EXERCISES FOR THE COURSE MATH 570, FALL 2010

EYAL Z. GOREN

(1) Let G be a group and $H \subset Z(G)$ a subgroup such that G/H is cyclic. Prove that G is abelian. Conclude that every group of order p^2 (p a prime number) is abelian and that the centre of any non-abelian group of order p^3 has p elements.
(2) ($\star$) Let H be a normal subgroup of a p-group G, $H \neq \{e\}$. Prove that $H \cap Z(G) \neq \{e\}$. In particular, one obtains that any normal subgroup with p-elements is contained in $Z(G)$.
(3) 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.
(4) ($\star$) 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.
(5) Show that up to isomorphism there are precisely 5 groups of order 8 given by $\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^3, D_8$ and Q. D_8 is the dihedral group with 8 elements and Q is the quaternion group $\{\pm 1, \pm i, \pm j, \pm k\}$ with $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$ (± 1 commute with any element).
(6) 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.)
(7) ($\star$) Give a formula for the number of roulette (resp. necklace) designs with n sectors (n beads), k of the coloured blue and the rest red. (The symmetry group is $\mathbb{Z}/n\mathbb{Z}$ for the first case, and D_{2n} in the second case.)
(8) ($\star$) Let $p \neq q$ be primes. Prove that a group of order p^2q is not simple. (Hint: assume both p-Sylow and q-Sylow are not normal and count how many elements are accounted for by p and q Sylow subgroups.)
(9) Let $p < q$ be primes such that $p \nmid (q - 1)$. Prove that a group of order pq is necessarily cyclic.
(10) Prove that a group of order pqr is solvable, where $p < q < r$ are primes.
(11) Prove that every group of order less than 60 is solvable.
(12) Show that G is solvable iff it has a normal series with cyclic quotients.
(13) Prove that S_4 is solvable but not supersolvable.
(14) Prove that a nilpotent group is supersolvable but the converse doesn't hold.
(15) ($\star$) Prove that a subgroup and quotient group of a nilpotent group are nilpotent.

(16) Prove that every maximal subgroup of a nilpotent group has index which is a prime power.
(17) Let $G \neq \{e\}$ be a nilpotent group. Prove that every maximal subgroup H of G has index which is a prime and H is normal in G.
(18) Prove that every element w of a free group $\mathscr{F}(X)$ (namely, an equivalence class of words in the alphabet X) has a unique representative of minimal length among all the words in the equivalence class w.
(19) ($\star$) Let $G : \mathbf{Top.Sp.} \to \mathbf{Sets}$ 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.
(20) ($\star$) Write the quaternion group Q of 8 elements in the form $\langle X|R\rangle$. Prove that your presentation is correct!
(21) Based on Zorn's lemma prove that every vector space has a basis. (We shall assume in this course that every two bases of a vector space have the same cardinality).
(22) Let R be a non-zero ring. Based on Zorn's lemma prove that R has a maximal left ideal.
(23) ($\star\star$) Let R be a commutative ring. Let M be a free R-module on a set X and N a free R-module on a set Y. Prove that $M \cong N$ if and only if X and Y have the same cardinality (i.e., there's a bijective function $f : X \to Y$). Hint: reduce to the case of vector spaces making use of the previous exercise.
(24) Give an example of a torsion-free module over an integral domain R which is not free. Can you give such an example which is also finitely generated?
(25) ($\star\star$) Let R be an integral domain and $0 \to M_1 \to M \to M_2 \to 0$ an exact sequence of R-modules of finite rank. Prove that $\mathrm{rk}(M) = \mathrm{rk}(M_1) + \mathrm{rk}(M_2)$.
(26) Let R be an integral domain. Prove that $M \mapsto \mathrm{Tors}(M)$ is a covariant functor from the category of R modules to itself. Is it an exact functor? (Namely, is it the case that $0 \to M_1 \to M \to M_2 \to 0$ exact implies $0 \to \mathrm{Tors}(M_1) \to \mathrm{Tors}(M) \to \mathrm{Tors}(M_2) \to 0$ exact?)
(27) Let $f : \mathbb{Z}^n \to \mathbb{Z}^n$ be a homomorphism represented by a matrix $M \in M_n(\mathbb{Z})$. Assume that $\det(M) \neq 0$. Prove that $[\mathbb{Z}^n : f(\mathbb{Z}^n)] = |\det(M)|$.
(28) Let R be an integral domain and $0 \to M_1 \to M \to M_2 \to 0$ an exact sequence of R-modules. Prove that if M_1 and M_2 are free then so is M.
(29) ($\star\star$) Let $\mathbb{F}$ be a field, V a finite dimensional vector space over $\mathbb{F}$ and $T : V \to V$ a linear transformation. We view V as an $\mathbb{F}[x]$ module where x acts through T. Prove that there is a vector $v \in V$ such that $\{v, Tv, T^2v, \dots T^m v\}$ is a basis for V (for some m) if and only the minimal polynomial of T is equal to its characteristic polynomial.
(30) Let $p(n)$ denote the partition function, $p : \mathbb{N}_0 \to \mathbb{N}$. For a positive integer n, $p(n)$ is the number of ways one can write n as $\lambda_1 + \cdots + \lambda_t$ (for some t), where the λ_i are increasing positive integers.

For example, $p(1) = 1, p(2) = 2, p(3) = 3, p(4) = 5$ and $p(5) = 7$ and the partitions of 5 are $1+1+1+1+1, 1+1+1+2$, $1+1+3, 1+2+2$, $1+4$, $2+3$, 5. Let n be a positive integer and $n = p_1^{a_1} \cdots p_r^{a_r}$ its unique factorization. Prove that the number of abelian groups of order n, up to isomorphism, is $p(a_1) \cdot p(a_2) \cdots p(a_r)$.
(31) Prove that the ring $\mathbb{Z}[i] = \{a + bi : a, b, \in \mathbb{Z}\}$ of Gaussian integers is a principal ideal domain. Suggestion: given an ideal consider a non-zero element z in that ideal of minimal norm $\|z\| = \sqrt{a^2 + b^2}$. Given another non-zero element try to perform "division by z with residue".

Show that the units of $\mathbb{Z}[i]$ are precisely $\{\pm 1, \pm i\}$ and that these are precisely the elements of norm 1. Show that 2 is not a prime in $\mathbb{Z}[i]$. Let $n > 2$ be an integer. Show

that if n is prime in $\mathbb{Z}[i]$ then n is a prime number and is congruent to 3 modulo 4, and vice versa. (You are not supposed to use any result about representation of numbers as a sum of 2 squares.) Hint: in a commutative ring R an ideal (z) is prime if and only if z is prime, if and only if $R/(z)$ is an integral domain; think about $\mathbb{Z}[i]/(p)$ as $(\mathbb{Z}/p\mathbb{Z})[x]/(x^2+1)$, but justify that too.

Conclude now that if n is a prime number congruent to 3 modulo 4 then one cannot write $n = x^2 + y^2$, a sum of squares of integers, but if n is a prime number congruent to 1 modulo 4 then one can in fact write n as a sum of squares. Hint: note that $x^2 + y^2 = (x + iy)(x - iy)$; use unique factorization in the PID $\mathbb{Z}[i]$.

(32) ($\star\star$) Let $\mathbb{F}$ be a field with q elements. Give a formula for the number of conjugacy classes of $n \times n$ matrices with entries in $\mathbb{F}$ for $n = 1, 2, 3$. Based on that, can you can prove a formula for every n?

(33) ($\star\star$) Prove that if F is an additive functor between categories of modules (of either variance) then $F(0) = 0$, where 0 is either the zero module, or the zero homomorphism.

(34) Let R be a commutative ring and let

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0,$$

be a complex of R-modules (that is, $\mathrm{Im}(f) \subseteq \mathrm{Ker}(g)$). Prove that this sequence is exact, if and only if, for every prime ideal $\mathfrak{p}$ of R the localized sequence

$$0 \longrightarrow M_{1,\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} M_{2,\mathfrak{p}} \xrightarrow{g_{\mathfrak{p}}} M_{3,\mathfrak{p}} \longrightarrow 0,$$

is exact. Suggestion: prove first that $\mathrm{Ker}(f)_{\mathfrak{p}} = \mathrm{Ker}(f_{\mathfrak{p}})$ and similar for the image.

(35) Prove that projective and injective limits exist in the category of sets.

(36) Prove that the category of topological spaces has projective and injective limits.

(37) Prove that projective and injective limits exist in the category of groups.

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

(39) Prove that the category of rings does not have injective limits, in general. (The problem is with the identity element!)

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

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

Does it follow that C is the pull-back?

(41) Recall the definition of $\mathbb{Z}_p$ as $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$. We defined

$$\mathrm{val}(\ldots, r_n, \ldots, r_1) = \max\{n : r_n \equiv 0 \pmod{p^n}.$$

Prove that this is a discrete valuation. Namely, that the following holds: (i) $\mathrm{val}(x) < \infty$ if $x \neq 0$; (ii) $\mathrm{val}(x + y) \geq \min\{\mathrm{val}(x), \mathrm{val}(y)\}$ with equality if $\mathrm{val}(x) \neq \mathrm{val}(y)$; (iii) $\mathrm{val}(xy) = \mathrm{val}(x) + \mathrm{val}(y)$.

(42) Prove that in $\mathbb{Z}_p$, $x|y$ if and only if $\mathrm{val}(x) \leq \mathrm{val}(y)$. Deduce that $\mathbb{Z}_p^\times = \{x : \mathrm{val}(x) = 0\}$. Deduce that every ideal of $\mathbb{Z}_p$ is principal and is generated by p^n for a suitable n.

(43) ($\triangle$) 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 prime p. Find in each case the direct and projective limit of the system.

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

(45) ($\triangle$) 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) $I = (p, x)$.

(46) 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 powerseries for $\varinjlim_D A(D)$.

(47) Let R be a PID and Q its quotient ring. Recall that we have unique factorization in both R and Q, similar to the situation for $\mathbb{Z}$ and $\mathbb{Q}$. Prove Gauss' lemma: a monic polynomial $f(x) \in R[x]$ is irreducible in $R[x]$ if and only if it is irreducible in $Q[x]$. (Remark: if you are able to do the proof for $R = \mathbb{Z}$, you'll be able to do it in the general case!)

(48) Let $f(x) \in F[x]$ be a non-zero polynomial of degree d. We say f is separable if f has d distinct roots in some splitting field. Prove that f is separable if and only if $\gcd(f(x), f'(x)) = 1$.

(49) ($\triangle$) Prove that $x^{p^n} - x = \prod f(x)$, where the product is over all irreducible polynomials $f(x) \in \mathbb{F}_p[x]$ of degree d, where d runs over integers dividing n. (Suggestion: use the theory of finite fields!)

(50) ($\triangle$) Let $f(x) \in \mathbb{F}_p[x]$ be a non-zero polynomial of degree r. Then f is irreducible if and only if for all $n \leq r/2$ we have $\gcd(f(x), x^{p^n} - x) = 1$. In particular, f has a root in $\mathbb{F}_p[x]$ if and only if $\gcd(f(x), x^p - x) \neq 1$. (Note that these criteria do not require factoring f!)

(51) The Mobius function μ is defined as follows. It is a function defined on positive integers n and

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & \exists d > 1, d^2 | n \\ (-1)^r & n = p_1 p_2 \cdots p_r \text{ (distinct primes)} \end{cases}$$

Note that μ is a multiplicative function; if $(n, m) = 1$ then $\mu(nm) = \mu(n)\mu(m)$.

Mobius inversion formula: let $f : \mathbb{N}_{>0} \to \mathbb{C}$ be a function. Then,

$$f(n) = \sum_{d|n} F(d)\mu(n/d).$$

Apply this to prove that the number of monic irreducible polynomials of degree n in $\mathbb{F}_p[x]$ is

$$\frac{1}{n}\sum_{d|n} p^d \mu(n/d).$$

(52) Let F be a field. Prove that $F(x)$ is a purely transcendental extension of F.

(53) Let $f(x) \in \mathbb{Q}[x]$ be a cubic irreducible polynomial. Prove that the splitting field of f has degree either 3 or 6 over $\mathbb{Q}$. Give an example of each case.

(54) ($\triangle$) Give an example of a degree 4 irreducible polynomial over $\mathbb{Q}[x]$ whose splitting field has degree: (i) 4; (ii) 8.

(55) Find the degree of the splitting field of the polynomial $x^3 - 3$ over $\mathbb{Q}$, over $\mathbb{Q}[i]$, and over the finite fields with 2, 3, 4, 5, 7 elements. The same with $x^4 - 1$.

(56) ($\triangle$) Let K be a finite extension of F.
   (a) Prove that K is a splitting field over F if and only if every irreducible polynomial in $F[x]$ that has a root in K splits completely in $K[x]$.
   (b) Let K_1, K_2 be finite extensions of F contained in the field K, and assume both are splitting fields over F. Prove that K_1K_2 and $K_1 \cap K_2$ are splitting fields over F.

   (Remark: (b) follows rather easily from (a), and one direction of (a) is easy.)

(57) Calculate the automorphism group $\mathrm{Aut}(K/F)$ for the following pairs of fields. In each case where the extension is a finite Galois extension write the lattice of subgroups and subfields and how they correspond. Also, in these cases, write each field as $F(\alpha)$ for a suitable α and find the minimal polynomial of α over F.
   (1) $F = \mathbb{Q}$ and K the splitting field of $x^3 + 3$.
   (2) $F = \mathbb{Q}$ and K the splitting field of $(x^3 - 1)(x^2 + 3)$.
   (3) $F = \mathbb{Q}$ and K the splitting field of $(x^3 - 1)(x^2 - 3)$.
   (4) $F = \mathbb{C}$ and $K = \mathbb{C}(t)$ (hint: a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ defines an automorphism by $t \mapsto \frac{at+b}{ct+d}$).
   (5) $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{2+\sqrt{2}})$.

(58) Let G be a finite group. Prove that there is a Galois extension of fields K/F such that $\mathrm{Aut}(K/F) \cong G$. (Hint: Show, for example, that S_n acts as automorphisms on the field $\mathbb{Q}(x_1, ..., x_n)$ – the field of fractions of the ring of polynomials in n variables $\mathbb{Q}[x_1, ..., x_n]$.)

(59) Give an example of an extension of fields $K \supset F$ such that $[K : F] = 4$ and such that there is no subfield $K \supset L \supset F$ with $[K : L] = 2$. (Hint: start the construction with a Galois extension of fields whose Galois group is A_4.)

(60) Exhibit an extension like in the previous exercise with $F = \mathbb{Q}$ and K explicitly described as $\mathbb{Q}[x]/(f(x))$.

(61) Construct, for any group G of order less than 9, a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to G.