Algebra I - Homework 7

Pablo Sánchez Ocal

November 14th, 2016

Exercise 1

Let $f : R \longrightarrow S$ be a homomorphism of commutative rings, $P \subset S$ a prime ideal, $M \subset S$ a maximal ideal. First, we remark that for any ideal $I \subset S$ we have that $f^{-1}(I) \subset R$ is an ideal, since for all $a, b \in f^{-1}(I)$ and $r \in R$ we have: $f(a-b) = f(a) - f(b) \in I$ and $f(ra) = f(r)f(a) \in I$ (because I is an ideal). Now:

1. Prove that $f^{-1}(P) \subset R$ is prime: let $r_1, r_2 \in R$ with $r_1 r_2 \in f^{-1}(P)$, we have $f(r_1)f(r_2) = f(r_1 r_2) \in P$ thus since P is prime we must have $f(r_1) \in P$ or $f(r_2) \in P$ hence $r_1 \in f^{-1}(P)$ or $r_2 \in f^{-1}(P)$, meaning that $f^{-1}(P)$ is prime.

2. Let f be surjective, prove that $f^{-1}(M) \subset R$ is maximal: consider the natural surjective (because f is surjective) map:

$$\begin{array}{cccccc} \tilde{f} & : & R & \longrightarrow & S/M \\ & & r & \longmapsto & f(r) \end{array}$$

   we have that $\ker(\tilde{f}) = \{r \in R : f(r) \in M\} = f^{-1}(M)$, hence by the First Isomorphism Theorem $R/f^{-1}(M) \cong S/M$. Now M maximal and S commutative implies that S/M is a field, thus $R/f^{-1}(M)$ is in particular a division ring hence $f^{-1}(M)$ is maximal.

Exercise 2

Let R be a commutative ring, $S \subset R$ a multiplicative set not containing 0.

1. Prove using Zorn's Lemma that there exists an ideal $I \subset R$ maximal among the ideals not intersecting S. Consider the set $\{J \subset R : J \text{ ideal}, J \cap S = \emptyset\}$ (which is non empty since it contains $\{0\}$) and a chain of elements belonging to such set: $J_0 \supset \cdots \supset J_n \supset \cdots$, we have that $J = \cup_{i=0}^{\infty} J_i$ is an ideal since for any $a, b \in J$ and $r \in R$ we must have $a, b \in J_n$ (for certain $n \in \mathbb{N}$) an ideal, in particular $a - b \in J_n \subset J$ and $ra \in J_n \subset J$. Since none of the J_i for $i \geq 0$ intersects S, we have that $J \cap S = \emptyset$ hence every chain has an upper bound. By Zorn's Lemma, there exists I a maximal element in the set $\{J \subset R : J \text{ ideal}, J \cap S = \emptyset\}$.

2. Prove that I as above is prime. Suppose there are ideals $A, B \subset R$ with $AB \subset I$. Note that since S is a multiplicative set, we must have $A \cap S = \emptyset$ and $B \cap S = \emptyset$: if there is $s \in A \cap S$ then for every $t \in I$ we have $st \in I \cap S = \emptyset$, a contradiction (and similarly for $s \in B \cap S$). Notice that $I \subset I + A$ and $I \subset I + B$ with $(I + A) \cap S = \emptyset$ $(I + B) \cap S = \emptyset$, both $I + A$ and $I + B$ being ideals since they are sum of ideals. Since I is maximal in the set $\{J \subset R : J \text{ ideal}, J \cap S = \emptyset\}$, we must have that either $I + A = I$ or $I + A = R$ in the first case and either $I + B = I$ or $I + B = R$ in the second case. If we have $I + A = I$ or $I + B = I$ this means that $A \subset I$ or $B \subset I$, obtaining that I is prime.

   We now prove that we cannot have $I + A = R = I + B$ (and hence the case above always happens, obtaining that I is indeed prime). Suppose we have $I + A = R = I + B$, since $1 \in R$ there exist $a \in A \backslash P$, $b \in B \backslash P$, $p_a, p_b \in I$ with $p_1 + a = 1 = p_2 + b$. Thus:
   $$1 = (p_1 + a)(p_2 + b) = p_1 p_2 + p_1 b + p_2 a + ab \in I,$$
   since I ideal means the first three terms belong to I and since $AB \subset I$ we have $ab \in I$. But now I is an ideal containing 1, thus $r = r1 \in I$ for every $r \in R$ thus $I = R$, which is a contradiction because $I \cap S = \emptyset$. Thus we cannot have $I + A = R = I + B$.

Exercise 3

Prove that the ring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is an Euclidean domain. That is, we want to see that it has no zero divisors and that there is a function $\varphi : \mathbb{Z}[i] \setminus \{0\} \longrightarrow \mathbb{N}$ such that for $a, b \in \mathbb{Z}[i]$, if $ab \neq 0$ we have $\varphi(a) \leq \varphi(ab)$ and if $b \neq 0$ there exist $q, r \in \mathbb{Z}[i]$ with $a = qb + r$ with $r = 0$ or $r \neq 0$ and $\varphi(r) < \varphi(b)$.

First, note that $\mathbb{Z}[i] \subset \mathbb{C}$, thus we will use for $z = z_1 + iz_2 \in \mathbb{Z}[i]$ the function $\varphi(z) = |z|^2 = z_1^2 + z_2^2$ (that is $|\cdot|$ being the usual norm of complex numbers) for $z \in \mathbb{Z}[i]$ (since $z_1, z_2 \in \mathbb{Z}$ we have $z_1^2 + z_2^2 \in \mathbb{N}$). In particular if we have $z, w \in \mathbb{Z}[i]$ with $zw = 0$, this means $|z|^2|w|^2 = |zw|^2 = 0$ hence $|z|^2 = 0$ or $|w|^2 = 0$ hence $z = 0$ or $w = 0$, so in particular $\mathbb{Z}[i]$ is an integral domain (a consequence of being a subring of $\mathbb{C}$).

Suppose we have $a, b \in \mathbb{Z}[i]$ with $ab \neq 0$. This means that $a \neq 0 \neq b$ and hence $|a|^2 \geq 1$ and $|b|^2 \geq 1$. Thus $\varphi(ab) = |ab|^2 = |a|^2|b|^2 \geq |a|^2 = \varphi(a)$ and φ satisfies the first property.

Suppose we have $a, b \in \mathbb{Z}[i]$ with $b \neq 0$. Consider the multiples of b in $\mathbb{Z}[i]$, that is: $\{kb : k \in \mathbb{Z}[i]\}$. They form a grid in the complex plane $\mathbb{C}$ centered at 0, the squares of such grid having vertexes kb, $(k+1)b$, $(k+1+i)b$, $(k+i)b$ in counterclockwise order for certain $k \in \mathbb{Z}[i]$, having sides of length $\varphi(b)$. Since $a \in \mathbb{C}$, it belongs to one of such squares, say the one delimited by the vertexes $\tilde{q}b$, $(\tilde{q}+1)b$, $(\tilde{q}+1+i)b$, $(\tilde{q}+i)b$ for some $\tilde{q} \in \mathbb{Z}[i]$. Now, a must be closer to at least one of the vertexes (if it is to more than one, just choose one of them) than to the rest, say that such vertex is qb for some $q \in \mathbb{Z}[i]$. Notice that the maximum distance that a can be to those vertexes is when it is just in the center of the square, and in such case said distance is no more than $\varphi(b)/\sqrt{2} < \varphi(b)$. Hence $\varphi(a - qb) < \varphi(b)$. Thus defining $r = a - qb \in \mathbb{Z}[i]$ because $a, q, b \in \mathbb{Z}[i]$ (notice that we can have $r = 0$), we obtain that φ satisfies the second property.

Hence $\mathbb{Z}[i]$ satisfies all the required properties and thus it is an Euclidean domain.

Exercise 4

Let R be an integral domain, S a multiplicative subset not containing 0. Prove that $S^{-1}R$ is isomorphic to a subring of the field of fractions of R. We denote such field $Q(R) = (R \setminus \{0\})^{-1}R$. Consider the natural function:

$$\begin{array}{cccc} f & : & S^{-1}R & \longrightarrow & Q(R) \\ & & r/s & \longmapsto & r/s \end{array}$$

we will see that it is a well defined injective morphism, thus by the First Isomorphism Theorem we will obtain that $S^{-1}R \cong \mathrm{im}(f)$ which is a subring of $Q(R)$.

1. It is well defined: if we have $r_1/s_1 \sim r_2/s_2$ in $S^{-1}R$ this means that there is $s \in S$ with $s(r_1s_2 - r_2s_1) = 0$, and since S does not contain 0, we have $s \in R \setminus \{0\}$ thus we have $r_1/s_1 \sim r_2/s_2$ in $Q(R)$ and f is well defined (notice that this function is well defined in every localization: we have not used that R is an integral domain).

2. It is injective: if we have $r_1/s_1, r_2/s_2 \in S^{-1}(R)$ with $f(r_1/s_1) = f(r_2/s_2)$ this means that we have $r_1/s_1 \sim r_2/s_2$ in $Q(R)$, that is there exists $r \in R \setminus \{0\}$ with $r(r_1s_2 - r_2s_1) = 0$, and since R is an integral domain we must have $r_1s_2 - r_2s_1 = 0$, in particular for every $s \in S$ we have $s(r_1s_2 - r_2s_1) = 0$ thus $r_1/s_1 \sim r_2/s_2$ in $S^{-1}R$ and f is injective.

3. It is a morphism (we use indistinctively the multiplication and addition defined in both localizations without explicit distinction, the context indicates if we are in $S^{-1}(R)$ or $Q(R)$, and when these operations can be done in $S^{-1}R$ then they also hold in $Q(R)$ because, as noticed when proven that f is well defined, $s \in S \subset R \setminus \{0\}$) since for every $r_1/s_1, r_2/s_2 \in S^{-1}(R)$ we have:

$$f\left(\frac{r_1}{s_1}\frac{r_2}{s_2}\right) = f\left(\frac{r_1r_2}{s_1s_2}\right) = \frac{r_1r_2}{s_1s_2} = \frac{r_1}{s_1}\frac{r_2}{s_2} = f\left(\frac{r_1}{s_1}\right)f\left(\frac{r_2}{s_2}\right)$$

$$f\left(\frac{r_1}{s_1} + \frac{r_2}{s_2}\right) = f\left(\frac{r_1s_2 + r_2s_1}{s_1s_2}\right) = \frac{r_1s_2 + r_2s_1}{s_1s_2} = \frac{r_1}{s_1} + \frac{r_2}{s_2} = f\left(\frac{r_1}{s_1}\right) + f\left(\frac{r_2}{s_2}\right)$$

as desired.

Hence by the First Isomorphism Theorem $S^{-1}R \cong \mathrm{im}(f)$ a subring of $Q(R)$.

Exercise 5

Let R be a commutative ring, $I \subset R$ an ideal, $(I) \subset R[x]$ generated by I. Prove that $R[x]/(I) \cong (R/I)[x]$. Consider the natural function:

$$\begin{array}{cccc} \varphi & : & R[x] & \longrightarrow & (R/I)[x] \\ & & f(x) & \longmapsto & \overline{f(x)} \end{array}$$

where given $f(x) = a_0 + \cdots + a_n x^n$ with $a_i \in R$ for $0 \leq i \leq n$ we obtain $\overline{f(x)} = \overline{a_0} + \cdots + \overline{a_n} x^n$ with $\overline{a_i} \in R/I$ for $0 \leq i \leq n$. Recall the basic operations that make R/I a ring, namely in this notation for $r_1, r_2 \in R$ we have $\overline{r_1} + \overline{r_2} = \overline{r_1 + r_2}$ and $\overline{r_2}\,\overline{r_2} = \overline{r_1 r_2}$. Clearly φ is well defined since we can always consider the projection of the coefficients from R onto R/I and this is a polynomial. Moreover, given any polynomial $\overline{f(x)} \in (R/I)[x]$, say $\overline{f(x)} = \overline{a_0} + \cdots + \overline{a_n} x^n$ with $\overline{a_i} \in R/I$ for $0 \leq i \leq n$, we have that $\varphi(f(x)) = \overline{f(x)}$ for $f(x) = a_0 + \cdots + a_n x^n$ with $a_i \in R$ for $0 \leq i \leq n$, hence φ is surjective.

We have that φ is a morphism since for $f(x) = a_0 + \cdots + a_n x^n$ and $g(x) = b_0 + \cdots + b_n x^n$ with $a_i b_i \in R$ for $0 \leq i \leq n$ (adding zero coefficients to equalize the degree if necessary), we have:

$$\varphi(f(x) + g(x)) = \overline{a_0} + \overline{b_0} + \cdots + \overline{a_n} x^n + \overline{b_n} x^n = \varphi(f(x)) + \varphi(g(x))$$
$$\varphi(f(x)g(x)) = \sum_{k=0}^{n} x^k \sum_{i+j=k} \overline{a_i b_j} = \sum_{k=0}^{n} x^k \sum_{i+j=k} \overline{a_i}\,\overline{b_j} = \varphi(f(x))\varphi(g(x)).$$

We now compute the kernel of φ, we claim that $\ker(\varphi) = (I)$ (recall R commutative, thus the elements of (I) have a nice expression as finite sums):

$\subseteq$) Suppose we have $f(x) = a_0 + \cdots + a_n x^n$ with $a_i \in R$ for $0 \leq i \leq n$ (that is $f(x) \in R[x]$) with $\varphi(f(x)) = 0$, that is $\overline{f(x)} = \overline{a_0} + \cdots + \overline{a_n} x^n = 0$ hence $\overline{a_i} = 0$ for $0 \leq i \leq n$. This means that $a_i \in I$ for $0 \leq i \leq n$, thus $f(x) \in (I)$.

$\supseteq$) Let $f(x) \in (I)$, that is $f(x) = a_0 + \cdots + a_n x^n$ with $a_i \in I$ for $0 \leq i \leq n$. This means that $\varphi(f(x)) = \overline{a_0} + \cdots + \overline{a_n} x^n = 0$ since $\overline{a_i} = 0$ in R/I for $0 \leq i \leq n$. Thus $f(x) \in \ker(\varphi)$.

Hence by the First Isomorphism Theorem: $(R/I)[x] \cong R[x]/\ker(\varphi) \cong R[x]/(I)$.

Exercise 6

Let R be an integral domain, prove that $R[x, y]$ is not a principal ideal domain. For this, consider the ideal (x, y), we will assume that it is principal and obtain a contradiction. Suppose $(x, y) = (f(x, y))$ for $f(x, y) = a_0 + a_{10}x + a_{01}y + a_{11}xy + \cdots + a_{nn}x^n y^n$.

1. We must have that $x = f(x, y)q_x(x, y)$ for some $q_x(x, y) \in R[x, y]$. Since R is an integral domain, we have $1 = \deg(x) = \deg(fq_x) = \deg(f)+\deg(q_x)$. If $\deg(f) = 0$, we directly obtain a contradiction since (x, y) has no constant polynomials. If $\deg(f) = 1$, this means that $f(x, y) = f(x) = ax$ for some $a \in R$ non zero.

2. Analogously we must have that $y = f(x, y)q_y(x, y)$ for some $q_y(x, y) \in R[x, y]$, and the same reasoning means that $f(x, y) = f(y) = by$ for some $b \in R$ non zero.

But $yb \neq ax$ when $a \neq 0 \neq b$, a contradiction. This means that such $f(x, y)$ cannot exist, hence (x, y) is not principal and thus $R[x, y]$ is not a principal ideal domain.