EXERCISE SHEET, MATH 570-571, FALL 2011 AND WINTER 2012

First assignment (due Wednesday, January 25). Solve questions (55)-(62), but in question (57) do only the first 3 rings. In my experience, (58) is tricky, though eventually elementary. Make sure to use the Chinese Remainder Theorem, and more than once! Remember that solutions must be typed, except for matrices and diagrams that you can insert by hand, if you wish.

Second assignment (due Monday, February 27). Solve questions 66 (any 2 of the four parts), 68, 69, 71, 74, 77, 78 79.

Third assignment (due Friday, March 23). Do exercise 80 - 89, but submit ONLY 81, 82, 83, 85, 89.

Fourth assignment (due Monday, March 26). Do exercises 90, 92, 96, 97.

Fifth assignment (due Friday, April 13). Do exercises 98, 103, 104, 105, 110, 117. (Questions 103 and 110 are more challenging than the rest, I think.)

(1) Prove the Cauchy-Frobenius formula (also known as Burnside's lemma). Let G be a finite group acting on a finite non-empty set S. Let N be the number of orbits of G in S. Then

$$N = \frac{1}{\sharp G} \sum_{g \in G} Fix(g),$$

where $Fix(g) = \sharp\{s \in S : gs = s\}$. (Hint: define a function $I(g, s)$ on $G \times S$ such that $I(g, s) = 1$ is $gs = s$ and otherwise 0. Express the sum in the formula using this function and switch the order of summation.)

(2) Let S be a finite set with $|S| > 1$ on which a finite group G acts. Assume that the action of G is transitive, i.e., there is only one orbit. Prove that there is an element in G with no fixed points.

(3) Consider a rectangular board consisting of 16 squares, 4 in each or row, or column. Imagine that we want to make 8 squares from red transparent plastic, and the rest from blue transparent plastic. How many different designs are there? (The group that acts is the dihedral group of 8 elements.)

(4) Let G be a group acting transitively on a set S (no finiteness assumption is necessary). Let N be a normal subgroup of G of finite index. Find a formula for the number of orbits of N.
(5) Prove that there is a transitive action of S_5 on a set of 12 elements.
(6) Let G be a finite p-group and $H \neq \{1\}$ a normal subgroup of G. Prove that $H \cap Z(G) \neq \{1\}$ and, in particular, any normal subgroup of G with p elements is contained in the centre of G.
(7) Let G be a p-group and $H < G$ a proper subgroup with p^k elements. Prove that there is a subgroup of G with p^{k+1} elements that contains H. Deduce that every maximal subgroup of a p group has index p.
(8) Let G be a finite group and H a normal subgroup of G. Let P be a Sylow subgroup of G. Prove that $H \cap P$ is a Sylow subgroup of H and HP/H is a Sylow subgroup of G/H.
(9) Prove that a group of order pq^2, where $p \neq q$ are primes, is not simple.
(10) Prove that a group of order pqr, where $p < q < r$ are primes, is not simple.
(11) Prove that every group of order less than 60 is not simple, unless its order is prime.
(12) Prove that $\mathrm{PSL}_2(\mathbb{F})$ is not simple if $\mathbb{F}$ has 2 or 3 elements. In fact, prove the stronger fact that

$$\mathrm{PSL}_2(\mathbb{F}_2) \cong S_3, \qquad \mathrm{PSL}_2(\mathbb{F}_3) \cong A_4.$$

(13) Show that $\mathrm{PSL}_2(\mathbb{F}_4) \cong \mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$. One can also show that $\mathrm{PSL}_3(\mathbb{F}_2) \cong \mathrm{PSL}_2(\mathbb{F}_7)$ are simple groups of order 168 and that there are unique simple groups of order 60 and 168, but these facts are harder.
(14) Prove that for $n > 1$ there is no embedding $S_n \to A_{n+1}$. What about $S_n \to A_{n+2}$?
(15) Prove that for $n \geq 5$, A_n is the only normal subgroup of S_n.
(16) Let $\mathscr{F}$ be a free group on n generators. Prove that every element g of $\mathscr{F}$ has a representative that is reduced, namely, does not contain a sequence of the form tt^{-1} or $t^{-1}t$ where t is a generator. Prove that such a representative is unique and is also the word of minimal length that represents g.
(17) Write the quaternion group Q of 8 elements in the form $\langle X|R\rangle$. Prove that your presentation is correct!
(18) Let $G : \mathbf{Top}.\mathbf{Sp}. \to \mathbf{Sets}$ be a the forgetful functor from the category of topological spaces to the category of sets. Prove that G has both a left adjoint and a right adjoint.
(19) Let G be a group and $N \triangleleft G$ a normal subgroup. What is the universal property that G/N has?
(20) Let G_1, G_2 be groups. Prove that $(G_1 * G_2)^{\mathrm{ab}} \cong G_1 \oplus G_2$.
(21) An R-module M is called *cyclic* if there's $m \in M$ such that $M = Rm$. Namely, M is generated by one element over R. Prove that M is cyclic if and only if M is isomorphic to R/I for some left ideal I of R. Further, suppose that R is commutative; what does I being prime/maximal imply about M?

(22) Being free is not a local property of modules. Let $R = \mathbb{Z}[\sqrt{-6}]$. Prove the following.
   (a) Prove that the units of R are $\{\pm 1\}$. Let $I = \langle 2, \sqrt{-6}\rangle$. Prove that I is a prime ideal and is the only prime ideal containing 2.
   (b) Prove that I is not a free R-module.
   (c) Prove that I is locally free. (Distinguish between the case where $2 \notin \mathfrak{p}$ - which is a very easy case, where one doesn't really need to know anything about $\mathfrak{p}$ - and $2 \in \mathfrak{p}$, where then $\mathfrak{p} = I$.)
   (d) Conclude also that being cyclic is not a local property.

(23) Let $\mathbb{F}$ be a field and $0 \to V_1 \to V_2 \to \ldots \to V_n \to 0$ an exact sequence of finite dimensional vector spaces over $\mathbb{F}$. Prove that $\sum_{i=1}^{n} (-1)^i \dim_{\mathbb{F}}(V_i) = 0$. (Hint: it is convenient to split the exact sequence into

$$0 \to V_1 \to V_2 \to V_2/V_1 \to 0, \quad 0 \to V_2/V_1 \to V_3 \to V_3/V_2 \to 0, \quad \text{etc}).$$

(24) Let $\mathbb{F}$ be a field, V an $\mathbb{F}[x]$-module, finite dimensional as an $\mathbb{F}$-vector space. Prove that V is a cyclic $\mathbb{F}[x]$-module (namely, that there exists a vector $v \in V$ such that $\{v, Tv, T^2v, \ldots, T^{n-1}v\}$ is a basis for V over $\mathbb{F}$), if and only if the minimal polynomial of T is equal to its characteristic polynomial.

(25) Deduce from the structure theorem for modules over PID that a linear transformation is diagonalizable over a field $\mathbb{F}$ if and only if its minimal polynomial factors into linear terms.

(26) Let $F \subset L$ be fields. Deduce from the structure theorem for modules over PID that the minimal polynomial of a matrix M in $M_n(F)$ is the same as the minimal polynomial of M viewed as a matrix in $M_n(L)$.

(27) Let $\mathbb{F}$ be a field and $M \in M_n(\mathbb{F})$ an $n \times n$ matrix with entries in $\mathbb{F}$. Prove that M is conjugate to a unique block diagonal matrix $\mathrm{diag}(M_{c_1(x)}, \ldots, M_{c_a(x)})$ where $c_1(x)|c_2(x)|\cdots|c_a(x)$ are non-constant monic polynomials and $M_{f(x)}$ is the matrix defined in class (1's below the diagonal and minus the coefficients of f along the last column). Furthermore, the minimal polynomial of M is $c_a(x)$ and the characteristic polynomial is $c_1(x)c_2(x)\cdots c_a(x)$.

   Note that this result explains the obstruction for two matrices with the same characteristic and minimal polynomials to be conjugate over $\mathbb{F}$ (or an extension of $\mathbb{F}$, for that matter).

   Use this to count the number of conjugacy classes in $M_n(\mathbb{F}_q)$ for $n = 1, 2, 3, 4$.

(28) Let $\mathbb{F}$ be a field. Denote the category of finite dimensional vector spaces over $\mathbb{F}$ by $\mathbf{f.d.}\mathbb{F} - \mathbf{Vsp}$. Prove that the duality functor

$$* : \mathbf{f.d.}\mathbb{F} - \mathbf{Vsp} \quad \Longrightarrow \quad \mathbf{f.d.}\mathbb{F} - \mathbf{Vsp}$$

[where $V^* := \mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F})$ is the dual vector space and for $T : V \to W$, $T^* : W^* \to V^*$, defined by $T^*(\phi)(v) = \phi(Tv)$, is the dual linear map], is an anti-equivalence of categories.

(29) **Pullback.** Consider the diagram of modules

$$\begin{array}{ccc} & & M_1 \\ & & \downarrow{\scriptstyle h_1} \\ M_2 & \xrightarrow{h_2} & M_3 \end{array}$$

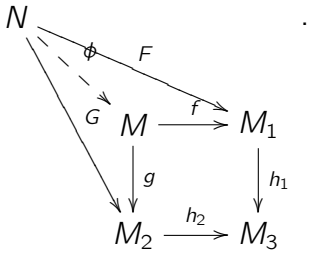
The projective limit of this diagram is called the *pull-back*, (in more "geometric categories" such as topological spaces, or manifolds, it is called the *fibre product*). Prove a simplified version: that the projective limit is a module M with homomorphisms such that the diagram

$$\begin{array}{ccc} M & \xrightarrow{f} & M_1 \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h_1} \\ M_2 & \xrightarrow{h_2} & M_3 \end{array}$$

commutes, and for every module N such that

$$\begin{array}{ccc} N & \xrightarrow{F} & M_1 \\ \downarrow{\scriptstyle G} & & \downarrow{\scriptstyle h_1} \\ M_2 & \xrightarrow{h_2} & M_3 \end{array}$$

commutes there is a unique commutative diagram:

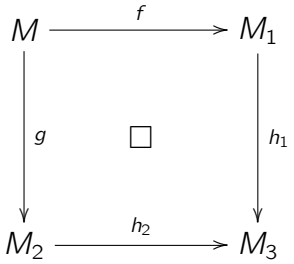


.

One also says that the diagram

$$\begin{array}{ccc} M & \xrightarrow{f} & M_1 \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h_1} \\ M_2 & \xrightarrow{h_2} & M_3 \end{array}$$

is a cartesian product and the notation



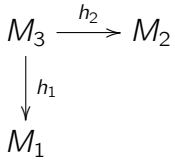
is often used to denote that.

Prove further that the pullback can be taken to be

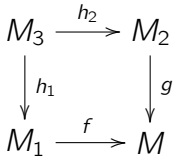
$$\{(m_1, m_2) : h_1(m_1) = h_2(m_2), m_i \in M_i\}$$

(with the natural projection maps).

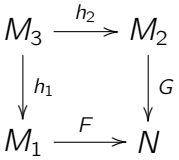
(30) **Pushout.** Consider the diagram of modules



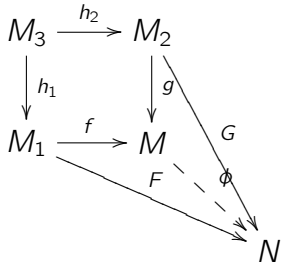
The injective limit of this diagram is called the *push-out*. Prove a simplified version: that the injective limit is a module M with homomorphisms such that the diagram



commutes, and for every module N such that



commutes there is a unique commutative diagram:



Prove further that the pushout can be taken to be

$$M_1 \oplus M_2/\{(h_1(m), -h_2(m)) : m \in M_3\}.$$

(with the natural maps).

(31) Let $\mathbf{C}$ be a category where direct limit exist. Consider the diagram below, where M is the push-out of $\begin{array}{ccc} & & B \\ & \nearrow & \\ C & & \\ & \searrow & \\ & & A \end{array}$,

$$\begin{array}{ccc} C & \xrightarrow{\beta} & B \\ {\scriptstyle\alpha}\downarrow & & \downarrow \\ A & \longrightarrow & M \end{array}$$

Does it follow that C is the pull-back?

(32) Let (F, G) be an adjoint pair of covariant functors. Prove that F commutes with direct limits and G with projective limits.

(33) Consider the following system of $\mathbb{Z}$-modules:
   (a) $\ldots \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z} \to \ldots$
   (b) $\ldots \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}$.
   (c) $\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z} \to \ldots$
   In each case, all arrows are multiplication by a fixed prime p. Find in each case the direct and projective limit of the system.

(34) Give an example of a category that doesn't have projective limits.

(35) Consider the ring $\mathbb{Z}[x]$. For each of the following ideals find the I-adic completion $\varprojlim \mathbb{Z}[x]/I^n$. "Find" means to give some concrete reasonable description of the limit.
   (a) $I = (p)$;
   (b) $I = (x)$;
   (c) $I = (p, x)$.

(36) For every open disk D in the complex plane around 0 let $A(D)$ be the ring of analytic functions on D. The collection of these disks is a directed poset, where we say $D \geq D'$ if $D \subseteq D'$. We have the restriction maps $A(D') \to A(D)$ and so we get a direct system. Find a concrete description in terms of power series for $\varinjlim_D A(D)$.

(37) Prove that for $x, y \in \mathbb{Z}_p$ one has $x|y$ if and only if $v(x) \leq v(y)$. Deduce that $\mathbb{Z}_p^\times = \{x : v(x) = 0\}$. Deduce that every ideal is principal and, in fact, $(0), (1), (p), (p^2), (p^3), \ldots$ is the complete list of ideals of $\mathbb{Z}_p$.

(38) Prove that $\mathbb{Z}_p^\times \cong \mu_{p-1} \times (1 + p\mathbb{Z}_p)$, where μ_{p-1} is the cyclic group of order $p-1$ consisting of the $(p-1)$-st roots of unity in $\mathbb{Z}_p$. Prove further that for $p > 2$

$$1 + p\mathbb{Z}_p \cong p\mathbb{Z}_p \cong \mathbb{Z}_p,$$

as topological groups (namely, there are bicontinuous isomorphisms). Hint: use the power series of $\exp(x) = 1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\dots$ and $\log(1+x) = x-\frac{x^2}{2}+\frac{x^3}{3}-\frac{x^4}{4}+\dots$ to define the isomorphisms. Note that you need of course to show that the series converge p-adically. On the other hand, you may use the identity of power series $\exp(\log(1+x)) = 1+x$, etc.)

(39) Let p be a prime. Show that the extension $\mathbb{Q}(\{e^{2\pi i/p^n} : n \in \mathbb{Z}_{>0}\})$, obtained from $\mathbb{Q}$ by adjoining all roots of unity of p power order in $\mathbb{C}$, is a Galois extension. Further, let G be its Galois group; prove

$$G \cong \mathbb{Z}_p^\times.$$

(40) Prove that every non-trivial closed subgroup of $\mathbb{Z}_p$ is open. Prove also that

$$\hat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/n\mathbb{Z} \cong \prod_p \mathbb{Z}_p$$

(where the limit is over all integers n with $\mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ being the natural map $x \mod mn \mapsto x \mod m$, and the product on the right hand side is over all primes). Use this to show that a profinite group could have non-finite, closed, subgroups that are not open.

(41) Let $G = \varprojlim_{\alpha\in I} G_\alpha$ be a profinite group (that is, an inverse limit with surjective transition maps over a directed index set). Let $\pi_j : G \to G_j$ be the canonical projection. Prove that a set $Z \subseteq G$ is dense if and only if $\pi_j(Z) = \pi_j(G)$ for every $j \in I$.

(42) Prove that a profinite group is totally disconnected. That is, every open subset U, $|U| \geq 2$, can be written as $U = V \coprod W$, a disjoint union of non-trivial open sets.

(43) Let p be a prime number and $\mathbb{F}_p$ a field with p elements. Prove that

$$x^{p^n} - x = \prod f(x),$$

the product being taken over all irreducible monic polynomials $f(x) \in \mathbb{F}_p[x]$ of degree dividing n.

Deduce that a non-constant polynomial $f(x) \in \mathbb{F}_p[x]$ is irreducible if and only if $\gcd(f(x), x^{p^n} - x) = 1$ for all $n \leq \deg(f(x))/2$. (The point is that the gcd can be calculated very quickly using the Euclidean algorithm while finding a root of f for $p \gg 0$ and $\deg(f) \gg 0$ is a hopeless task.)

(44) Prove that $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_d)$ where $d = \gcd(m, n)$.

(45) Let $K = \mathbb{Q}(\{\zeta_n : n \in \mathbb{Z}_{>0}\})$ be the field obtained from $\mathbb{Q}$ by adjoining all roots of unity of all orders. Using Galois theory (and the ring isomorphism $\hat{\mathbb{Z}} \cong \prod_{\ell \text{ prime}} \mathbb{Z}_\ell$) determine the structure of $\mathrm{Gal}(K/\mathbb{Q})$ and show that for every n, K has a subfield K_n such that $[K : K_n] = n$. (The field K_n is not unique and the exercise is, admittedly, more of a gymnastique in Galois theory than a valuable fact.)

(46) **Artin-Schreier Extensions.** Let $\mathbb{F}$ be a field of characteristic p and $K/\mathbb{F}$ a cyclic Galois extension of degree p. There are no roots of unity of order p in characteristic

p so we cannot even hope for Kummer's theory to apply. Artin-Schreier theory is a replacement.

(a) Let a be an element of $\mathbb{F}$ and consider the polynomial $x^p - x - a$. If α is a root of this polynomial, then so is $\alpha + b$ for every $b \in \mathbb{F}_p$. Let $K = F(\alpha)$. Then K is the splitting field of $x^p - x - a$. Prove that K is Galois and there is a natural homomorphism $\mathrm{Gal}(K/\mathbb{F}) \to \mathbb{F}_p$. Further, prove that if a is not of the form $c^p - c$ for some $c \in \mathbb{F}$ then $x^p - x - a$ is irreducible and $\mathrm{Gal}(K/\mathbb{F}) \cong \mathbb{F}_p$ is a cyclic group of order p.

(b) Let $K/\mathbb{F}$ be a cyclic extension of order p and σ a generator for the Galois group. Define the trace map

$$\mathrm{Tr} : K \to \mathbb{F}, \qquad \mathrm{Tr}(a) = a + \sigma(a) + \cdots + \sigma^{p-1}(a).$$

This is a surjective $\mathbb{F}$-linear map with kernel $\{b - \sigma(b) : b \in K\}$. (Hint: you may want to use independence of characters.)

(c) So, in particular $-1 = b - \sigma(b)$ for some $b \in K$. Prove that $b^p - b \in \mathbb{F}$. Let $a = b^p - b$. Then show that K is the splitting field of $x^p - x - a$.

(47) Prove that the polynomial $x^4 + px + p \in \mathbb{Q}[x]$ is irreducible for every prime p. Let G be its Galois group. Prove that $G \cong S_4$, unless p equals 3 or 5, in which case it is isomorphic to D_4 and C_4, respectively.

(48) Determine the Galois group of $(x^3 - 2)(x^3 - 3)$ over $\mathbb{Q}$ as a subgroup of S_6. Write the lattice of its subfields. Which ones are Galois over $\mathbb{Q}$?

(49) Let k be a field and $R = k[x, y]/(y^2 - x^3)$. Prove that R is an integral domain. Let $t = y/x$, an element of the fraction field K of R. Prove that $k[t]$ is the integral closure of R in K.

(50) Generalize the previous exercise to the ring $R = k[x, y]/(y^a - x^b)$, where a, b are relatively prime positive integers.

(51) Let $A \subseteq B$ be an integral extension and $\varphi : A \to k$ a homomorphism of A into an algebraically closed field k. Prove that φ can be extended to B. Further, give an example showing that the assumption that k is algebraically closed is necessary. (Suggestions: for the first part "think ideals"; for the second part one can take $A = \mathbb{Z}$, $k = \mathbb{Z}/3\mathbb{Z}$ and $B = \mathbb{Z}[i]$.)

(52) Let $A \subseteq B$ be an integral extension and $\mathfrak{n}$ a maximal ideal of B. Let $\mathfrak{m} = \mathfrak{n} \cap A$ (a maximal ideal of A). Is the extension $A_{\mathfrak{m}} \subseteq B_{\mathfrak{n}}$ necessarily integral? [Consider the subring $k[x^2 - 1]$ of $k[x]$ and the ideal $\mathfrak{n} = (x - 1)$. Can the element $1/(x + 1)$ be integral?]

$2^{\mathbf{nd}}$ Term

(53) Show that the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Z}[\sqrt[3]{2}]$. (Lots of computations...)

(54) Show that the ring of integers of $\mathbb{Q}(\sqrt{2},\sqrt{5})$ is $\mathbb{Z}[\sqrt{2},\frac{1+\sqrt{5}}{2}]$. (Lots of computations...)

(55) Let $p \neq 5$ be a prime number. By considering the number of roots of unity of order 5 in finite fields, argue that if $p \equiv 1 \pmod 5$ the polynomial $x^4+x^3+x^2+x+1$ splits modulo p, if $p \equiv -1 \pmod 5$ the polynomial is a product of two quadratic polynomials modulo p and if $p \equiv 2,3 \pmod 5$ the polynomial is irreducible modulo 5. Using these results write for every prime p how many prime ideals $\mathfrak{p}$ there are in $\mathbb{Z}[\zeta_5]$ such that $\mathfrak{p} \cap \mathbb{Z} = (p)$. Furthermore, for $p = 2,3,5,11,19$ find generators for these ideals.

(56) Compare $\mathrm{Spec}(\mathbb{Q}[x]/(x^p-1))$ and $\mathrm{Spec}(\overline{\mathbb{Q}}[x]/(x^p-1))$. Explain the morphism $\mathrm{Spec}(\overline{\mathbb{Q}}[x]/(x^p-1)) \to \mathrm{Spec}(\mathbb{Q}[x]/(x^p-1))$.

(57) Draw a picture of $\mathrm{Spec}(\mathbb{Z}/30\mathbb{Z})$ and all its points. Same for $\mathrm{Spec}(k[x])$, $\mathrm{Spec}(k[x]/(x^n))$, $\mathrm{Spec}(k[x,y]/(y-x^3))$, $\mathrm{Spec}(k[x,y]/(y^2-x^2))$ and $\mathrm{Spec}(k[x,y]/(x^2+y^2-1))$, where k is an algebraically closed field of characteristic $\neq 2$. In the cases where the spectrum consists of finitely many points calculate the local ring of each point.

(58) Let A be a commutative ring. Prove that $\mathrm{Spec}(A)$ is a disjoint union of two non-trivial closed sets if and only if $A \cong A_1 \times A_2$, a product of two non-zero rings.

(59) Let A be a commutative ring. Prove that the sets $D(f) = \{[\mathfrak{p}] : f \notin \mathfrak{p}\}$, as f varies over A, are a basis for the topology on $\mathrm{Spec}(A)$.

(60) Let A be a commutative ring. Prove that a closed set $V(\mathfrak{a}) \subseteq \mathrm{Spec}(A)$ is irreducible (meaning, if it's equal to $T \cup Z$, two closed sets, then it is equal to T, or to Z) if and only if $\sqrt{\mathfrak{a}}$ is a prime ideal.

(61) Let $A \subseteq B$ be an integral extension of integral domains and assume that A is integrally closed in its quotient field. Show, by example, that for $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ prime ideals of A and $f : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ the natural map, one may have $\sharp f^{-1}([p_2])$ greater, equal, or less than $\sharp f^{-1}([p_1])$. Also show that $\overline{f^{-1}([p_2])} \subset \overline{f^{-1}([p_1])}$.

(62) Write down Noether's normalization explicitly for the ring $k[x,y,z,w]/(xy-zw)$. Is the extension $k[x,y,z] \subset k[x,y,z,w]/(xy-zw)$ integral?

(63) Let k be a field. Prove that every finitely generated k-algebra is Noetherian.

(64) Let R be a commutative ring, $\mathfrak{p}$ a prime ideal of R and $\mathfrak{a}_1,\ldots,\mathfrak{a}_b$ any ideals of R. Prove that if $\mathfrak{p} \supseteq \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_b$ then $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some i.

(65) Give an example of a ring R such that the localization of R at any prime ideal is Noetherian, but R is not Noetherian.

(66) Which of the following rings are Noetherian?

- (a) The ring of rational functions of the complex variable z that have no pole on the circle $|z| = 1$.
- (b) The ring of complex power series in z with a positive radius of convergence, i.e., converging on some open disk around zero. (Hint: consider first the units in this ring.)
- (c) The ring of complex power series in z with an infinite radius of convergence.

(d) The ring of complex polynomials in z whose first k derivatives vanish at the origin.

(67) In this exercise we prove that every commutative Artin ring is isomorphic to a product of local Artin rings.
   (a) Let A be a commutative ring and let $\mathfrak{a}, \mathfrak{b}$ relatively prime ideals, i.e., two ideals such that $\mathfrak{a}+\mathfrak{b} = A$. Prove that for every $k > 0$ also $\mathfrak{a}^k, \mathfrak{b}^k$ are relatively prime ideals. Prove also that $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$.
   (b) Let R be an Artin ring and let $\mathfrak{m}_1, \ldots, \mathfrak{m}_a$ be its distinct maximal ideals. Prove that for every k, $(\prod_{i=1}^a \mathfrak{m}_i)^k = \prod_{i=1}^a \mathfrak{m}_i^k = \cap_{i=1}^a \mathfrak{m}_i^k$ and that for $k \gg 0$, $\cap_{i=1}^a \mathfrak{m}_i^k = 0$.
   (c) Prove that for $k \gg 0$ the map $R \to \prod_{i=1}^a R/\mathfrak{m}_i^k$ is an isomorphism. (Use the Chinese Remainder Theorem.)
   (d) Finally, prove that each $R/\mathfrak{m}_i^k$ is a local Artin ring.

(68) Let $f : M \to M$ be a surjective endomorphism of a noetherian R-module. Prove that f is an isomorphism.

(69) Prove that the following rings are not notherian:
   (a) $\mathbb{C}[t^{1/n} : n \in \mathbb{N}_>0]$. Conclude that a direct limit of noetherian rings need not be noetherian.
   (b) The ring of continuous functions $f : [0,1] \to \mathbb{R}$.
   (c) The ring $\mathbb{C}[x, x^2y, x^3y^2, \ldots, x^iy^{i-1}, \ldots] \subset \mathbb{C}[x,y]$. Conclude that a subring of a noetherian ring need not be noetherian.

(70) Show that the number of generators for ideals in $\mathbb{C}[x,y]$ is not bounded. Namely that for every $n \in \mathbb{N}$ there is an ideal of $\mathbb{C}[x,y]$ that cannot be generated by less than n elements.

(71) Let p be a prime number. Let $P = \cup_{k=1}^\infty \frac{1}{p^k}\mathbb{Z}/\mathbb{Z}$. Prove that P is an artinian but not noetherian $\mathbb{Z}$-module.

(72) Show that the ring $R = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a \in \mathbb{Z}, b, c \in \mathbb{Q} \right\}$ is left noetherian but not right noetherian.

(73) Let R be a commutative ring and let $\mathfrak{a}, \mathfrak{b}$ be ideals of R. We define

$$(\mathfrak{a} : \mathfrak{b}) = \{r \in R : r\mathfrak{b} \subseteq \mathfrak{a}\}.$$

This is an ideal of R. In spite of the nice notation, it can be badly behaved.
   (a) For $x, y \in R$, write $(x : y)$ for $(\langle x \rangle, \langle y \rangle)$. Using prime factorization, calculate for $m, n \in \mathbb{Z}$ the ideal $(m : n)$.
   (b) Show that $\mathfrak{b}(\mathfrak{a} : \mathfrak{b}) \subseteq \mathfrak{a}$ but that equality doesn't hold in general.
   (c) Suppose that $\mathfrak{b}|\mathfrak{a}$ in the sense that there exists and ideal $\mathfrak{c}$ such that $\mathfrak{b}\mathfrak{c} = \mathfrak{a}$. Show that also $\mathfrak{b}(\mathfrak{a} : \mathfrak{b}) = \mathfrak{a}$, but $\mathfrak{c} \neq (\mathfrak{a} : \mathfrak{b})$, in general.

(74) Let R be a Noetherian commutative ring. Prove that any non-zero ideal of R contains a product of non-zero prime ideals. (Hint: suppose not. Choose an ideal

I maximal relative to this property. Prove that whether I is prime or not leads to a contradiction.)

(75) Let $A \in {}_R\mathrm{Mod}_S$. Prove that $A \otimes_S (-)$ is not a left exact functor.

(76) Let (F, G) be an adjoint pair of covariant functors between additive categories. Prove that F is right-exact and G is left-exact. (In particular, $A \otimes_S (-)$ and $\mathrm{Hom}_R(A, -)$ are right and left exact, respectively).

(77) Let V, W be finite-dimensional k vector-spaces. Prove (directly) that there is a natural isomorphism

$$\mathrm{Hom}_k(V, W) \cong V^* \otimes_k W,$$

where V^* is the dual vector space. On the other hand, show, based on what we had done in class, that

$$\mathrm{Hom}_k(V, W) \cong (V \otimes_k W^*)^*.$$

Conclude that $(V \otimes_k W)^* \cong V^* \otimes_k W^*$.

Prove that there is an isomorphism of k-vector spaces,

$$\mathrm{Bilin_k}(\mathrm{V} \times \mathrm{W}, \mathrm{k}) \cong \mathrm{V}^* \otimes_{\mathrm{k}} \mathrm{W}^*.$$

(78) Let n, m be positive integers. Denote by n the multiplication by n map. Analyze the sequence obtained from

$$0 \longrightarrow \mathbb{Z} \xrightarrow{[n]} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0\ ,$$

upon tensoring over $\mathbb{Z}$ with $\mathbb{Q}$, and with $\mathbb{Z}/m\mathbb{Z}$.

(79) Let R be a commutative ring and I an ideal of R. Let M be an R-module. Prove an isomorphism of R-modules,

$$(R/I) \otimes_R M \cong M/IM.$$

(80) Let k be a field.

(a) Let V, W be k vector spaces of finite dimension. Let $\{v_i : i = 1, \ldots, a\}$ be a basis for V, $\{w_i : i = 1, \ldots, b\}$ be a basis for W. Prove that $\{v_i \otimes w_j : i = 1, \ldots, a, j = 1, \ldots, b\}$ is a basis for $V \otimes W$.

(b) Let $V^{\otimes n}$ be equal to k for $n = 0$, V for $n = 1$ and, in general, $V^{\otimes n+1} = V^{\otimes n} \otimes_k V$ for every non-negative integer n. Find a basis for $V^{\otimes n}$ as a k-vector space.

(c) Define $T(V)$, the tensor algebra of V, as

$$T(V) = \oplus_{n=0}^{\infty} V^{\otimes n}.$$

Prove that $T(V)$ is a graded algebra, where the multiplication law

$$V^{\otimes m} \times V^{\otimes n} \to V^{\otimes m+n}$$

is determined by

$$(v_1 \otimes \cdots \otimes v_m, v_1' \otimes \cdots \otimes v_n') \mapsto v_1 \otimes \cdots \otimes v_m \otimes v_1' \otimes \cdots \otimes v_n'.$$

Note that it is not commutative in general.

(d) We define the symmetric algebra of V, $\mathrm{Sym}(V)$, as the quotient of $T(V)$ by the (graded) ideal generated by all expressions of the form

$$v_1 \otimes \cdots \otimes v_i \otimes \cdots \otimes v_j \otimes \cdots \otimes v_n - v_1 \otimes \cdots \otimes v_j \otimes \cdots \otimes v_i \otimes \cdots \otimes v_n,$$

in $\mathrm{Sym}(V)$ for any v_i, v_j and n.
Prove that this is the same ideal of relations as the one where we take all the generators

$$v_1 \otimes \cdots \otimes v_n - v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)},$$

where σ is any permutation.
Prove that $\mathrm{Sym}(V)$ is a commutative algebra.

(e) Suppose that V has dimension n, prove that $\mathrm{Sym}(V) \cong k[x_1, \ldots, x_n]$, the ring of polynomials in n variables.

(f) Formulate and prove a universal property for the morphism $V \to \mathrm{Sym}(V)$.

(g) Let Q a symmetric bilinear form $V \times V \to k$ and let $Q(v) := Q(v, v)$. Define the Clifford algebra $C(V)$ as the quotient of the algebra $T(V)$ by the ideal generated by all the expressions $v \otimes v - Q(v)$. Note that $C(V)$ has a $\mathbb{Z}/2\mathbb{Z}$ grading. The even part, $C^+(V)$, is called the even Clifford algebra. Let $e_1, \ldots, e_n$ be an orthogonal basis for V. Prove that the 2^n elements of $C(V)$ given by $e_{i_1} e_{i_2} \cdots e_{i_j}$, where $1 \leq i_1 < i_2 < \cdots < i_j \leq n$, form a basis for $C(V)$. (Here $e_{i_1} e_{i_2} \cdots e_{i_j}$ is the image of $e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_j}$ under $T(V) \to C(V)$.) Conclude that $C(V)$ is a 2^n-dimensional algebra over k.
Remark: it is not hard to show this is a spanning set; it's harder to show linear independence.

(h) Prove that the Clifford algebra has the following universal property: There is a linear map $f : V \to C(V)$ such that $f(v)^2 = Q(v)$ and this map is universal. Namely, for every k-algebra A and a linear map $g : V \to A$ for which $g(v)^2 = Q(v)$ for all $v \in V$, there is a unique morphism of k-algebras $G : C(V) \to A$ such that $G \circ f = g$.

(i) Consider now the special case $Q = 0$. In this case the Clifford algebra is called the exterior algebra of V and is denoted $\bigwedge^* V$ and the image of $e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_j}$ under $T(V) \to \bigwedge^* V$ is denoted $e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_j}$. Prove that in $\bigwedge^* V$ we have $v_1 \wedge \cdots \wedge v_i \wedge \cdots \wedge v_j \wedge \cdots \wedge v_r = 0$ if $v_i = v_j$ for $i < j$. So moding out by the linear span of all these relations is an equivalent definition of $\bigwedge^* V$.
Prove, further, that for every permutation $\sigma \in S_r$ we have

$$v_1 \wedge v_2 \wedge \cdots \wedge v_r = \mathrm{sgn}(\sigma) v_{\sigma(1)} \wedge v_{\sigma(2)} \wedge \cdots \wedge v_{\sigma(r)},$$

and, conversely, if k has characteristic different from 2, these relations are equivalent to the relations defining $\bigwedge^* V$.

Show that $\bigwedge^* V$ is a graded algebra $\bigwedge^* V = \oplus_{k=0}^n \bigwedge^k V$, where $\bigwedge^k V$ has dimension $\binom{n}{k}$ and basis $e_{i_1} \wedge \cdots \wedge e_{i_k}$, $1 \leq i_1 < \cdots i_k \leq n$. Multiplication in $\bigwedge^* V$ is "commutative up to a sign"; make this precise!

(81) Let R be a commutative ring and M, N, two projective R-modules. Prove that $M \otimes_R N$ is projective without using that M, or N, are direct summands of free modules.

(82) We consider the category of $\mathbb{Z}$-modules (= abelian groups). Show that $\mathbb{Q}/\mathbb{Z}$ is injective, but is not flat. Show that $\mathbb{Z} \oplus \mathbb{Q}$ is flat, but is not injective or projective. Show that $\mathbb{Z}$ is projective and not injective. Show that $\mathbb{Q}$ is injective but not projective.

(83) Let R be an integral domain. Prove that R is a field if and only if R is both injective and projective as an R-module.

(84) Let R be a commutative ring. Prove that $R[x]$ is a flat R-module. (This is easier than it seems at first sight....)

(85) Let M, N be flat R modules, where R is a commutative ring. Prove that $M \otimes_R N$ is flat too.

(86) Prove that the direct sum of divisible groups and a quotient of a divisible group is divisible.

(87) Let R, S be rings, such that R is a left S-module. Let $M \in {}_S\mathrm{Mod}$ be an injective S-module. Prove that $\mathrm{Hom}_S(R, M)$, which is a left R-module, is injective too.

(88) Let R be a PID. Prove that an R-module A is injective iff it is divisible.

(89) Prove that a direct summand of an injective module is injective.

(90) Prove that the following are equivalent for a ring R: (i) R is semisimple as a left R-module; (ii) every left R module is injective; (iii) every left R-module is projective.

(91) Let D be a division ring and n a positive integer. Prove that D^n is the only simple $M_n(D)$-module. Show that $M_n(D)$ is a semisimple module over itself and find its factorization a sum of simple modules. Prove that $\mathrm{End}_{M_n(D)}(D^n) \cong D^{\mathrm{opp}}$.

(92) Prove that R is a division ring if and only if R is a simple R-module. (Caution: given a nonzero element $x \in R$ you need to show that there is $y \in R$ such that both xy and yx are equal to 1. In fact, show that if $xy = 1$ then $yx = 1$.)

(93) Let R be a ring and let $\tilde{J}(R)$ be the intersection of all maximal right ideals of R. Find a characterization of the elements of $\tilde{J}(R)$ using right quasi-regular elements. Using this, show that $J(R) = \tilde{J}(R)$.

(94) Show that the condition on finite generation appearing in Nakayama's lemma is necessary.

(95) Consider the ring $R = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a \in \mathbb{Q}, b, d \in \mathbb{R}\}$. Classify all the right ideals of R and all the left ideals of R. Prove that R is right artinian but is not left artinian. Calculate the Jacobson radical of R.

(96) Prove that a ring R that is a semisimple left R-module is a finite sum of simple left R-modules and hence left artinian.

(97) Prove, using the Artin-Wedderburn theorem that a ring is left semisimple over itself if and only if it is right semisimple over itself.

In the following questions the representations are over an algebraically closed field k whose characteristic does not divide the number of elements of G. (Unless explicitly stated otherwise).

(98) Another proof of Maschke's theorem for $\mathbb{C}[G]$: Let G be a finite group. We wish to prove that $\mathbb{C}[G]$ is semisimple. Explain why it is enough to prove that every finite dimensional representation of G is semisimple. Thus, let $\rho : G \to \mathrm{GL}(V)$ be a linear representation of G. Prove that there is a hermitian form $\langle \cdot, \cdot \rangle$ that is G-invariant. That is, $\langle \rho(g)v, \rho(g)w \rangle = \langle v, w \rangle$ for all $v, w \in V$.

Given a subrepresentation $U \subseteq V$ show that $V = U \oplus U^{\perp}$ and $U^{\perp}$ is also a representation of G. Finish the proof.

(99) Let G be a finite group. Prove that the number of irreducible one dimensional representations of G is $|G/G'|$.

(100) Let A be an $n \times n$ matrix with characteristic polynomial $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$ and let B be an $m \times m$ matrix with characteristic polynomial $g(x) = \prod_{i=1}^{m}(x - \beta_i)$. Prove that the Kronecker product has characteristic polynomial $\prod_{i=1}^{n}\prod_{j=1}^{m}(x - \alpha_i\beta_j)$. Also, prove that although $A \times B$ need not be equal to $B \times A$, they are nonetheless conjugate.

(101) Let V be a finite dimensional representation of G. Prove that $\mathrm{Sym}^n(V)$ and $\bigwedge^n V$ are representations of G as well. As a particular (and often used) case, suppose that we have a two dimensional representation and that $g \in G$ acts by $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Write the matrix for g in the 3-dimensional representation $\mathrm{Sym}^2(\mathbb{C}^2)$.

(102) Let R be a ring, M a semisimple R-module and N a simple R module. Prove that N is isomorphic to a quotient module of M if and only if N is isomorphic to a submodule of M. Phrase this conclusion for the case $R = k[G]$ in terms of representations.

(103) Let W be an irreducible finite dimensional representation of a group G, finite or infinite, over an algebraically closed field k. Prove (not using Artin-Wedderburn, but just linear algebra) that $\mathrm{End}_{k[G]}(W) \cong k$, namely, that every G-equivariant map $W \to W$ is multiplication by a scalar.

In the following exercises use characters, whenever convenient. G is a finite group, k an algebraically closed field of characteristic prime to $\sharp G$, and all linear representations of G are finite dimensional and over k.

(104) Let (V, ρ) be an irreducible representation of G. Let (k, χ) be a one dimensional representation of G. Prove that $(V \otimes k, \rho \otimes \chi)$ is an irreducible representation of G

and provide a criterion to determine if it is isomorphic to ρ or not. We will denote this representation $V(\chi)$ or $\rho \otimes \chi$.

(105) Let P^0 be the trace zero permutation representation of S_n. Let sgn be the sign representation of S_n. Prove that $P^0 \otimes$sgn is irreducible as well. When is it isomorphic to P^0?

(106) Find the character table of the group Q, the quaternion group with 8 elements.

(107) Find the character table of the group A_4, the alternating group with 12 elements.

(108) Find the character table of the group S_4, the symmetric group with 24 elements.

(109) If χ is an irreducible character of S_4 calculate its restriction to A_4 as a sum of irreducible characters of A_4.

(110) Prove that $\bigwedge^2 P^0$ is an irreducible representation of S_n. In fact, this is true $\bigwedge^a P^0, a = 1, 2, \ldots, n-1$, but is combinatorially harder to prove. Is $\bigwedge^2 P^0 \cong \bigwedge^2 P^0 \otimes \text{sgn}$?

(111) For each character ϕ of A_3 write $\text{Ind}_{A_3}^{S_3}\phi$ in terms of the irreducible representations of S_3.

(112) For each irreducible representation ρ of S_3 write $\text{Ind}_{S_3}^{S_4}$ in terms of the irreducible representations of S_4.

(113) Use the formula for the character of $\text{Hom}_k(V, W)$, and Schur's lemma to prove the orthogonality relations of characters.

(114) Let $V^G = \{v \in V : \rho(g)v = v, \forall g \in G\}$ be the subspace of fixed vectors. Prove from first principles that

$$\dim_k(V^G) = \frac{1}{\sharp\, G} \sum_{g \in G} \chi_\rho(g).$$

(Hint: consider the operator $\frac{1}{\sharp\, G} \sum_{g \in G} \rho(g)$.)

(115) Let G be a finite group acting on a finite non-empty set S. Use the formula for $\dim(V^G)$ to deduce the Cauchy-Frobenius formula (also knows as Burnside's lemma) that states that the number of orbits of G in S is equal to $\frac{1}{\sharp\, G} \sum_{g \in G} I(g)$, where $I(g)$ is the number of fixed points of g in S.

(116) Deduce from the previous question that if $|S| = n > 1$ and G acts transitively on S then there is an element $g \in G$ without fixed points. Let $G_0 = \{g \in G :$ g has no fixed point in S$\}$. It is a subset of G (but usually not a subgroup). Let

$$c_0 = \sharp\, G_0 / \sharp\, G.$$

Jordan proved that $c_0 \geq 1/\sharp\, G$. Here we prove the stronger result (a result of Cameron-Stewart) that $c_0 \geq 1/\sharp S$.

To prove that construct the vector space on the basis S and let χ be the character of the representation of G on that space. First prove that

$$\frac{1}{\sharp\, G} \sum_{g \in G} \chi^2(g) \geq 2.$$

(Which representation is lurking in the background?...) Then prove that theorem on c_0 by arguing that

$$\sum_{g\in G}(\chi(g)-1)(\chi(g)-n)\leq n\,\sharp G_0$$

and continuing to examine this inequality.

(117) Let G_1, G_2 be finite groups. Prove (under the usual conditions on k) that every irreducible representation of $G_1\times G_2$ is isomorphic to the tensor product $V_1\otimes V_2$, where V_i is an irreducible representation of G_i and in fact, letting V_1 range over the irreducible representations of G_1 and V_2 range over the irreducible representations of G_2 we get every irreducible representation of $G_1\times G_2$ once. (Suggestion: do first the last part and count how many irreducible representations you get this way.)

(118) Consider the group $\mathbb{Z}/2\mathbb{Z}\times S_3$ - a non abelian group of order 12. Write its character table. Compare it with the character table of A_4 to deduce it is not isomorphic to A_4 (although it is not hard to see that directly either).

(119) Find the character table of D_{2n} for n even.