EXERCISE SHEET, MATH 570, FALL 2011

First assignment (due Wednesday, October 12). Solve questions 4, 5, 7, 13, 17, 19. Remember that solutions must be typed, except for matrices and diagrams that you can insert by hand, if you wish. You may use other questions on the assignment to solve the questions you need to submit, even without including the proofs.

Second assignment (due Thursday, October 27). Solve questions 22, 25, 32, 33. Same instructions as assignment 1. I prefer that you send me pdf files, as opposed to hard copies. You can still print the tex; add diagrams etc. by hand. Scan it and send me a pdf. But hard copies are also OK.

Third assignment (due Monday, November 21). Solve questions 37 - 42. Same instructions as assignment 2.

Fourth assignment (due Tuesday, December 6). Solve questions 44, 47, 49, 51. Solve (any of) questions 46, 50, 52 as bonus questions to improve your overall grade on assignments. Otherwise, same instructions as previous assignments.

(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

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

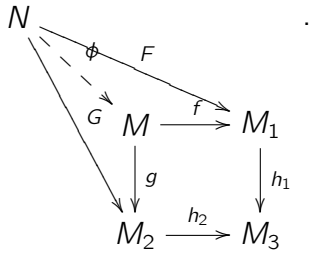
The projective limit of this diagram is called the *pull-back*, (in more "geometric categories" such as topological spaces, or manifolds, it is called the *fibre product*). Prove a simplified version: that the projective limit is a module M with homomorphisms such that the diagram

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

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:

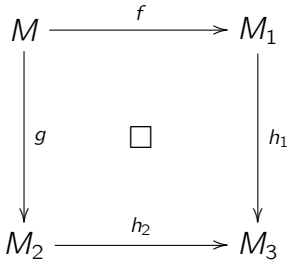


.

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



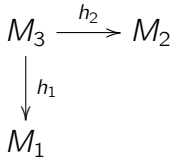
is often used to denote that.

Prove further that the pullback can be taken to be

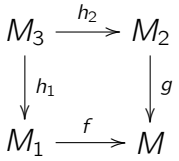
$$\{(m_1, m_2) : h_1(m_1) = h_2(m_2), m_i \in M_i\}$$

(with the natural projection maps).

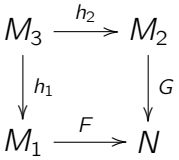
(30) **Pushout.** Consider the diagram of modules



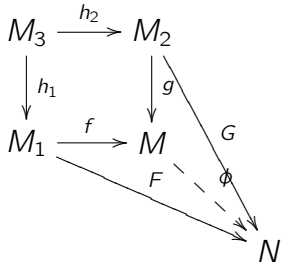
The injective limit of this diagram is called the *push-out*. Prove a simplified version: that the injective limit is a module M with homomorphisms such that the diagram



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?]