MATH3195/5195M EXERCISE SHEET 2
SOLUTIONS

DUE: FEBRUARY 19, 2020

Problem 1. *Monomial orders:* Show that $<_{lex}$ is a monomial order on $K[x_1, \dots, x_n]$ (or equivalently, on $\mathbb{N}^n$).

Solution. We have to show that $<_{lex}$ is a total order on $\mathbb{N}^n$ (or equivalently on $K[x_1, \dots, x_n]$ - we will work with $\mathbb{N}^n$) and conditions (i) and (ii) from the lecture are satisfied. For the first assertion, let $\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$. We use induction on n: if $n = 1$, then $<_{lex}$ is the natural order on $\mathbb{N}$, which is a total order. Assume that $<_{lex}$ is a total order on $\mathbb{N}^{n-1}$, then either $(\alpha_1, \dots, \alpha_{n-1}) <_{lex}$ or $>_{lex}$ or $= (\beta_1, \dots, \beta_{n-1})$. In the first two cases, this implies that $\alpha <_{lex}$ or $>_{lex}$ β, for the last case, if $\alpha_n <$ or $>$ or $= \beta_n$, then $\alpha <_{lex}$ or $>_{lex}$ or $= \beta$.
For condition (i), we have to show that if $\alpha <_{lex} \beta$ in $\mathbb{N}^n$ and $\gamma \in \mathbb{N}^n$ is arbitrary, then $\alpha + \gamma <_{lex} \beta + \gamma$. For this assume that $\alpha_i = \beta_i$ and $\alpha_j < \beta_j$ for all $i < j$ and a fixed $1 \leq j \leq n$. Now $(\alpha + \gamma)_i = \alpha_i + \gamma_i$ and $(\beta + \gamma)_i = \beta_i + \gamma_i$, so $(\alpha + \gamma)_i = (\beta + \gamma)_i$ for any $i < j$ and $(\alpha + \gamma)_j = \alpha_j + \gamma_j < \beta_j + \gamma_j = (\beta + \gamma)_j$ since $\alpha_j < \beta_j$.
Condition (ii) says that $<_{lex}$ is a well-ordering on $\mathbb{N}^n$. This can be shown by induction and using that the integers are well-ordered: for $n = 1$ this is precisely the claim that $\mathbb{N}$ is well-orderd. Assume now that $A \subseteq \mathbb{N}^n$ is a non-empty subset and define $A_1 = \{\alpha \in A : \alpha_1 \text{ is minimal}\}$. Then $A_1 \neq \varnothing$ (since $\mathbb{N}$ is well-ordered). Now define $A_2 = \{\alpha \in A_1 : \alpha_2 \text{ is minimal}\}$. Again, this set is non-empty. Continue until $A_n = \{\alpha\} = \min_{<_{lex}}(A)$.

Problem 2. (a) Show that $\mathbb{R}[x, y]/(x^3 - y^2)$ is isomorphic to $\mathbb{R}[t^2, t^3]$. [Hint: First homomorphism theorem. First show that $f(x, y) = x^3 - y^2$ is in the kernel of the map φ as defined in the lecture. In order to see that $(f(x, y))$ is the full kernel, you may use the fact, that the kernel of φ is generated by elements of the form $x^a y^b - x^{a'} y^{b'}$, where $a, a', b, b' \in \mathbb{N}$. This fact can be proved using Gröbner bases methods]

(b) Is $(x^3 - y^2)$ a prime ideal in $\mathbb{R}[x, y]$? Explain!

(a) Define $\varphi : \mathbb{R}[x, y] \to \mathbb{R}[t]$ by $\varphi(x) = t^2$ and $\varphi(y) = t^3$. The image of φ is the subring of $\mathbb{R}[t]$ generated by t^2 and t^3, that is, the ring $\mathbb{R}[t^2, t^3]$. Then by the first homomorphism theorem, $\operatorname{im}(\varphi) = \mathbb{R}[t^2, t^3] \cong \mathbb{R}[x, y]/\ker \varphi$. It remains to determine $\ker \varphi$. The element $f(x, y) = x^3 - y^2$ is in $\ker \varphi$ since $\varphi(f(x, y)) = f(t^2, t^3) = (t^2)^3 - (t^3)^2 = 0$. Now use the hint, which says that $\ker \varphi = (x^a y^b - x^{a'} y^{b'}$, where a, a', b, b' are some integers $\in \mathbb{N}$). Assume that $g(x, y) = x^a y^b - x^{a'} y^{b'}$ is in $\ker \varphi$, that means that $t^{2a+3b} - t^{2a'+3b'} = 0$. So we are looking for all integer linear combinations such that $2a + 3b = 2a' + 3b'$, or $2(a - a') = 3(b' - b)$. We may assume w.l.o.g. that $a > a'$ and hence $b' > b$ (if $a = a'$ we would get $b = b'$ and the binomial would be 0). Since $a - a'$ and $b' - b$ are integers and 2 and 3 are coprime, the above equation implies that $3|(a - a')$ and $2|(b' - b)$. Thus $a - a' = 3k$, which implies that $b' - b = 2k$ for some $k \in \mathbb{N}_{>0}$. Thus any $g(x, y)$ in $\ker \varphi$ is of the form $x^{a'+3k} y^{b'-2k} - x^{a'} y^{b'} = x^{a'} y^{b'-2k}(x^{3k} - y^{2k})$. Since $x^{3k} - y^{2k} = (x^3)^k - (y^2)^k = (x^3 - y^2)(\sum_{i=0}^{k-1} x^{3i} y^{2(k-1-i)})$, one sees that $f(x, y)|g(x, y)$, which means that $g(x, y) \in (f(x, y))$. Thus $\ker \varphi = (x^3 - y^2)$ and the first isomorphism theorem shows that $\mathbb{R}[t^2, t^3] \cong$

$\mathbb{R}[x,y]/(x^3-y^2)$.
(b) Since $\mathbb{R}[t^2,t^3]$ is a subring of the integral domain $\mathbb{R}[t]$, it is itself an integral domain (if we had $a(t^2,t^3)b(t^2,t^3)=0$, then since both $a,b\in\mathbb{R}[t]$, this implies that either a or b is 0). By (a) $\mathbb{R}[x,y]/(x^3-y^2)\cong\mathbb{R}[t^2,t^3]$, hence $\mathbb{R}[x,y]/(x^3-y^2)$ is an integral domain. By the theorem from the lecture (x^3-y^2) is a prime ideal in $\mathbb{R}[x,y]$.

Problem 3. (a) Show that the ideal $(x^4-5x^3+7x^2-5x+6, x^4+2x^2+1, x^4-2x^3+x^2-2x)$ in $\mathbb{R}[x]$ is maximal.
(b) Let R be a ring such that every element satisfies $x^n=x$ for some $n>1$ (here the integer n depends on x). Show that every prime ideal in R is maximal.

(a) If $(f(x),g(x),h(x))$ is an ideal in $K[x]$, where K is a field, then one can see that $(f(x),g(x),h(x))=(\gcd(f,g,h))$.
We first calculate the factorizations of the polynomials $f(x)=x^4-5x^3+7x^2-5x+6=(x-2)(x-3)(x^2+1)$, $g(x)=x^4+2x^2+1=(x^2+1)^2$ and $h(x)=x^4-2x^3+x^2-2x=x(x-2)(x^2+1)$ into irreducible polynomials in $\mathbb{R}[x]$ (use e.g. rational root test). Thus we see that the gcd of $f(x),g(x),h(x)$ is x^2+1 and $(f(x),g(x),h(x))=(x^2+1)$. But x^2+1 is irreducible in $\mathbb{R}[x]$, thus $\mathbb{R}[x]/(x^2+1)$ is a field. This means that (x^2+1) is a maximal ideal in $\mathbb{R}[x]$.
(b) Let $\mathfrak{p}\subseteq R$ be a prime ideal and let $x\in R\backslash\mathfrak{p}$ with $x^n=x$ for some $n>1$. Since $\mathfrak{p}$ is prime, $R/\mathfrak{p}$ is an integral domain and $\bar{x}\neq\bar{0}$ is a nonzero-divisor. Then from the equation $\bar{x}^n-\bar{x}=\bar{x}(\bar{x}^{n-1}-\bar{1})=\bar{0}$ we can cancel $\bar{x}$ and obtain $\bar{x}^{n-1}=\bar{1}$. But this means that $\bar{x}\bar{x}^{n-2}=\bar{1}$, that is, $\bar{x}^{n-2}$ is a multiplicative inverse of $\bar{x}$. Thus any element $\bar{x}\neq\bar{0}\in R/\mathfrak{p}$ is invertible, which implies that $R/\mathfrak{p}$ is a field. But then (as shown in the lecture) $\mathfrak{p}$ is a maximal ideal.

Problem 4. (a) Consider $K[x,y,z]$ and order all monomials of degree less than or equal to 3 with respect to the following monomial orders: (i) $<_{lex}$, (ii) $<_{deglex}$, (iii) $<_\lambda$, where λ is a suitable linear form $\lambda:\mathbb{R}^3\to\mathbb{R}$.
(b) Determine leading monomial and coefficient of the polynomial $f=x^4+z^5+x^3z+yz^4+x^2y^2$ with respect to the momomial orders from (a).

Solution. (a) All monomials of degree ≤ 2 are: $1,x,y,z,x^2,xy,xz,yz,y^2,z^2$.The orders are:
(i) $1<_{lex} z<_{lex} z^2<_{lex} y<_{lex} yz<_{lex} y^2<_{lex} x<_{lex} xz<_{lex} xy<_{lex} x^2$
(ii) $1<_{deglex} z<_{deglex} y<_{deglex} x<_{deglex} z^2<_{deglex} yz<_{deglex} y^2<_{deglex} xz<_{deglex} xy<_{deglex} x^2$.
(iii) We have to choose a λ with $\mathbb{Q}$-linearly independent entries. Take e.g. $\lambda=(1,\sqrt{2},\sqrt{5})$. Then
$1<_\lambda x<_\lambda y<_\lambda z<_\lambda x^2<_\lambda xy<_\lambda y^2<_\lambda xz<_\lambda yz<_\lambda z^2$.
(b) (i) $lm_{lex}(f)=x^4$ and $lc_{lex}(f)=1$, (ii) $lm_{deglex}(f)=yz^4$ and $lc_{lex}(f)=1$, (ii) with λ from above $lm_\lambda(f)=z^5$ and $lc_\lambda(f)=1$.

Problem 5. Let R be a ring. Show that R is local if and only if the nonunits of R form a maximal ideal.

Solution. Let R be local, that is, there is a unique maximal ideal $\mathfrak{m}\subseteq R$. Denote $S=\{\text{ nonunits of } R\}$. We have to show that S is an ideal. Let $s,t\in S$. Then $\langle s\rangle+\langle t\rangle$ is an ideal and clearly $\langle s\rangle\subseteq\mathfrak{m}$ and $\langle t\rangle\subseteq\mathfrak{m}$. But this implies that $s-t\in\mathfrak{m}$. If $s\in S$ and $r\in R$, then $rs\in\mathfrak{m}$ since $s\in\mathfrak{m}$, thus S is an ideal in R. If $S\subsetneq\mathfrak{m}$, then there would exist a unit in $\mathfrak{m}$ (by definition of S). But this would mean that $\mathfrak{m}=R$, contradiction to the fact that $\mathfrak{m}$ is a proper ideal of R.
For the other direction, assume that S is a maximal ideal in R.This means that S is a proper ideal of R. Let M be an arbitrary maximal ideal of R. Then every element of M has to be a non-unit of R (since M is supposed to be proper). This implies that $M\subseteq S$ and by maximality, $M=S$.

Problem 6. Let I be an ideal of R and A be a multiplicatively-closed subset of R. Show that:

(a) $A^{-1}I$ is an ideal of $A^{-1}R$;
(b) $\frac{x}{a} \in A^{-1}I$ if and only if there is some $b \in A$ with $xb \in I$;
(c) $A^{-1}I = A^{-1}R$ if and only if $I \cap A \neq \emptyset$;
(d) localization commutes with quotients, that is

$$A^{-1}R/A^{-1}I \cong \overline{A}^{-1}(R/I), \text{ where } \overline{A} = \{a + I : a \in A\}.$$

Solution. (a) Firstly, since $0 \in I$ and $1 \in A$ we have $\frac{0}{1} \in A^{-1}I$. Now suppose that $\frac{r}{a}, sb \in A^{-1}I$, then $\frac{r}{a} - \frac{s}{b} = \frac{rb-sa}{ab}$. Since $r, s \in I \subseteq R$ we have $rb - sa \in I$, and since A is multiplicatively closed we have $ab \in A$. Thus $\frac{r}{a} - \frac{s}{b} \in A^{-1}I$. Finally if $\frac{t}{c} \in A^{-1}R$ then $\frac{t}{c}\frac{r}{a} = \frac{tr}{ac}$, and again since $tr \in I$ and $ac \in A$ we have $\frac{t}{c}\frac{r}{a} \in A^{-1}I$, so $A^{-1}I \subseteq A^{-1}R$.
(b) If $\frac{x}{a} \in A^{-1}I$ then setting $b = 1$ gives the result. Conversely if $xb \in I$ then $\frac{xb}{ab} \in A^{-1}I$, but $\frac{xb}{ab} = \frac{x}{a}$.
(c) Suppose $A^{-1}I = A^{-1}R$, then $1_{A^{-1}R} = \frac{1}{1} \in A^{-1}I$. By (b), this implies that there is some $b \in A$ with $1 \cdot b \in I$, i.e. $I \cap A \neq \emptyset$. Conversely if $I \cap A \neq \emptyset$ then choose $a \in I \cap A$. Now $\frac{a}{a} \in A^{-1}I$, but $\frac{a}{a} = \frac{1}{1} = 1_{A^{-1}R}$, so $A^{-1}I = A^{-1}R$.
(d) Define $\phi : A^{-1}R \to \bar{A}^{-1}(R/I)$ by $\phi(\frac{r}{a}) = \frac{r+I}{a+I}$. It is easy to check that ϕ is well-defined. This map is a homomorphism as given $\frac{r}{a}, \frac{s}{b} \in A^{-1}R$ we have

$$\begin{aligned}
\phi\left(\frac{r}{a} + \frac{s}{b}\right) &= \phi\left(\frac{rb+sa}{ab}\right) \\
&= \frac{(rb+sa)+I}{ab+I} \\
&= \frac{(r+I)(b+I)+(s+I)(a+I)}{(a+I)(b+I)} \\
&= \frac{r+I}{a+I} + \frac{s+I}{b+I} \\
&= \phi\left(\frac{r}{a}\right) + \phi\left(\frac{s}{b}\right), \\
\phi\left(\frac{r}{a}\frac{s}{b}\right) &= \phi\left(\frac{rs}{ab}\right) \\
&= \frac{rs+I}{ab+I} \\
&= \frac{(r+I)(s+I)}{(a+I)(b+I)} \\
&= \frac{r+I}{a+I}\frac{s+I}{b+I} \\
&= \phi\left(\frac{r}{a}\right)\phi\left(\frac{s}{b}\right), \text{ and} \\
\phi(1_{A^{-1}R}) &= \phi\left(\frac{1}{1}\right) \\
&= \frac{1+I}{1+I} \\
&= 1_{\bar{A}^{-1}(R/I)}.
\end{aligned}$$

Also ϕ is clearly surjective, and $\phi(\frac{r}{a}) = \frac{r+I}{a+I} = \frac{I}{1+I}$ iff there is some $c + I \in \bar{A}$ such that $(r + I)(1 + I)(c + I) = I(a + I)(c + I)$, that is iff there is some $c \in A$ such that $rc \in I$. By part (b) this is iff $\frac{r}{a} \in A^{-1}I$, so $\ker \phi = A^{-1}I$. By the first isomorphism theorem the result follows.