphisms of K given by $\sigma(X) = -X$; $\tau(X) = 1 - X$ (i.e., $\sigma\big(f(X)\big) = f(-X)$, etc.). Show the fixed field of σ is $k(X^2)$; that of τ is $k(X^2 - X)$. If $\mathrm{char}(k) = 0$, show that $\mathrm{Gp}\{\sigma, \tau\}$ is an infinite group and prove that $k = k(X^2) \cap k(X^2 - X)$.

4. Now assume again $\mathrm{char}(k) = p > 2$. Show in this case $k(X^2) \cap k(X^2 - X)$ is strictly bigger than k—determine it explicitly and find the degree
$$\big[k(X) : (k(X^2) \cap k(X^2 - X))\big].$$

5. What is the situation in (3) and (4) if $\mathrm{char}(k) = 2$?

Problem 131 (Various Galois groups). Determine the Galois groups of the following polynomials over the given fields:

1. $(X^2 - p_1) \cdots (X^2 - p_t)$ over $\mathbb{Q}$, where $p_1, \ldots, p_t$ are distinct prime numbers.

2. $X^4 - t$ over $\mathbb{R}(t)$.

3. $X^p - m$ over $\mathbb{Q}$, where p is a prime number and m is a square free integer. (Hint: Here, $\mathfrak{g}$ fits into a split exact sequence of groups
$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z}/p\mathbb{Z} \arrow[r] & \mathfrak{g} \arrow[r, shift left] & ? \arrow[l, dashed, shift left] \arrow[r] & 0.) \end{tikzcd}$$

4. $X^8 - 2$ over $\mathbb{Q}(\sqrt{2})$, over $\mathbb{Q}(i)$, over $\mathbb{Q}$. (Cf. Problem 128)

Problem 132 Show that $x^7 - 7x + 3$ has a simple group of order 168 as its Galois group over $\mathbb{Q}$. Can you be more precise as to which group this is?

Problem 133

1. Here K/k is a finite extension of fields. Show the following are equivalent:
   (a) K/k is separable
   (b) $K \otimes_k L$ is a product of fields (product in the category of rings) for *any* field L over k
   (c) $K \otimes_k \overline{k}$ is a product of fields
   (d) $K \otimes_k K$ is a product of fields.

2. Now assume K/k is also a normal extension, and let
$$K_{\mathrm{pi}} = \{\alpha \in K \mid \alpha \text{ is purely inseparable over } k\}.$$
For the map
$$\theta : K_{\mathrm{pi}} \otimes_k K_{\mathrm{pi}} \to K_{\mathrm{pi}} \ \textit{via}\ \theta(\xi \otimes \eta) = \xi\eta,$$
show that the kernel of θ is exactly the nilradical of $K_{\mathrm{pi}} \otimes_k K_{\mathrm{pi}}$.

3. Prove: If K/k is a finite normal extension, then $K \otimes_k K$ is an Artin ring with exactly $[K : k]_{\mathrm{s}}$ prime ideals. The residue fields of all its localizations at these prime ideals are each the same field, K. A necessary and sufficient condition that K/k be purely inseparable is that $K \otimes_k K$ be a local ring. (Hints: $K = K_{\mathrm{s}} \otimes_k K_{\mathrm{pi}}$ and the normal basis theorem.)

Problem 134 Throughout this problem, G is a finite group, k is a field, and $R = k[G]$. We further assume that $(\#(G), \mathrm{char}(k)) = 1$.

(1) If S is a k-algebra (not necessarily commutative) write $\mathrm{Fcn}(G, S)$ for the k-module of all functions from G to S under pointwise addition and k-multiplication.

For $f \in \mathrm{Fcn}(G, S)$, we set
$$\int_G f(\sigma)d\sigma = \frac{1}{\#(G)} \sum_{\sigma \in G} f(\sigma).$$

Further, write $f_\tau(\sigma) = f(\tau\sigma)$ and show that
$$\int_G f_\tau(\sigma)d\sigma = \int_G f(\tau\sigma)d\sigma = \int_G f(\sigma)d\sigma$$
as well as
$$\int_G 1d\sigma = 1.$$
(We can write this as $d(\tau\sigma) = d\sigma$ and refer to the above as the "left invariance of the integral". Of course, the integral is also right invariant as well as "inverse invariant" (i.e., $d(\sigma^{-1}) = d\sigma$.) The integral is also called a "mean" on G as it averages the values of the function f.

(2) If M is an R-module (i.e., a G-module which is also a k-vector space) and N is a sub-R-module of M, write π for any k-projection of M onto N. (So then, $M = \mathrm{Ker}\ \pi \amalg N$ *as k-spaces*.) Now $\pi \in \mathrm{End}_k(M)\,(= S)$, so we can form
$$T = \int_G (\sigma^{-1}\pi\sigma)d\sigma.$$

Prove that T is a G-invariant projection from M onto N and that

$$M = \mathrm{Ker}\, T \amalg N, \quad \textit{as } R\textit{-modules.}$$

Deduce

Maschke's Theorem (1898) *If G, R and k are as above with $(\#(G), \mathrm{char}(k)) = 1$, then R is semi-simple as k-algebra.*

(3) If M is a simple R-module, prove that M is finite-dimensional as a k-vector space. (R-modules are called (linear) *representation spaces for G* and the map $G \longrightarrow \mathrm{Aut}(M)$, making M a G-module, is called *a representation of G with space M*. The dimension of M (as k-space) is called the *degree* of the representation.) It is a known theorem of Wederburn that a simple k-algebra with the D.C.C. (on left ideals) is isomorphic (as k-algebra) to the $r \times r$ matrices over a division ring, D. If k is algebraically closed, prove that D is k itself. Now prove that

(a) For each finite group, G, and algebraically closed field, k, with $(\#(G), \mathrm{char}(k)) = 1$, the number of non-isomorphic simple $k[G]$-modules is finite,

and

(b) We have $g = f_1^2 + \cdots + f_t^2$, where f_j is the degree of the j^{th} simple R-module and $g = \#(G)$.

Problem 135 Say R is a not necessarily commutative ring but that R is noetherian (on the left).

(1) Given a f.g. R-module, M, show that $\mathrm{projdim}_R(M) \le d$ if and only if for all **finitely generated** R-modules, N, we have

$$\mathrm{Ext}_R^{d+1}(M, N) = (0).$$

(2) Does the same criterion work for non f.g. R-modules M?

Problem 136 (Yoneda) Here, R is a ring and M', M'' are R-modules.

(1) Consider exact sequences of the form

$$0 \longrightarrow M' \longrightarrow X_1 \longrightarrow X_2 \longrightarrow M'' \longrightarrow 0 \qquad (E_2)$$

where the X_i are R-modules. Call such "2-fold extensions of M'' by M'" and, on the model of ordinary extensions, define an equivalence relation on the 2-fold extensions. Prove that the equivalence classes so defined are in 1-1 correspondence with $\mathrm{Ext}_R^2(M'', M')$.

(2) Generalize part (1) to "n-fold extensions":

$$0 \longrightarrow M' \longrightarrow X_1 \longrightarrow \cdots \longrightarrow X_n \longrightarrow M'' \longrightarrow 0 \qquad (E_n)$$

including the 1-1 correspondence of the equivalence classes with $\mathrm{Ext}_R^n(M'', M')$.

(3) We know $\mathrm{Ext}_R^n(A, B)$ is a co-functor in A and a functor in the variable B. If $M' \longrightarrow \widetilde{M}'$ and if $\xi \in \mathrm{Ext}_R^n(M'', M')$ is represented by

$$0 \longrightarrow M' \longrightarrow X_1 \longrightarrow \cdots \longrightarrow X_n \longrightarrow M'' \longrightarrow 0,$$

describe explicitly an n-fold extension representing the image of ξ in $\mathrm{Ext}_R^n(M'', \widetilde{M}')$. Same question but for a morphism $M'' \longrightarrow \widetilde{M}''$ and an element $\widetilde{\xi} \in \mathrm{Ext}_R^n(\widetilde{M}'', M')$.

(4) $\mathrm{Ext}_R^n(-,-)$ is an abelian group, as we know. Start with $n = 1$ and describe, in terms of representing extensions,

$$0 \longrightarrow M' \longrightarrow X \longrightarrow M'' \longrightarrow 0,$$

the abelian group structure on $\mathrm{Ext}^n_R(M'', M')$. (Of course, you must show your explicit construction of the equivalence class of a sum of two extensions

$$0 \longrightarrow M' \longrightarrow X \longrightarrow M'' \longrightarrow 0 \tag{a}$$

$$0 \longrightarrow M' \longrightarrow Y \longrightarrow M'' \longrightarrow 0 \tag{b}$$

is independent of the choice of the representatives (a) and (b).) Continue with the general case of n-fold extensions.

(5) Say

$$0 \longrightarrow M' \longrightarrow X_1 \longrightarrow \cdots \longrightarrow X_r \longrightarrow Z \longrightarrow 0$$

and

$$0 \longrightarrow Z \longrightarrow Y_1 \longrightarrow \cdots \longrightarrow Y_s \longrightarrow M'' \longrightarrow 0$$

are an r-fold (resp. s-fold) extension of Z by M' (resp. of M'' by Z). We can splice these to obtain an $r+s$-fold extension of M'' by M':

$$0 \longrightarrow M' \longrightarrow X_1 \longrightarrow \cdots \longrightarrow X_r \longrightarrow Y_1 \longrightarrow \cdots \longrightarrow Y_s \longrightarrow M'' \longrightarrow 0.$$

Prove that this process respects the equivalence relation on extensions and therefore yields a map

$$\theta\colon \mathrm{Ext}^s_R(M'', Z) \prod \mathrm{Ext}^r_R(Z, M') \longrightarrow \mathrm{Ext}^{r+s}_R(M'', M').$$

Show that from an r-fold extension

$$0 \longrightarrow M' \longrightarrow X_1 \longrightarrow \cdots \longrightarrow X_r \longrightarrow Z \longrightarrow 0 \tag{E_r}$$

we obtain an "iterated connecting homomorphism"

$$\delta_r\colon \mathrm{Hom}_R(M', A) \longrightarrow \mathrm{Ext}^r_R(Z, A)$$

for any R-module, A. If we take $A = M'$ and compute $\delta_r(\mathrm{id}_{M'})$, we get an element $\chi(E_r)$ in $\mathrm{Ext}^r_R(Z, M')$. Prove that $\chi(E_r)$ depends only on the equivalence class of E_r and gives the 1-1 correspondence of part (2). Discuss the pairing θ in terms of these "characteristic classes", $\chi(E_r)$, of extensions.

(6) Show that θ is actually bi-additive, hence it is $\mathbb{Z}$-bilinear and therefore we get a map

$$\mathrm{Ext}^s_R(M'', Z) \otimes_{\mathbb{Z}} \mathrm{Ext}^r_R(Z, M') \longrightarrow \mathrm{Ext}^{r+s}_R(M'', M').$$

Take $M = Z = M''$, call the common value M. Then we can compute $\theta(\alpha, \beta)$ and $\theta(\beta, \alpha)$ for
$\alpha \in \mathrm{Ext}^r_R(M, M)$ and $\beta \in \mathrm{Ext}^s_R(M, M)$. Is θ commutative? Is θ graded commutative
($\theta(\alpha, \beta) = (-1)^{rs}\theta(\beta, \alpha)$)? Neither?

Problem 137 We take G to be a group and write R for $\mathbb{Z}[G]$.

(1) Recall from Chapter 5, Section 5.3, that there is an isomorphism

$$H^p(G, M) \cong \mathrm{Ext}^p_R(\mathbb{Z}, M)$$

for every $p \geq 0$. Here, M is a G-module (so, an R-module). When $p = 2$, the left hand group classifies group extensions

$$0 \longrightarrow M \longrightarrow \mathfrak{G} \longrightarrow G \longrightarrow 1 \tag{E}$$

up to equivalence, while the right hand side classifies 2-extensions (of R-modules)

$$0 \longrightarrow M \longrightarrow X_1 \longrightarrow X_2 \longrightarrow \mathbb{Z} \longrightarrow 0, \tag{$\mathcal{E}$}$$

again up to equivalence.

In terms of exact sequences and natural operations with them describe the 1-1 correspondence between sequences (E) and $(\mathcal{E})$.

(2) Again, with the G-action on M fixed, extensions (E) can be classified by equivalence classes of 2-cocycles of G with values in M. Given such a 2-cocycle, show how to construct, explicitly, a 2-extension $(\mathcal{E})$. Carry through the verification that cohomologous 2-cocycles yield equivalent 2-extensions.

(3) Transfer the Yoneda addition of 2-extensions from Problem 136 to the addition of group extensions—the so called Baer addition.

Problem 138

1. Let $A = k[X_1, \dots, X_n]/\big(f(X_1, \dots, X_n)\big)$, where k is a field. Assume, for each maximal ideal, $\mathfrak{p}$, of A, we have $(\operatorname{grad} f)(\mathfrak{p}) \neq 0$ (i.e., $(\forall\, \mathfrak{p})(\exists$ component of $\operatorname{grad} f$ not in $\mathfrak{p}$)). Show that $\operatorname{Der}_k(A, A)$ is a projective A-module.

2. Suppose now $A = k[X, Y]/(Y^2 - X^3)$, $\operatorname{char}(k) \neq 2, \neq 3$. Consider the linear map $A \amalg A \to A$ given by the matrix (X^2, Y); find generators for the kernel of this map.

3. In the situation of (2), show that $\operatorname{Der}_k(A, A)$ is *not* projective over A.

Problem 139 Suppose in a ring R (assumed commutative for simplicity) we have elements $f_1, \dots, f_r$. We let $\overrightarrow{f} = (f_1, \dots, f_r)$; prove that

$$K_\bullet(\overrightarrow{f}) \cong K_\bullet(\overrightarrow{f_1}) \otimes_R \cdots \otimes_R K_\bullet(\overrightarrow{f_r}),$$

where on the right hand side we mean the total complex.

Problem 140 For G a group and M a right G-module, let M be considered as a "trivial" (left) $\mathbb{Z}[G]$-module and consider the bar complex as in Section 5.3, Chapter 5 of the text with boundary map

$$\partial_n(m \otimes \sigma_1 \otimes \cdots \otimes \sigma_n) = m\sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n + \sum_{i=1}^{n-1} (-1)^i m \otimes \sigma_1 \otimes \cdots \otimes \sigma_i \sigma_{i+1} \otimes \cdots \otimes \sigma_n$$
$$+ (-1)^{n+1} m \otimes \sigma_1 \otimes \cdots \otimes \sigma_{n-1}.$$

Define

$$\widetilde{H}_n(G, M) = \operatorname{Ker} \partial_n / \operatorname{Im} \partial_{n+1}$$

and prove that $M \rightsquigarrow \{\widetilde{H}_\bullet(G, M)\}$ is a universal ∂-functor as stated in the text. Thus, complete, by elementary methods, the identification of group homology for (right) G-modules, M, and Hochschild homology for the ring $\mathbb{Z}[G]$ and the modules $\epsilon_* M$ (definition on page 283, top).

Problem 141 Suppose that G is a profinite group and that H is a closed subgroup of G.

(1) Show that $\mathrm{c.d}(H) \leq \mathrm{c.d}(G)$.

(2) If H is open in G (and hence automatically closed in G), can you strengthen the inequality of (1)?

(3) Suppose G is a *finite* group. Prove that

$$\mathrm{c.d}(G) = \begin{cases} 0 \\ \infty \end{cases}$$

and $\mathrm{c.d}(G) = 0$ when and only when $G = \{1\}$.

Problem 142 For simplicity, assume in this problem that A is a commutative ring. If $\overrightarrow{f} = (f_1, \ldots, f_r)$ and $\overrightarrow{g} = (g_1, \ldots, g_r)$ are two ordered sequences of elements of A, write $\overrightarrow{fg}$ for the sequence $(f_1g_1, \ldots, f_rg_r)$. Now, we have a map

$$\varphi_{\overrightarrow{g}} \colon K_\bullet(\overrightarrow{fg}) \longrightarrow K_\bullet(\overrightarrow{f})$$

induced by

$$\varphi_{\overrightarrow{g}}(\xi_1, \ldots, \xi_r) = (g_1\xi_1, \ldots, g_r\xi_r).$$

(1) Show that this map is a chain map.

(2) Write $\overrightarrow{f^p} = (f_1^p, \ldots, f_r^p)$, then, for $0 < s < t$, we get a map

$$\varphi_{\overrightarrow{f^{t-s}}} \colon K_\bullet(\overrightarrow{f^t}) \longrightarrow K_\bullet(\overrightarrow{f^s})$$

and hence

$$\varphi^\bullet_{\overrightarrow{f^{t-s}}}(M) \colon K^\bullet(\overrightarrow{f^s}, M) \longrightarrow K^\bullet(\overrightarrow{f^t}, M).$$

We set

$$C^\bullet((\overrightarrow{f}), M) = \varinjlim K^\bullet(\overrightarrow{f^t}, M)$$

(with respect to these maps) and further set

$$H^\bullet((\overrightarrow{f}), M) = H^\bullet(C^\bullet((\overrightarrow{f}), M)).$$

Prove that

$$H^\bullet((\overrightarrow{f}), M) = \varinjlim H^\bullet(\overrightarrow{f^t}, M).$$

(3) Now, fix $\overrightarrow{f}$ and for the given $\overrightarrow{g}$, define

$$E_g \colon K_\bullet(\overrightarrow{f}) \longrightarrow K_\bullet(\overrightarrow{f})$$

by the equation

$$(E_g)_\bullet(z) = \left(\sum_{j=1}^{r} g_j e_j\right) \wedge z; \quad \text{the } e_j \text{ are a base for } A^r.$$

Prove that

$$d \circ E_g + E_g \circ d = \left(\sum_{i=1}^{r} g_i f_i\right) \text{id} \quad \text{on } K_t(\overrightarrow{f}), \text{ all } t \geq 0.$$

Deduce the

Proposition *Suppose $f_1, \ldots, f_r$ generate the unit ideal of A, then for all A-modules, M, the complexes*

$$K_\bullet(\overrightarrow{f^t});\ K_\bullet(\overrightarrow{f^t}, M);\ K^\bullet(\overrightarrow{f^t}, M);\ C^\bullet((\overrightarrow{f^t}), M)$$

have trivial (co)homology in **all** *dimensions.*

(4) The homology and cohomology modules $H_0(\overrightarrow{f}, M)$, $H_r(\overrightarrow{f}, M)$, $H^0(\overrightarrow{f}, M)$, $H^r(\overrightarrow{f}, M)$ depend only on the ideal, $\mathfrak{A}$, generated by $f_1, \ldots, f_r$. Is it true that $H^\bullet((\overrightarrow{f}), M)$ depends only on $\mathfrak{A}$ as (3) suggests?

Problem 143 Give the proof of "Lemma C" (= Lemma 5.51 of the text) following the methods used for "Lemmas A & B".

Problem 144 If A is a P.I.D., prove that $\mathrm{gldim}(A) \leq 1$. Under what conditions does the strict inequality hold? You may wish to investigate first the relations between $\mathrm{gldim}(A)$ and $\mathrm{gldim}(A_{\mathfrak{p}})$ for a commutative (noetherian?) ring, A, and all its prime ideals, $\mathfrak{p}$. Is the inequality $\mathrm{gldim}(A) \leq 1$ still valid if A is just a principal ideal ring (not a domain)? If A is a Dedekind ring, what is $\mathrm{gldim}(A)$?

Problem 145

1. Prove the six conditions of Proposition 5.72 are indeed equivalent.
2. Prove that the ten conditions listed in Proposition 5.73 are equivalent.

Problem 146 Here, A is a commutative ring, $\mathfrak{A}$ is an ideal of A and M is an A-module.

1. Prove that the number of elements in a maximal M-regular sequence from $\mathfrak{A}$ is independent of the choice of these elements (from $\mathfrak{A}$). Thus, $\mathrm{depth}_{\mathfrak{A}}\, M$ is well-defined.
2. Reformulate Koszul's Proposition (our 5.68) in terms of $\mathfrak{A}$-depth.
3. If A and M are graded and $(f_1, \ldots, f_t) = \overrightarrow{f}$ is an M -regular sequence of *homogeneous* elements then any permutation of $(f_1, \ldots, f_t)$ is still an M-regular sequence.

Problem 147 (R. Brauer) Here, G is a group and T is a finite subgroup of order m. For $\sigma, \tau \in G$, we define

$$\sigma \sim \tau \Longleftrightarrow (\exists t \in T)(\sigma^{-i} t \tau^{i} \in T, \text{ all } i \in \mathbb{Z}).$$

1. Show that $\sim$ is an equivalence relation and that each equivalence class has m elements.
2. Say $\sigma \sim \tau$, prove there is an $x \in T$ so that $\tau^m = x^{-1}\sigma^m x$.
3. Let S be a subset of $Z(G)$; pick a suitable T as above and show: Given $n \in \mathbb{Z}$, either

$$\#(\{z \in G \mid z^n \in S\}) = \infty$$

   or this cardinality is divisible by $\mathrm{g.c.d}(n, m)$.

4. When $\#(G) = g < \infty$, show that the cardinality of the set in (3) is divisible by $\mathrm{g.c.d}(g, n)$.

Problem 148 If $F(r)$ is the free group of rank r, and if $\Gamma_n(F(r))$ is the n^{th} term in the lower central series for $F(r)$, prove that the group $G = F(r)/\Gamma_n(F(r))$ is torsion-free.

Problem 149 Suppose A is a commutative ring, write $\mathrm{GL}(A)$ for the group $\bigcup_{n=1}^{\infty} \mathrm{GL}(n, A)$ in which $\mathrm{GL}(n, A)$ is a subgroup of $\mathrm{GL}(n+1, A)$ by the map

$$\xi \mapsto \left(\begin{array}{c|c} \xi & 0 \\ \hline 0 & 1 \end{array}\right)$$

1. When $A = \mathbb{Z}$, consider elements of $\mathrm{GL}(n+1, \mathbb{Z})$ of the form

$$\left(\begin{array}{c|c} \begin{matrix} \\ I \\ \\ \end{matrix} & \begin{matrix} * \\ \vdots \\ * \end{matrix} \\ \hline \underbrace{0 \quad \cdots \quad 0}_{n} & * \end{array}\right) \begin{matrix} \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} n \\ \\ \end{matrix}$$

   and their transposes. Show these matrices generate $\mathrm{GL}(n+1, \mathbb{Z})$ (as a group).

2. Prove that for any $\alpha \in \mathrm{GL}(n, A)$, there exist elements $x, \beta \in \mathrm{GL}(A)$ with β of the form

$$\beta = \begin{array}{c} \left(\begin{array}{c|c} I & 0 \\ \hline 0 & * \end{array}\right) \begin{array}{l} \}\,n \\ \}\,r \end{array} \\ \begin{array}{cc} \underbrace{}_{n} & \underbrace{}_{r} \end{array} \end{array}$$

and $\alpha = x\beta x^{-1}$.

Problem 150 Let k be a field, $\mathrm{ch}(k) \neq 2$ and write F for any overfield of k. Denote by $V_n(F)$ the set of all *symmetric, nilpotent* $n \times n$ matrices, A, with *entries in* F and $\mathrm{rank}(A) = n - 1$.

1. In the ring of all $n \times n$ matrices over F, show that if a matrix commutes with A it must be a polynomial (coefficients in F) in A.

2. When $n = 2$ and $F = \mathbb{F}_p$, prove that $V_2(F)$ is non-empty when and only when $p \equiv 1 \pmod 4$.

3. If $n = 3$ and $p \equiv 1 \pmod 4$ then $V_3(\mathbb{F}_p) \neq \emptyset$. Show, moreover, that $V_3(\mathbb{F}_3) \neq \emptyset$.

4. Let $\mathbb{Z}_p$ denote the ring of p-adic integers with $p \neq 2$. Prove there is an $n \times n$ symmetric matrix, B, with entries in $\mathbb{Z}_p$ so that $B^n = pC$ iff $V_n(\mathbb{F}_p) \neq \emptyset$. (Here, C is an *invertible* $n \times n$ matrix with entries in $\mathbb{Z}_p$.)

5. As usual, write $\overline{F}$ for the algebraic closure of F and $O_n(\overline{F})$ for the group of orthogonal matrices for the standard diagonal form (entries in $\overline{F}$). If $D \in \mathrm{GL}(n, \overline{F})$, write $\mathrm{Cay}(D) = D^\top D$ (this is the *Cayley transform of* D) and show the map
$$D \mapsto \mathrm{Cay}(D)$$
is an isomorphism of the coset space $O_n(\overline{F})\backslash GL(n, \overline{F})$ with the set, $S_n(\overline{F})$, consisting of symmetric, invertible $n \times n$ matrices from $\overline{F}$. Is this true when F replaces $\overline{F}$?

6. Write N for the nilpotent matrix $(n \times n)$
$$N = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$
If S is a symmetric $n \times n$ matrix prove that $SN = N^\top S$ iff S has the form
$$S = \begin{pmatrix} s_n & s_{n-1} & \cdots & s_2 & s_1 \\ s_{n-1} & s_{n-2} & \cdots & s_1 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ s_2 & s_1 & \cdots & 0 & 0 \\ s_1 & 0 & \cdots & 0 & 0 \end{pmatrix}$$
and show further that S is invertible iff s_1 is a unit.

7. Say $p \neq 2$, prove that $V_n(\overline{\mathbb{F}_p}) \neq \emptyset$. Using only (5) and (6) above, determine how big an extension, K, of $\mathbb{F}_p$ you need to guarantee $V_n(K) \neq \emptyset$.

Problem 151 (Continuation of Problem 150) Here, $\mathrm{ch}(F) \neq 2$.

1. Prove $O_n(\overline{F})$ acts transitively on $V_n(\overline{F})$.

2. Show $V_n(\overline{F})$ is a principal homogeneous space (= a *torsor*) for the group $PO_n(\overline{F})$, which, by definition, is $O_n(\overline{F})/(\pm I)$.

3. If n is odd, show $V_n(\overline{F})$ is a torsor for $SO_n(\overline{F})$; while if n is even, prove $V_n(\overline{F})$ has two components.

Problem 152 (Sierpinski) Write $\pi(x)$ for the nunmber of prime integers less than or equal to the positive real number x. The Prime Number Theorem asserts that $\lim_{x\mapsto\infty} \pi(x)\Big/\left(\frac{x}{\log x}\right) = 1$. Call a rational number *special* if it has the form $\frac{p}{q}$ where p and q are prime integers. Prove that the special rational numbers are dense in the positive reals.

Problem 153 Suppose $(B_\alpha, \varphi_\alpha^\beta)$ is a right mapping system of Artinian rings. Write B for $\varinjlim B_\alpha$, and assume B is noetherian. Prove that B is Artinian. That is, B is Artinian iff it is noetherian.

Problem 154 Fix a commutative ring, R, and an R-module, E. Suppose A and B are submodules of E so that B is free (of rank r) and is a direct summand of E. Prove that for an integer $q \geq 0$, the following are equivalent:

(a) The map $\bigwedge^q A \longrightarrow \bigwedge^q (E/B)$ is zero.

(b) The map $\bigwedge^q ((A+B)/B) \longrightarrow \bigwedge^q (E/B)$ is zero.

(c) The map $\bigwedge^{q+r} (A+B) \longrightarrow \bigwedge^{q+r} E$ is zero.

Problem 155 Throughout this problem A, B, C are three subgroups of a group, G, and we assume $AB = BA$, $AC = CA$ and $C \subseteq B$.

1. Prove that $(B\colon C) = (AB\colon AC)/(A\cap B\colon A\cap C)$.

2. Suppose φ maps B onto a group B^* and write C^* for the image of C under φ. Prove that
$$(B\colon C) = (B^*\colon C^*)(\mathrm{Ker}\,\varphi\colon \mathrm{Ker}\,(\varphi \restriction C)).$$

3. Here, let φ and ψ be in $\mathrm{End}(G)$; assume $\varphi\psi$ and $\psi\varphi$ are each the trivial homomorphism. Let H be any subgroup of G stable under both φ and ψ. Show that
$$(G\colon H)(\mathrm{Ker}\,(\varphi \restriction H)\colon \mathrm{Im}(\psi \restriction H)) = (\varphi(G)\colon \varphi(H))(\psi(G)\colon \psi(H))(\mathrm{Ker}\,\varphi\colon \mathrm{Im}\,\psi).$$

4. Under the hypotheses of (3), if $(G\colon H) < \infty$, deduce *Herbrand's Lemma*:
$$(\mathrm{Ker}\,\varphi\colon \mathrm{Im}\,\psi)(\mathrm{Ker}\,(\psi \restriction H)\colon \varphi(H)) = (\mathrm{Ker}\,\psi\colon \mathrm{Im}\,\varphi)(\mathrm{Ker}\,(\varphi \restriction H)\colon \psi(H)).$$

Problem 156 Suppose A is a (commutative) local or semi-local ring. Recall that the (*strict*) *Henselization of* A, denoted A^h, is the right limit, $\varinjlim C$, in which C runs over the family of finitely presented *étale* A-algebras.

1. If B is a semi-local A-algebra (A also being semi-local) and if B is integral over A, prove that $B \otimes_A A^h$ is both semi-local and isomorphic to B^h.

2. Suppose A is local and Henselian (*i.e.* $A = A^h$), show that for every $\mathfrak{p} \in \mathrm{Spec}\, A$ the integral closure of $A/\mathfrak{p}$ in $\mathrm{Frac}(A/\mathfrak{p})$ is again a local ring.

Problem 157 (Eilenberg) Let R be the non-commutative polynomial ring in n variables, $T_1, \ldots, T_n$, over the field k; so, $R = k\langle T_1, \ldots, T_n\rangle$. If M is a two-sided R-module, then a *crossed homomorphism* from R to M is an R-module map $R \longrightarrow M$ so that
$$f(\xi\eta) = \xi f(\eta) + f(\xi)\eta.$$
(Also called a derivation).

1. Given elements $m_1, \dots, m_n$ from M, show that the assigment $T_j \mapsto m_j$ gives rise to a unique crossed homomorphism $R \longrightarrow M$. Here, there is no restriction on the m_j.

2. As in Section 5.3 of the text, consider the augmentation ideal, $\mathfrak{J}$, for the map $\partial_0 \colon R^e \to R$. Prove that $\mathfrak{J}$ is a free R^e-module on the base $T_j \otimes 1 - 1 \otimes T_j^{\mathrm{op}}$, $j = 1, 2, \dots, n$.

3. Deduce from (2) that $\dim_{R^e}(R) = 1$ $(n > 0)$ in contradistinction to the commutative case.

Problem 158 (Serre) Here, G is a group and it acts on a set, S.

1. Suppose G is finite and S is finite. Write χ for the function on G to $\mathbb{C}$ given by

$$\chi(\sigma) = \#\,\text{of fixed points of } \sigma \text{ on } S.$$

Prove *Burnside's Lemma*: The number of orbits of G acting on S equals $\int \chi(\sigma)d\sigma$ (cf. Problem 134 for notation). (Suggestions. Show it suffices to give the proof when S *is* an orbit. In this case write

$$\int \chi(\sigma)d\sigma = \int \Big(\sum_{x \in S^\sigma} 1\Big) d\sigma = \sum_{s \in S} \int_{G_x} 1 d\sigma,$$

where $G_x = \{\sigma \in G \mid \sigma x = x\}$.)

2. Apply part (1) to the set $S \prod S$ with its G-action to see that $\chi^2(\sigma)$ counts the fixed points of σ on $S \prod S$. Prove: $\int \chi^2(\sigma)d\sigma \geq 2$.

3. Write $G_0 = \{\sigma \in G \mid \chi(\sigma) = 0\}$ = the σ's of G having no fixed points. Set $n = \#(S)$ and prove

$$\int_{G - G_0} (\chi(\sigma) - 1)(\chi(\sigma) - n) d\sigma \leq 0.$$

Next assume $n \geq 2$ and G acts transitively on S. Prove that

$$\int_G (\chi(\sigma) - 1)(\chi(\sigma) - n) d\sigma \geq 1$$

and evaluate $\int_{G_0} (\chi(\sigma) - 1)(\chi(\sigma) - n) d\sigma$. Put all together to prove the

Cameron-Cohen Inequality: If $n \geq 2$ and S is a G-orbit then

$$\frac{\#(G_0)}{\#(G)} \geq \frac{1}{n}.$$

Deduce *Jordan's Theorem*: If G acts on S transitively and $\#(S) \geq 2$, then there is a $\sigma \in G$ having no fixed point on S.

Problem 159 (Kaplansky) R is a ring and we are interested in "big" R-modules, i.e., those generated by more than $\aleph_0$ generators. For this reason, modules finitely or countably generated will be called "atoms" and we use the locution "finite atom" for a f.g. module.

1. Suppose M is an R-module that is a coproduct of (an arbitrary number of) atoms, say $M = \coprod M_i$. Suppose further P is a direct summand of M; that is,

$$M = P \amalg Q \qquad \text{(some } Q\text{)}$$

Prove there exists a well-ordered increasing family $\{S_\alpha\}_{\alpha \text{ an ordinal}}$ of submodules of M having the following properties:

(a) Each S_α is a coproduct of some of the M_i

(b) Each S_α splits as $(S_\alpha \cap P) \coprod (S_\alpha \cap Q)$

(c) If α is a limit ordinal, then $S_\alpha = \bigcup_{\beta<\alpha} S_\beta$

(d) $S_{\alpha+1}/S_\alpha$ is an atom.

(Hints: We use transfinite induction. By (c) we know how to proceed at a limit ordinal, check properties (a) and (b). The only point is to construct $S_{\alpha+1}$ from S_α. One of the M_i is not contained in S_α, call it M^*. Write the generators of the atom M^* as

$$x_{11}\, x_{12}\, x_{13}\, x_{14}\, \cdots$$

Begin with x_{11} and split it into its P and Q components giving us two new elements of M. Show only finitely many M_i's appear in the coproduct decomposition of these new elements; so, if we take $\coprod\{M_i \mid M_i \text{ appears}\}$ we get an atom. Write its generators as a second row of the infinite matrix being constructed. Repeat for x_{12} and get the third row $x_{31}\, x_{32}\, \cdots$. Now just as in the counting of $\mathbb{Q}$ take the elements in "diagonal order": $x_{11}, x_{12}, x_{21}, x_{13}, x_{22}, x_{31}, \cdots$ and keep repeating. Show that

$$S_{\alpha+1} = \text{module generated by } S_\alpha \text{ and all } x_{ij}$$

has (a) and (b) ((d) is obvious).)

2. Write $P_\alpha = P \cap S_\alpha$, show P_α is a direct summand of $P_{\alpha+1}$, that $P_\alpha = \bigcup_{\beta<\alpha} P_\beta$ (when α is a limit ordinal) and that $P_{\alpha+1}/P_\alpha$ is an atom. Finally, deduce P is a coproduct of atoms and so prove

Kaplansky's Theorem. Every direct summand of a module which is a coproduct of atoms is itself a coproduct of atoms. Every projective R-module is a coproduct of atoms.