**Lior Silberman's Math 501: Problem Set 3 (due 2/10/2020)**

**Fields and extensions**

1. (Concrete extensions) By Eisenstein's criterion and Gauss's Lemma, the polynomials $x^2-2, x^3-2 \in \mathbb{Q}[x]$ are irreducible. Without using tools from abstract algebra (except that a root of an irreducible polynomial isn't also a root of a polynomial of smaller degree):
   (a) Let $K = \mathbb{Q}(\alpha)$ where $\alpha^2 = 2$ (this means: "$K$ is an extension of $\mathbb{Q}$ generated by an element $\alpha$ so that $\alpha^2 = 2$"). Show that $\{1, \alpha\} \subset K$ are linearly independent over $\mathbb{Q}$.
   (b) Show that $\{1, \alpha\}$ spans $K$ (hint: you need to show that the span is a subfield of $K$; start by showing it's a subring). Conclude that $[K : \mathbb{Q}] = 2$.
   (c) Repeat with appropriate modifications for $L = \mathbb{Q}(\beta)$ where $\beta^3 = 2$.

2. (The hard way) Continuing with the notation of proble 1, let $\gamma \in L$ satisfy $\gamma^3 = 2$.
   (a) Write $\gamma = a + b\beta + c\beta^2$ and convert the equation $\beta^3 = 2 = 2 + 0\alpha + 0\alpha^2$ to a system of three non-linear equations in the three variables $a, b, c$ (justify your claim!).
   (b) Taking a clever linear combination of two of the equations, show that $a = 0$.
   (c) Now show that $b = 1$, $c = 0$, that is that $\gamma = \beta$.

3. (The easy way) Let $\gamma \in L$ satisfy $\gamma^3 = 2$ and suppose $\gamma \neq \beta$.
   (a) Show that $\zeta = \gamma/\beta$ satisfies $\zeta^3 = 1$.
   (b) Let $m \in \mathbb{Q}[x]$ be the minimal polynomial of $\zeta$ over $\mathbb{Q}$. Show that $\deg m = 2$.
   *Hint*: Start by showing that $m$ is an irreducible factor of $x^3 - 1$.
   (c) Consider the field $\mathbb{Q}(\zeta) \subset L$. Show that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$ and obtain a contradiction.
   *Hint:* $[L : \mathbb{Q}] = [L : \mathbb{Q}(\zeta)] \cdot [\mathbb{Q}(\zeta) : \mathbb{Q}]$.

*4. Let $K = \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Show that $K = L$.

**Fields of fractions**

5. Let $R$ be an integral domain.
   (a) Consider the set $X$ of *formal expresions* $\frac{a}{b}$ where $a, b \in R$ and $b \neq 0$. Define a relation on $X$ by $\frac{a}{b} \sim \frac{c}{d}$ if $ad = bc$. Show that this is an equivalence relation.
   (b) Let $F$ be the set $X/\sim$ of equivalence relations, and define operations on $F$ by $\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad+bc}{bd}\right]$, $\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] = \left[\frac{ac}{bd}\right]$. Show that these are well-defined and give $F$ the structure of a ring.
   (c) Show that $F$ is a field, and that $a \mapsto \left[\frac{a}{1}\right]$ defines an embedding $\iota \colon R \to F$.
   DEF $F$ is called the *field of fractions* of $R$. If $K$ is a field, the field of fractions of the polynomial ring $K[x]$ is called the *field of rational functions* (in one variable) *over* $K$ and denoted $K(x)$.
   (d) Show that for any field $K$, any injective ring homomorphism $\iota \colon R \to K$ extends uniquely to a homomorphism $F \to K$ compatible with $\iota$.

6. Fix an extension of fields $\iota \colon K \to L$.
   (a) Carefully show that for any $\alpha \in L$ there is a unique homomorphism of rings $\psi_\alpha \colon K[x] \to L$ ("evaluation at $\alpha$") restricting to $\iota$ on $K$ and satisfying $\psi_\alpha(x) = \alpha$.
   (b) Suppose that $\alpha$ is transcendental over $K$. Show that $\iota$ extends uniquely to a map $\tilde{\psi}_\alpha \colon K(x) \to L$ so that $\tilde{\psi}_\alpha(x) = \tilde{\psi}_\alpha(\frac{x}{1}) = \alpha$.

**Supplement I: the two quadratic** $\mathbb{R}$-algebras

A. Let $i$ be a formal symbol, and let $\mathbb{C}$ be the set of formal expressions $a + bi$ where $a, b \in \mathbb{R}$. Set $(a+bi) + (c+di) \stackrel{\text{def}}{=} (a+c) + (b+d)i$ and $(a+bi) \cdot (c+di) \stackrel{\text{def}}{=} (ac-bd) + (ad+bc)i$.
   (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 ring 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.

B. Let $\mathbb{R}$ be the field of real numbers. Let $A = \{a + bi \mid a, b \in \mathbb{R}\}$ where $i$ is a formal symbol, and define $(a+bi) + (c+di) \stackrel{\text{def}}{=} (a+b) + (c+d)i$, $(a+bi)(c+di) \stackrel{\text{def}}{=} (ac + 2bd) + (ad + bc)i$.

(a) Show that the definition makes $A$ into a ring.
(b) Show that $\{a + 0i \mid a \in \mathbb{R}\}$ is a subfield of $A$ isomorphic to $\mathbb{R}$.
(c) Show that the *complex conjugation* map $\tau(a + bi) = a - bi$ is a ring isomorphism $\tau \colon A \to A$ which restricts to the identity map on the image of $\mathbb{R}$ from part (b).
(d) Show that for $z \in A$ the condition $z \in \mathbb{R}$ and $\tau z = z$ are equivalent. Conclude that $Nz = N_{\mathbb{R}}^{A} z \stackrel{\text{def}}{=} z \cdot \tau z$ is a multiplicative map $A \to \mathbb{R}$.
(e) Show that $A \simeq \mathbb{R} \oplus \mathbb{R}$, and in particular that it is not a field.
(f) Assume that multiplication is defined by $(a+bi)(c+di) \stackrel{\text{def}}{=} (ac + tbd) + (ad + bc)i$ for some fixed $t \in \mathbb{R}$. For which $t$ is the algebra a field? Find the isomorphism class of the algebra, depending on $t$.

## Supplement II: More on 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.

C. (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 $a_{v(f)} \in R^\times$.
(d) Show that $F((x))$ is a field for any field $F$.

D. (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 every nonzero $f \in F[[x]]$ can be uniquely 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.

E. (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.

F. (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 $R[[x]]/x^k R[[x]]$.

G. (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 $v_\infty$ 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 $\infty$", 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 $v_\infty$ is exactly $R((\frac{1}{x}))$.