Algebra II

Mathematical Institute, University of Oxford
Hilary Term 2014

Problem Sheet 1

In this problem sheet, all rings are assumed to be commutative unless it is explicitly stated otherwise.

1. Let k be a field. Find when an element $f \in \mathsf{k}[[t]]$ is a unit. Do the same for the ring $\mathsf{k}[t]$.

Solution: Suppose that $f \in \mathsf{k}[[t]]$. Then f is a unit if and only if there is some $g \in \mathsf{k}[[t]]$ such that $f.g = 1$. Writing $f = \sum_{i \geq 0} a_i t^i$ and $g = \sum_{j \geq 0} b_j t^j$ we see that the equation $f.g = 1$ becomes the system of equations:

$$a_0 b_0 = 1; \quad \sum_{i+j=n} a_i b_j = 0, \forall n > 0.$$

Now given any f as above we can solve for $b_0 = a_0^{-1}$ provided $a_0 \neq 0$ (again since k is a field). But then if we have found $b_0, \ldots, b_{n-1}$ we may find b_n inductively using the second equation above: indeed rearranging it (and again using the fact that $a_0 \neq 0$) we see that

$$b_n = -a_0^{-1} \sum_{i=1}^{n} a_i b_{n-i},$$

where by induction all the terms on the right-hand side have already been calculated. It follows that $f = \sum_{i \geq 0} a_i t^i \in \mathsf{k}[[t]]$ is a unit precisely when $a_0 \neq 0$.

On the other hand, if $f \in \mathsf{k}[t] \backslash \{0\}$ and we have $f = \sum_{i=0}^{n} a_i t^i$ where $a_n \neq 0$, then set $\deg(f) = n$. Thus $\deg \colon \mathsf{k}[t] \backslash \{0\} \to \mathbb{Z}_{\geq 0}$. It is easy to check that $\deg(f.g) = \deg(f) + \deg(g)$ (in fact this holds in any polynomial ring $R[t]$ where R is an integral domain). Thus if $f \in \mathsf{k}[t]$ is a unit, so that there is some $g \in \mathsf{k}[t]$ with $f.g = 1$, taking degrees we see that $\deg(f) + \deg(g) = 0$ and since both degrees are nonnegative this can only happen if $\deg(f) = \deg(g) = 0$. It follows $f \in \mathsf{k} \backslash \{0\}$. Since any element of $\mathsf{k} \backslash \{0\}$ is clearly a unit (since k is a field) it follows the units in $\mathsf{k}[t]$ are exactly the nonzero elements of k (viewed as degree zero polynomials). $\square$

2. Let $\mathcal{H}$ denote the space of holomorphic (*i.e.* complex differentiable) functions $f \colon \mathbb{C} \to \mathbb{C}$, and let

$$\mathcal{C} = \{ f \colon \mathbb{R} \to \mathbb{R} : f \text{ is differentiable } \}.$$

Which (if either) of $\mathcal{H}$ or $\mathcal{C}$ is an integral domain?

Solution: Recall from complex analysis the Identity theorem: if a holomorphic function $f \colon U \to \mathbb{C}$ defined on a connected open set U vanishes on some open subset of U, then $f = 0$ on all of U. But now suppose that $f, g \in \mathcal{H}$ has $f.g = 0$. Then if $g \neq 0$ identically on $\mathbb{C}$, there is some $z_0 \in \mathbb{C}$ such that $g(z_0) \neq 0$. But then by continuity there is a $\delta > 0$ such that $g(z) \neq 0$ for all $z \in B(z_0, \delta)$, the ball of radius δ centred at z_0. Hence it follows from $f.g = 0$ that we must have $f(z) = 0$ for all $z \in B(z_0, \delta)$, and thus by the identity theorem shows that $f = 0$ on all of $\mathbb{C}$, and hence it follows $\mathcal{H}$ is an integral domain.

On the other hand, if $\mathcal{C}$ is the space of $\mathbb{R}$-valued differentiable functions on $\mathbb{R}$, then $\mathcal{C}$ is *not* an integral domain. For example, if we set $f(x) = 0$ for $x \leq 0$ and $f(x) = x^2$ for $x \geq 0$, and set $g(x) = f(-x)$, then both f and g are differentiable (even continuously differentiable) but $f.g = 0$ while clearly neither f nor g is zero. $\square$

3. Show that there is a unique homomorphism from $\mathbb{Z}$ to any (not necessarily commutative) ring R. Can you describe all ring homomorphisms from $\mathbb{C}$ to itself which are the identity on the subring (in fact subfield) of real numbers?

Solution: From the theory of cyclic groups, a homomorphism from the abelian group $\mathbb{Z}$ to any group is completely determined by the image of $1 \in \mathbb{Z}$: if $f\colon \mathbb{Z} \to (R, +)$ is a homomorphism of abelian groups then $f(n) = f(1)+f(1)+\ldots f(1)$ (n terms on the righthand side) when $n \geq 0$ and $f(n) = -f(-n)$ when $n < 0$. But if $f\colon \mathbb{Z} \to R$ is a ring homomorphism it is certainly a homomorphism of abelian groups and $f(1) = 1$, so that we see there is at most one homomorphism from $\mathbb{Z}$ to any ring R. To check that there is exactly one, it is enough to check that the map f defined above respects multiplication. But it is easy to see (say by induction on m) that $f(m.n) = f(m).f(n)$ when $m, n \geq 0$ and then since $f((-m).n) = f(-(m.n)) = -f(m.n)$ it is easy to see that this implies $f(m.n) = f(m).f(n)$ for all $m, n \in \mathbb{Z}$ as required.

If $\phi\colon \mathbb{C} \to \mathbb{C}$ is an homomorphism which is the identity on $\mathbb{R}$, then we have $\phi(a + ib) = a + \phi(i).b$ (where $a, b \in \mathbb{R}$). Thus ϕ is determined by its value on i. Since $i^2 + 1 = 0$, we see that $\phi(i)^2 + 1 = 0$ also (as $0, 1 \in \mathbb{R}$), thus $\phi(i) = \pm i$. Thus ϕ must either be the identity or complex conjugation.

□

4. If R and S are rings and $f\colon R \to S$ is a nonzero map such that $f(r.s) = f(r).f(s)$ and $f(r + s) = f(r) + f(s)$ for all $r, s \in R$, is it necessarily the case that $f(1) = 1$? Give a proof or counterexample. If the answer is "no" is there a class of rings for which the answer is "yes"?

Solution: Let $R = \mathbb{Z} \oplus \mathbb{Z}$ and consider the map $\theta\colon \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z}$ given by $\theta(a) = (a, 0)$. Then θ is certainly nonzero and it is easy to check that it respects addition and multiplication. However $\theta(1) = (1, 0)$, which is not the identity in $\mathbb{Z} \oplus \mathbb{Z}$.

On the other hand. if S is an integral domain, and $f\colon R \to S$ then we have $f(1) = f(1).f(1)$, so that $f(1).(f(1) - 1) = 0$ and hence since we are in a domain, $f(1) = 1$ or $f(1) = 0$. But if $f(1) = 0$ then

$$f(r) = f(r.1) = f(r).f(1) = f(r).0 = 0,$$

so that the condition that f is nonzero ensures that it does in fact respect the multiplicative identity elements. □

5. Check that if A is a subring of a ring R and B is an ideal of R, Then $A + B = \{a + b : a \in A, b \in B\}$ is a subring.

Solution: Clearly $A + B$ is closed under addition and contains $0 = 0 + 0$ and $1 = 1 + 0$. To see that it is preserved under multiplication, note that if $r_1, r_2 \in R$ and $s_1, s_2 \in S$ then

$$(r_1 + s_1)(r_2 + s_2) = r_1r_2 + s_1r_2 + r_1s_2 + s_1s_2,$$

where $r_1r_2 \in A$ and the remaining terms $s_1r_2 + r_1s_2 + s_1s_2$ all lie in B because it is an ideal of R. □

6. If R is a ring and I, J are ideals, show that IJ can be strictly smaller than $I \cap J$.

Solution: This is straight-forward: if $R = \mathbb{Z}$ and $I = \langle 4\rangle$, $J = \langle 6\rangle$ we see that $IJ = \langle 24\rangle$ while $I \cap J = \langle 12\rangle$. (Thus it is just the difference between the product of elements and their least common multiple. □

7. Check that the abstract Chinese Remainder Theorem becomes the classical statement when applied to the integers $\mathbb{Z}$, and two ideals $n\mathbb{Z}$, $m\mathbb{Z}$.

Solution: If $m, n \in \mathbb{Z}$ are such that h.c.f.$\{m, n\} = 1$, then by Bezout's theorem we can write $1 = am + bn$, and hence if $I = \langle m\rangle$ and $J = \langle n\rangle$ then $I + J = \mathbb{Z}$, and their intersection is $\langle m.n\rangle$ (again since m, n are coprime. The abstract chinese remainder theorem then yields the standard version of the Chinese Remainder theorem. □

8. Check that a ring is a field precisely when it has no nontrivial ideals.

Solution: If R is a field, then if I is a nonzero ideal, there is some $r \in R\backslash\{0\}$ such that $r \in I$. But then $1 = r^{-1}.r \in I$ so that $I = R$. Conversely if R is a ring with no nontrivial ideal then for any $r \in R\backslash\{0\}$ we must have $\langle r \rangle = R = \langle 1 \rangle$, hence r is a unit as required. $\square$