Math 513. Homework Set 9  
Professor Karen E. Smith  
Due Friday March 23, 2012

1. Classical constructions. (Do not turn in).
   (1) Given a line $L$ and a point $p$, know how to construct a line through $p$ perpendicular to $L$ using straightedge and compass.
   (2) Given a line $L$ and a point $p$ not on $L$, know how to construct a line through $p$ parallel to $L$ using straightedge and compass.
   (3) Given a segment $q_1q_2$ and a point $p$ on a line $L$, know how to construct a segment along $L$ starting at $p$ with the same length as $q_1q_2$.
   (4) Know how to use straightedge and compass to construct a division of a given segment into $n$ congruent segments.
   (5) Given segments of lengths $a$ and $b$, know how to use straightedge and compass to construct segments of lengths $|a \pm b|, ab$ and $a \div b$.
   (6) Know the point of doing (5) in modern language.

2. The field of constructible numbers. Show that there is no irreducible polynomial of degree two with real roots over the field of constructible numbers. (We might say that the field of constructible numbers is “real quadratically closed”).

3. Constructing regular $n$-gons.
   (1) Show that $\alpha = 2\cos(2\pi/5)$ satisfies the polynomial $x^2 + x - 1$.
   (2) Show that a regular pentagon can be constructed with straightedge and compass.
   (3) Show that $\beta = 2\cos(2\pi/7)$ satisfies $x^3 + x^2 - 2x - 1 = 0$.
   (4) Show that the regular heptagon is not constructible.

4. The two uses of the word “minimal polynomial”. Let $F \subset K$ be a field extension of finite degree $n$. Let $\alpha \in K$ be any element.
   (1) Show that “multiplication by $\alpha$” is a $F$-linear map of the $F$-vector space $K$ to itself.
   (2) Let $f(t)$ be the minimal polynomial of the linear transformation described in (1). Show that $\alpha$ is a root of $f(t)$.
   (3) Show that $f(t)$ is irreducible (over $F$).
   (4) Show that $f$ is the minimal polynomial $\alpha$ over $F$ in the sense of field theory.
   (5) Use these ideas to find the minimal polynomial of $1 + 3\sqrt{2} + 3\sqrt{4}$.

5. Derivatives as purely algebraic operators. Let $F[x]$ be a polynomial ring over a field. Consider the linear transformation $\partial$ sending $x^n$ to $nx^{n-1}$. Here we interpret $n$ in the field $F$. Let $f$ and $g$ be polynomials in $F[x]$.
   (1) Show the “Leibnitz rule”: $\partial(fg) = f\partial g + g\partial f$. [Hint: reduce it to checking the case where $f$ and $g$ are monomials.]
   (2) Show that $\partial f^n = nf^{n-1}\partial f$ for all $n \in \mathbb{N}$.
   (3) Show that $\alpha$ is a multiple root of $f$ (meaning that $(x - \alpha)^2$ divides $f$) if and only if $\alpha$ is a root of both $f$ and $\partial f$.
   (4) Find a criterion in terms of $\partial$ for when $\alpha$ is a root of multiplicity $a$ of $f$. 
6. Classification of Finite Fields. Let $\overline{\mathbb{F}}_p$ be an algebraic closure\(^1\) which is unique up to of the field $\mathbb{F}_p$. Let $q = p^n$ for some $n \in \mathbb{N}$.

1. Show that $x^q - x$ factors into distinct linear factors in $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$. [Use 5.]

2. Show that the set of all roots of $x^q - x$ (in $\overline{\mathbb{F}}_p$) forms a subfield of $\overline{\mathbb{F}}_p$ of order $p^n$. Therefore there exists a field of order $p^n$.

3. Let $K$ be a finite field. Show that every element of the group of units $K^\times$ is a root of the polynomial $x^{q-1} - 1$, where $q$ is the order of $K$. [Hint: Recall that $K^\times$ is cyclic.]

4. Let $\alpha$ be a generator for $K^\times$ as a group. Show that $K = \mathbb{F}_p(\alpha)$.

5. Show that any two fields of order $q$ are isomorphic. [Hint: If $K$ and $K'$ show that the minimal polynomial of $\alpha$ over $\mathbb{F}_p$ also has a root in $K'$.]

6. Conclude that there is (up to isomorphism) exactly one field of order $p^n$ as we range over all primes $p$ and all natural numbers $n$.

7. Direct Sums vs Direct Products of $R$-modules. Let $\{M_i\}_{i \in I}$ be a collection of $R$ modules. Let $\bigoplus_{i \in I} M_i$ be the Cartesian product.

1. (Direct Product) Show that the Cartesian product $\Pi_{i \in I} M_i$ is an $R$-module, and that there are $R$-module homomorphisms $\pi_i : \Pi_{i \in I} M_i \to M_i$ satisfying the following “universal property of products:” Given any $R$-module $W$ and $R$-module maps $f_i : W \to M_i$, there is a unique $R$-module map $g : W \to \Pi_{i \in I} M_i$ satisfying $\pi_i \circ g = f_i$ for all $i \in I$. We say $\Pi_{i \in I} M_i$ is a product in the category of $R$-modules.

2. (Direct Sum) Consider the subset $\bigoplus_{i \in I} M_i$ of $\Pi_{i \in I} M_i$ consisting of all $(m_1, m_2, \ldots)$ with the property that $m_i = 0$ for $i \gg 0$. Show that $\bigoplus_{i \in I} M_i$ is a $R$-submodule of $\Pi_{i \in I} M_i$.

3. Let $R = \mathbb{Z}$ and $M_i = \mathbb{Z}/p^i$. Show that every element of $\bigoplus_{i \in I} M_i$ has finite order, but that this is not so for $\Pi_{i \in I} M_i$.

4. Explain why the direct sum does not have the analogous universal property described in (1).

5. Show that there are natural $R$-module maps $\nu_i : M_i \to \bigoplus_{i \in I} M_i$ for all $i \in I$.

6. (Universal property of Coproducts) Show that the direct sum satisfies the following “universal property of coproducts:” Given any $R$-module $W$ and $R$-module maps $f_i : M_i \to W$, there is a unique $R$-module map $g : \bigoplus_{i \in I} M_i \to W$ satisfying $f_i = g \circ \nu_i$ for all $i$. We say that the direct sum $\bigoplus_{i \in I} M_i$ is a co product in the category of $R$-modules.

8. Category Theory. Consider any category, consisting of objects and morphisms (for example, the category $\mathcal{C} top$ whose objects are topological spaces and whose morphisms are continuous maps; or the category $\mathcal{C} ring$ whose objects are rings and morphisms are ring maps; or the category $\mathcal{C} set$ whose objects are sets and whose morphisms are set maps.)

1. With some buddies, think up a bunch more categories; describe the objects and morphisms. [Ideas: topological spaces $(X, x_0)$ with a “marked point,” extensions of $F$, complex representations of a group,...]  

2. A product of objects $\{A_i\}_{i \in I}$ in a category $\mathcal{C}$ is an object $P$, which admits morphism $\pi_i : P \to A_i$ for all $i \in I$, satisfying the following universal property: Given any object $W$ and morphisms $f_i : W \to A_i$ for each $i$, there is a unique morphism $g : W \to P$ satisfying $g \circ \pi_i = f_i$ for all $i \in I$. NOTE: not every category admits products for every collection of objects!

3. Formulate a definition of coproduct in any category.

4. For the categories you’ve identified, think about whether of not they admit products and/or coproducts.

5. Speculate about what a “subcategory” might mean, and give a few examples. One example is that the category of vector spaces over $F$ is a subcategory of abelian groups.

\(^1\)Every field $F$ admits an algebraic closure $\overline{F}$—a field in which every polynomial over $F$ splits completely, but containing no subfield with this same property. The algebraic closure of $F$ is unique up to isomorphism.