Math 422/501: Problem set 5 (due 14/9/09)

Ideals in Rings

Let R be a ring. Recall that an *ideal* $I \lhd R$ is an additive subgroup $I \subset R$ so that $rI \subset I$ for all $r \in R$.

1. (Working with ideals)
   (a) Let $\mathscr{I}$ be a set of ideals in R. Show that $\bigcap \mathscr{I}$ is an ideal.
   (b) Given a non-empty $S \subset R$ show that $(S) \stackrel{\text{def}}{=} \bigcap \{I \mid S \subset I \lhd R\}$ is the smallest ideal of R containing S.
   (c) Show that $(S) = \{\sum_{i=1}^{n} r_i s_i \mid n \geq 0, r_i \in R, s_i \in S\}$.
   (d) Let $a \in R^{\times}$. Show that a is not contained in any proper ideal.
   Hint: Show that $a \in I$ implies $1 \in I$.

2. (Prime and maximal ideals) Call $I \lhd R$ *prime* if whenever $a, b \in R$ satisfy $ab \in I$, we have $a \in I$ or $b \in I$. Call I *maximal* if it is not contained in any proper ideal of R.
   (a) Show that R is an integral domain iff $(0) = \{0\} \lhd R$ is prime.
   (b) Show that $I \lhd R$ is prime iff R/I is an integral domain.
   (c) Show that R is a field iff (0) is its unique ideal (equivalently, a maximal ideal).
   (d) Use the correspondence theorem to show that I is maximal iff R/I is a field.
   (e) Show that every maximal ideal is prime.
   Hint: Every field is an integral domain.

3. (Polynomials and maps of fields) Let $\varphi : F \to K$ be a map of fields, and let $\alpha \in K$.
   (a) Show that φ is injective.
   Hint: consider the kernel of the map.
   (b) Show that there is a unique homomorphism of rings ("evaluation at α") $\tilde{\varphi}_\alpha : F[x] \to K$ compatible with the embedding $F \hookrightarrow F[x]$ so that $\tilde{\varphi}_\alpha(x) = \alpha$. For $f \in F[x]$ we usually write $f(\alpha)$ for $\tilde{\varphi}_\alpha(f)$.
   Hint: Write $\tilde{\varphi}_\alpha$ as the composition of a map $F[x] \to K[x]$ and a map $K[x] \to K$.
   (c) Show that $\tilde{\varphi}_\alpha$ is not injective iff there exists $f \in F[x]$ (or $f \in K[x]$ with coefficients in the image of φ) so that $f(\alpha) = 0$.
   OPTIONAL If $\tilde{\varphi}$ is not injective, show that its kernel is of the form (f) for an irreducible polynomial $f \in F[x]$ and its image is a subfield of K.

4. (The field of rational functions) Let F be a field.
   (a) For $f, g, h, k \in F[x]$ with $g, k \neq 0$ say $\frac{f}{g} \sim \frac{h}{k}$ if $fk = gh$. Show that $\sim$ is an equivalence relation.
   (b) Show that $F(x) = \left\{ \frac{f}{g} \mid f, g \in F[x], g \neq 0 \right\} / \sim$ is a field, and that the natural map $\iota : F[x] \to F(x)$ given by $f \mapsto \frac{f}{1}$ is an embedding.
   (c) $\varphi : F \to K$ be an embedding of fields, and let $\alpha \in K$. Assume that $f(\alpha) \neq 0$ for all non-zero $f \in F[x]$, and show that φ extends uniquely to a map $\tilde{\varphi}_\alpha : F(x) \to K$ so that $\tilde{\varphi}_\alpha(x) = \alpha$.

DEFINITION. Call $\alpha \in K$ *algebraic over* F if the situation of 3(c) holds, *transcendental over* F if the situation of 4(c) holds.

Irreducible polynomials and zeroes

5. Let $f \in \mathbb{Z}[x]$ be non-zero and let $\frac{a}{b} \in \mathbb{Q}$ be a zero of f with $(a,b) = 1$. Show that constant coefficient of f is divisible by a and that the leading coefficient is divisible by b. Conclude that if f is monic then any rational zero of f is in fact an integer.

6. Decide while the following polynomials are irreducible:
   (a) $t^4 + 1$ over $\mathbb{R}$.
   (b) $t^4 + 1$ over $\mathbb{Q}$.
   (c) $t^3 - 7t^2 5 + 3t + 3$ over $\mathbb{Q}$.

7. Show that $t^4 + 15t^3 + 7$ is reducible in $\mathbb{Z}/3\mathbb{Z}$ but irreducible in $\mathbb{Z}/5\mathbb{Z}$. Conclude that it is irreducible in $\mathbb{Q}[x]$.

8. Let $\mathbb{R}$ be the field of real numbers. Let $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$, and define $(a+bi) + (c+di) \stackrel{\text{def}}{=} (a+b) + (c+d)i$, $(a+bi)(c+di) \stackrel{\text{def}}{=} (ac - bd) + (ad + bc)i$.
   (a) Show that the definition makes $\mathbb{C}$ into a ring.
   (b) Show that $\{a + 0i \mid a \in \mathbb{R}\}$ is a subfield of $\mathbb{C}$ isomorphic to $\mathbb{R}$.
   (c) Show that the *complex conjugation* map $\tau(a+bi) = a - bi$ is a field isomorphism $\tau \colon \mathbb{C} \to \mathbb{C}$ which restricts to the identity map on the image of $\mathbb{R}$ from part (b).
   (d) Show that for $z \in \mathbb{C}$ the condition $z \in \mathbb{R}$ and $\tau z = z$ are equivalent. Conclude that $Nz = N_{\mathbb{R}}^{\mathbb{C}} z \stackrel{\text{def}}{=} z \cdot \tau z$ is a multiplicative map $\mathbb{C} \to \mathbb{R}$.
   (e) Show that $\mathbb{C}$ is a field.
   Hint: Show first that if $z \in \mathbb{C}$ is non-zero then Nz is non-zero.

9. (Quadratic equations in $\mathbb{C}$).
   (a) Let $d \in \mathbb{C}$. Show that there exist $z \in \mathbb{C}$ such that $z^2 = d$.
   (b) Let $a, b, c \in \mathbb{C}$ with $a \neq 0$, and let $d = b^2 - 4ac$. Show that the equation $az^2 + bz + c = 0$ has two solutions in $\mathbb{C}$ when $d \neq 0$, and one solution when $d = 0$.

Optional - The field of Laurent series

DEFINITION. Let R be a ring. A *formal Laurent series* over R is a formal sum $f(x) = \sum_{i \geq i_0} a_i x^i$, in other words a function $a\colon \mathbb{Z} \to R$ for which there exists $i_0 \in \mathbb{Z}$ so that $a_i = 0$ for all $i \leq i_0$. We define addition and multiplication in the obvious way and write $R((x))$ for the set of Laurent series. For non-zero $f \in R((x))$ let $v(f) = \min\{i \mid a_i \neq 0\}$ ("order of vanishing at 0"; also set $v(0) = \infty$). Then set $|f| = q^{-v(f)}$ ($|0| = 0$) where $q > 1$ is a fixed real number.

A. Show that $R((x))$ is a ring, and that $R[[x]]$ is a subring.

B. (Invertibility)
   (a) Show that $1 - x$ is invertible in $R[[x]]$.
   Hint: Find a candidate series for $\frac{1}{1-x}$ and calculate the product.
   (b) Show that $R[[x]]^\times = \{a + xf \mid a \in R^\times, f \in R[[x]]\}$.
   (c) Show that $f \in R((x))$ is invertible iff it is non-zero, and
   (d) Show that $F((x))$ is a field for any field F.

C. (Locality) Let F be a field.
   (a) Let $I \lhd F[[x]]$ be a non-zero ideal. Show that $I = x^n F[[x]]$ for some $n \geq 1$.
   Hint: Show that $f \in F[[x]]$ can be written in the form $x^{v(f)} g(x)$ where $g \in F[[x]]^\times$.
   (b) Show that the natural map $F[x]/x^n F[x] \to F[[x]]/x^n F[[x]]$ is an isomorphism.

C. (Completeness)
   (a) Show that $v(fg) = v(f) + v(g)$, equivalently that $|fg| = |f|\,|g|$ for all $f, g \in R((x))$.
   (b) Prove the *ultrametric inequality* $v(f+g) \geq \min\{v(f), v(g)\} \iff |f+g| \leq \max\{|f|, |g|\}$ and conclude that $d(f,g) = |f-g|$ defines a metric on f.
   (c) Show that $\{f_n\}_{n=1}^\infty \subset R((x))$ is a Cauchy sequence iff there exists i_0 such that $v(f_n) \geq i_0$ for all n, and if for each i there exists $N = N(i)$ and $r \in R$ so that for $n \geq N$ the coefficient of x^i in f_n is r.
   (d) Show that $(R((x)), d)$ is complete metric space.
   (e) Show that $R[[x]]$ is closed in $R((x))$.
   (f) Show that $R[[x]]$ is compact iff R is finite.

D. (Ultrametric Analysis) Let $\{a_n\}_{n=1}^\infty \subset R((x))$. Show that $\sum_{n=1}^\infty a_n$ converges in $R((x))$ iff $\lim_{n\to\infty} a_n = 0$.
   Hint: Assume first that $a_n \in R[[x]]$ for all n, and for each k consider the projection of $\sum_{n=1}^N a_n$ to $R[[x]]/x^k R[[x]]$.

E. (The degree valuation) Let F be a field.
   (a) For $f \in F[x]$ set $v_\infty(f) = -\deg(f)$ (and set $v_\infty(0) = \infty$). Show that $v_\infty(fg) = v_\infty(f) + v_\infty(g)$. Show that $v_\infty(f+g) \geq \min\{v_\infty(f), v_\infty(g)\}$.
   (b) Extend v_∞ to the field $F(x)$ of rational functions and show that it retains the properties above. For a rational function f you can think of $v_\infty(f)$ as "the order of f at ∞", just like $v(f)$ measures the order of f at zero.
   (c) Show that the completion of $F(x)$ w.r.t. the metric coming from v_∞ is exactly $R((\frac{1}{x}))$.