EXERCISES, MATH 570, FALL 2012

I suggest solving all the exercises, as soon as they get posted. Periodically, I will ask you to submit selected exercises, in LaTeX (or at any rate, as a pdf file).

Note carefully: The pdf file should be called as follows

YourLastName.AssignmentNumber.pdf

and sent to the following email address (and **NOT** to my McGill address):

2eyalgoren@gmail.com

(So Mr. Smith will submit his second assignment as a pdf file titled Smith.2.pdf)

Assignment 1: Please submit questions (2), (3), (4), (5), (7), (8) by Wednesday, September 19, 20:00.
Assignment 2: Please submit questions (10), (11), (12), (13), (14) by Wednesday, September 26, 20:00.
Assignment 3: Please submit questions (19) - (24) by Wednesday, October 10, 20:00.
Assignment 4: Please submit questions (25) - (29) by Monday, October 29, 20:00.
Assignment 5: Please submit questions (30) - (33) by Monday, November 5, 20:00.
Assignment 6: Please submit questions (34), (35), (36), (39) (enough to prove for either F or G) and (40) by Wednesday, November 14, 20:00.
Assignment 7: Please submit questions (44) -(49) and (52) by Wednesday, November 21, 20:00.

(1) A subgroup H of a group G is called a characteristic subgroup if for every automorphism $f : G \to G$, $f(H) \subseteq H$.
   (a) Prove that a characteristic subgroup is normal.
   (b) Prove that the commutator subgroup of G and the centre of G are characteristic subgroups.
   (c) Prove that if H is normal in G and K is a characteristic subgroup of H, then K is normal in G.
(2) Let G be a finite non-trivial p-group. Prove that G' (the commutator subgroup of G) is a proper subgroup of G.
(3) Let G be a finite p group and $H \triangleleft G$ a non-trivial normal subgroup. Prove that $H \cap Z(G) \neq \{1\}$.
(4) Let G be a finite p group and H a normal subgroup of G with p^a elements, $a > 0$. Prove that H contains a subgroup of order p^{a-1} that is normal in G. (Hint: use the previous exercise to prove the result by induction.)
(5) Let $G = \mathrm{GL}_n(\mathbb{F}_q)$, where $\mathbb{F}_q$ is a finite field, $q = p^r$ where p is prime.

(a) Prove that the upper unipotent matrices $\left\{ \begin{pmatrix} 1 & * & * & \dots & * \\ 0 & 1 & * & \dots & * \\ \vdots & & & \vdots & \\ 0 & \dots & & & 1 \end{pmatrix} \right\}$ are a p-Sylow subgroup P of G by calculating the order of P and G.
(b) Find conditions so that every element of P has order dividing p. (Hint: use the binomial theorem for $(I+N)^p$, where I is the identity matrix.)
(c) In particular, deduce that for any $p \neq 2$ there are non-abelian p-groups such that every element different from the identity has order p.
(d) Prove that a group G in which $a^2 = 1$ for all $a \in G$ is an abelian group.

(6) There are up to isomorphism precisely two non-abelian groups of order 8, the dihedral group D_4 and Q the quaternion group. Q is the group whose elements are $\{\pm 1, \pm i, \pm j, \pm k\}$, where -1 is a central element and the relations $ij = k, jk = i, ki = j$, $i^2 = j^2 = k^2 = -1$ hold (in addition to the implicit relations such as $-1^2 = 1$, $-1 \cdot j = -j$, ...). Prove the following
(a) D_4 is not isomorphic to Q.
(b) D_4 and Q are non-abelian. (Calculate, for instance what is ji.)
(c) Let P be the 2-Sylow subgroup of $\mathrm{GL}_3(\mathbb{F}_2)$. Find whether P is isomorphic to D_4 or to Q.

(7) Let p be an odd prime. In this exercise we show that a non-abelian group G of order p^3 that has an element x of order p^2 is isomorphic to the group we have constructed in class. It is enough to show it is a semi-direct product $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.
(a) Show that $Z(G) = G'$ is a subgroup of order p and that $G/Z(G) \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. In particular, any commutator is in the centre of G and is killed by raising to a p power.
(b) Prove that x^p generates the centre of G.
(c) Prove that to show that G is a semi-direct product $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$, it is enough to show that there is an element $y \in G$ such that $y^p = 1$ and $y \notin Z(G)$.
(d) Let $y \notin \langle x \rangle$ and suppose that y is of order p^2. Show that G is generated by x and y. We want to show that we can find an element $\tilde{y}$ of order p such that $\tilde{y} \notin Z(G)$. We show that by counting how many elements of order p the group G has.
(e) Prove the surprising property, that the function $f : G \to G$, $f(t) = t^p$, is a homomorphism of groups. For that, explain why it is enough to prove the identity $x^p y^p = (xy)^p$ and proceed to prove this property by making use of identities of the form $xyxy = x[y,x]xyy = [y,x]x^2y^2$, etc.
(f) By estimating the image and the kernel of f show that there exists an element $\tilde{y}$ as wanted.

(8) Let $p < q < r$ be primes. Prove that a group of order pqr is not simple.
(9) If there are a colours available, prove that there are $\frac{1}{n}\sum_{d|n} \varphi(n/d) a^d$ coloured roulette wheels with n sectors.
(10) Let G be a group acting on a non-empty set S transitively. Let N be a normal subgroup of G of finite index. Find the number of orbits of N in S.
(11) Let the symmetric group S_n act transitively on a set of m elements. Assume that $n \geq 5$ and that $m > 2$. Show that $m \geq n$.
(12) Exhibit A_4 as a semi-direct product.
(13) Prove that there is another non-abelian group, that is not isomorphic to A_4, which is a semi-direct product.
(14) Let G act transitively on a set S. Then, G acts primitively if and only if the point stabilizer of a point of S is a proper maximal subgroup of G. (One direction was done in class.)

(15) Give an example of a group G acting on a set primitively, but not 2-transitively.
(16) Prove that every simple group G of order 60 is isomorphic to A_5. [Suggestion: construct first a subgroup of index 5 as a normalizer of a certain Sylow subgroup. As to what should be the definition, take your cue from considering what happens for A_5.] Conclude the following isomorphisms: $\mathrm{PSL}_2(\mathbb{F}_4) \cong \mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$.
(17) Combining the Sylow theorems (and, in particular, the examples we analyzed above) and the coset representation (and perhaps additional tricks, if you wish) show that every group of order smaller than 60 is solvable. Note that $|A_5| = 60$, so the value 60 is a natural barrier.
(18) Let G be a group and $N \lhd G$ a normal subgroup. What is the universal property that G/N has?
(19) 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, but they are not equal!
(20) Given a set S define a partially ordered set 2^S whose elements are the subsets of S and where for two subsets A, B of S (that is, elements of 2^S) say that $A \leq B$ if $A \subseteq B$.

The category **Poset** of partially ordered sets has as objects partially ordered sets $(T, \leq)$ and the morphisms $\mathrm{Mor}((T_1, \leq), (T_2, \leq))$ are functions $f : T_1 \to T_2$ such that if $x \leq y$ are elements of T_1 then $f(x) \leq f(y)$. Determine if $S \mapsto 2^S$ (with the partial order defined above) is a functor. Is it full? faithful?
(21) Let k be a field and $\mathbf{C}$ the category of finite dimensional vector spaces over k. Let F associate to a vector space V the vector space $F(V) = V^* := \mathrm{Hom}_k(V, k)$ and to a linear map $T : V \to W$ the linear map $F(T) = T^* : W^* \to V^*$ defined by $T^*(\phi) = \phi \circ T$. Prove that F is a contravariant functor that is fully faithful.
(22) Find a presentation for the following groups: D_n (the dihedral group with $2n$ elements) and Q (the quaternion group of order 8). You need to prove your presentation is correct!
(23) Prove that $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ is an infinite group. Show, further, that it has a group of order 6 as a quotient.
(24) Let G_1, G_2 be groups. Prove that $(G_1 * G_2)^{\mathrm{ab}} \cong G_1^{\mathrm{ab}} \oplus G_2^{\mathrm{ab}}$.
(25) Let R be a commutative ring. Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of R-modules. Then, if M_1 and M_3 are free also M_2 is free.
(26) Let R be a commutative ring. Prove that "being equal" is a local property. That is, suppose that A, B are two submodules of a module M then $A = B$ if and only if for all $\mathfrak{p}$ prime $A_{\mathfrak{p}} = B_{\mathfrak{p}}$. (Suggestion: reduce first to the case $A \subseteq B$.)
(27) Let R be a commutative ring. Prove that a morphism $f : M \to N$ of R-modules is the zero morphism if and only if $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is the zero morphism for all prime ideals $\mathfrak{p}$.
(28) Let R be any ring and M a left R-module. M is called a cyclic R-module if there is a surjection of left R-modules $R \to M$. Equivalently, if there is an element $m \in M$ such that $Rm = M$. Show that M is cyclic if and only if $M \cong R/I$, where I is a left ideal of R. Suppose further that R is commutative. If I is prime, or maximal, what module property does the cyclic R-module R/I have?
(29) Let R be a commutative ring. Prove that being free is not a local property. For example, let $I = \langle 2, \sqrt{-6} \rangle$ be the ideal of the ring $R = \mathbb{Z}[\sqrt{-6}]$ generated by 2 and $\sqrt{-6}$. Show that I is locally free, but not a free R-module. (This shows also that being cyclic is not a local property.) Some guidance: For a prime ideal $\mathfrak{p}$ of R, note that $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ and so is "well-known". This should be enough for you to deal with all the localizations at primes $\mathfrak{p}$ such that $\mathfrak{p} \cap \mathbb{Z}$ is not the ideal $2\mathbb{Z}$. To deal with primes $\mathfrak{p}$ such that $\mathfrak{p} \cap \mathbb{Z} = 2\mathbb{Z}$ consider the element $2/\sqrt{-6}$ in such a localization and re-write it appropriately.

(30) Prove that the category of groups is not equivalent to the category of sets. (Hint: look for a property that one category has and the other doesn't and show that this property is preserved under equivalence.)

(31) Fix a group G. Consider the category $\mathbf{C}$ whose objects are subgroups of G and the morphisms are the inclusion maps. Consider the category $\mathbf{D}$ of sets S endowed with a *transitive* action of G and with a choice of base point $s_0 \in S$. Namely, objects are triples $(S, s_0, G \to \Sigma_S)$, where the image of G is transitive subgroup of Σ_S. A morphism

$$f : (S, s_0, G \to \Sigma_S) \to (T, t_0, G \to \Sigma_T),$$

is a function $f : S \to T$ such that $f(s_0) = t_0$ and such that f is equivariant for the action of G: $f(g * s) = g * f(s)$. Prove that the categories $\mathbf{C}$ and $\mathbf{D}$ are equivalent.

(32) Let $F : \mathbf{C} \to \mathbf{D}$ and $G : \mathbf{D} \to \mathbf{C}$ be a pair of covariant functors. It is a theorem that the following are equivalent statements:
(a) $FG \cong I_{\mathbf{D}}$ and $GF \cong I_{\mathbf{C}}$.
(b) F is left adjoint to G and both functors are full and faithful.
(c) F is right adjoint to G and both functors are full and faithful.

Prove one of the 6 possible implications in this theorem.

(33) 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 if and only if there exists a vector $v \in V$ such that $\{v, Tv, T^2v, ..., T^{n-1}v\}$ is a basis for V over $\mathbb{F}$ (where T is the linear transformation corresponding to x), if and only if the minimal polynomial of T is equal to its characteristic polynomial.

(34) *An example of a division algebra which is not a field.* Let α, β be negative integers. Consider the rank 4 $\mathbb{Q}$-vector space

$$\mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k,$$

where i, j, k are formal symbols. Define addition component-wise and multiplication by extending linearly the rules

$$i^2 = \alpha, \quad j^2 = \beta, \quad ij = -ji = k.$$

Find an embedding of this $\mathbb{Q}$ vector space into $M_2(\mathbb{C})$ such that multiplication matches multiplication of matrices. Use this to prove that we have defined an associative $\mathbb{Q}$-algebra. This is an example of a quaternion algebra B over $\mathbb{Q}$ (denoted $\left(\frac{\alpha,\beta}{\mathbb{Q}}\right)$). Prove further that B is a (non-commutative) division algebra.

Define the norm of an element of B by

$$N(x + yi + zj + wk) = (x + yi + zj + wk)(x - yi - zj - wk).$$

Show that the norm takes values in $\mathbb{Q}$ and is multiplicative: $N(ab) = N(a)N(b)$. Prove that if $a \neq 0$ then $N(a) \neq 0$. Can you use that to prove that B is a division algebra? (The special case $\alpha = -1, \beta = -1$ gives the Hamilton quaternions (over $\mathbb{Q}$).)

(35) Show that direct limits do not exist in the category of linearly ordered sets. (Hint: a counterexample involving just two sets exists.)

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

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

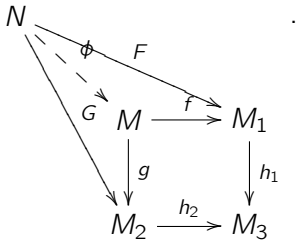
The projective limit of this diagram is called the pull-back, (in more "geometric categories" such as topological spaces, or manifolds, it is called the fibre product). Prove a simplified version: that the projective limit is a module M with homomorphisms such that the diagram

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

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

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

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).

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

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

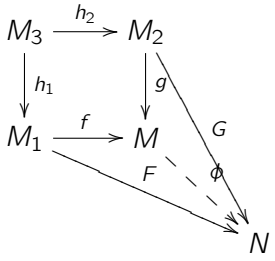
The injective limit of this diagram is called the push-out. Prove a simplified version: that the injective limit is a module M with homomorphisms such that the diagram

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

commutes, and for every module N such that

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

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).

(38) Let $\mathbf{C}$ be a category where direct limit exist. Consider the diagram below, where M is the push-out of $\begin{array}{ccc} C & \xrightarrow{\beta} & B \\ \downarrow{\scriptstyle \alpha} & & \\ A & & \end{array}$,

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

Does it follow that C is the pull-back?

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

(40) 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 a concrete description of the direct and projective limit of the system.

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

(42) 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) $I = (p, x)$.

(43) 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 $\varinjlim_{D} A(D)$.

(44) We defined a function v on $\mathbb{Z}_p$ by $v(x) = v((\ldots, x_3, x_2, x_1)) = \max\{n : x_n \equiv 0 \pmod{p^n}\}$. Prove that this is a valuation. Namely, that (i) $v(xy) = v(x) + v(y)$; (ii) $v(x + y) \geq \min\{v(x), v(y)\}$. Prove further that the function $d(x, y) = p^{-v(x-y)}$ is a metric on $\mathbb{Z}_p$.

(45) Prove that every triangle in $\mathbb{Z}_p$ is isosceles and the two equal sides are each bigger or equal to the third. More precisely, given x, y, z, if $d(x, y) < d(x, z)$ then $d(x, z) = d(y, z)$.

(46) Prove that every point in an open ball in $\mathbb{Z}_p$ (relative to the metric) is a centre for the ball.

(47) Let $a(n)$ be a sequence of elements of $\mathbb{Z}_p$. Prove that $a(n)$ converges in $\mathbb{Z}_p$ if it is a Cauchy sequence relative to the metric d. That is, $\mathbb{Z}_p$ is a complete metric space.

(48) Prove that every element x in $\mathbb{Z}_p$ can be written in the form

$$x = a_0 + a_1 p + a_2 p^2 + \ldots,$$

with a_i integers, $0 \leq a_i \leq p - 1$, uniquely determined by x. The precise meaning of that is that the sequence $\sum_{i=0}^{n} a_i p^i \to x$ as $n \to \infty$.

(49) Recall that a consequence of Hensel's lemma was that $\mathbb{Z}_p$ contains the $p-1$-th roots of unity. Take the case $p = 5$. Write down the 4-th roots of unity in $\mathbb{Z}_5$ to several 5-adic digits. Say, at least to 4 digits. That is, if μ is a 4-th root of unity, write $\mu = a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + a_3 \cdot 5^3 + \ldots$, where the a_i are integers, $0 \leq a_i \leq 4$, and find a_0, a_1, a_2, a_3 at the very least.

(50) Let p be an odd prime. Using Hensel's lemma determine which quadratic equations $x^2 + ax + b$, $a, b \in \mathbb{Z}_p$, can be solved in $\mathbb{Z}_p$.

(51) 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 $\exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots$ and $\log(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \ldots$ to define the isomorphisms. Note that you need of course to show that the series converge p-adically on the domains where we consider them. On the other hand, you may use the identity of power series $\exp(\log(1 + x)) = 1 + x$, etc.)

(52) Classify all closed subgroups of $\mathbb{Z}_p \times \mathbb{Z}_\ell$ where $p \neq \ell$ are primes. (Hint: prove first that every such subgroup is an ideal. For that you may wish to show that $\mathbb{Z}$ is dense in $\mathbb{Z}_p \times \mathbb{Z}_\ell$, under the diagonal map $\mathbb{Z} \to \mathbb{Z}_p \times \mathbb{Z}_\ell$.) Construct a Galois extension with Galois group $\mathbb{Z}_p \times \mathbb{Z}_\ell$ and determine the fixed field for each closed subgroup.