ALGEBRA 2B (MA20217)

PROBLEM SHEET 5 WITH SOLUTIONS

1 H. For each of the following commutative rings, say whether it is an integral domain, a field, or neither. Give brief reasons. What are the units in each case?

(a) The set of *Gaussian integers* $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$, (where $i = \sqrt{-1}$) with the usual operations of complex numbers.

(b) $\mathbb{Z}/9$, with the usual operations.

(c) $\mathbb{C}[t]$.

(d) $\mathbb{Q}[i] = \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$, with the usual operations of complex numbers.

Solution:

(a) This is contained in $\mathbb{C}$ and contains 1 so it is at least an integral domain, but it is not a field because $2 \in \mathbb{Z}[i]$ but $\frac{1}{2} \notin \mathbb{Z}[i]$. The units are the elements $a+ib$ such that $\frac{1}{a+ib} \in \mathbb{Z}[i]$. Since the inverse of $a+ib$ in $\mathbb{C}$ is $\frac{a-ib}{a^2+b^2}$, that happens if and only if $\frac{a}{a^2+b^2} \in \mathbb{Z}$ and $\frac{b}{a^2+b^2} \in \mathbb{Z}$. If $|a| > 1$ (or $|b| > 1$) that is not possible because $\left|\frac{a}{a^2+b^2}\right| < 1$, and the same happens if $|a| = |b| = 1$. We are left with $a = \pm 1$, $b = 0$ and $b = \pm 1$, $a = 0$: that is, the units are ± 1 and $\pm i$.

(b) This is not an integral domain because $3 \neq 0$ but $3^2 = 0$. The units are the numbers coprime to 3, that is ± 1, ± 2 and ± 4, whose inverses are ± 1, $\pm 5 = \mp 4$, and $\pm 7 = \mp 2$.

(c) This is an integral domain: for instance because $\deg fg = \deg f + \deg g > 0$ so $fg \neq 0$, unless f and g are both constants when it follows from $\mathbb{C}$ being a domain. Note that it contains 1. It is not a field because t is not invertible: if $f(t) \in \mathbb{C}[t]$ has degree $d \geq 0$ then $tf(t)$ has degree $d + 1 > 0$ so cannot be equal to 1, which has degree 0. The same argument applies to any polynomial $g(t)$ of positive degree $d' > 0$: then $\deg(g(t)f(t)) = d + d' > 0$ so $g(t)f(t) \neq 1$. So the only possible units are of degree 0, i.e., the nonzero constants: and they are indeed units, because $\mathbb{C}$ is a field. So the units here are $\mathbb{C}^*$.

(d) This is a field. It is an integral domain because it contains 1 and is contained in $\mathbb{C}$, and if $0 \neq a + ib \in \mathbb{Q}[i]$ then $\frac{1}{a+ib} = \frac{a}{a^2+b^2} + i\frac{-b}{a^2+b^2} \in \mathbb{Q}[i]$.

2 W Decide whether each of the following is a subring, an ideal, or neither; prove your assertions.

(a) $S_1 = \{-1, 0, 1\} \subset \mathbb{Z}$;

(b) $S_2 = \{a_0 + a_2t^2 + a_4t^4 + \cdots . \mid a_i \in \mathbb{Q}\} \subset \mathbb{Q}[t]$;

(c) $S_3 = \{a_2t^2 + a_3t^3 + a_4t^4 + \cdots . \mid a_i \in \mathbb{Q}\} \subset \mathbb{Q}[t]$;

(d) $S_4 = \{\text{polynomials of degree } \leq 2\} \subseteq \mathbb{Q}[t]$;

(e) $S_5 = \{p \in \mathbb{Q}[t] \mid p(1) = 0\} \subset \mathbb{Q}[t]$.

Solution:

(a) S_1 is not a subring and therefore not an ideal, because $1 + 1 \notin \{-1, 0, 1\}$.

(b) S_2 is not an ideal, because it is not closed under multiplication by $t \in \mathbb{Q}[t]$. However, it is a subring: it is non-empty because it contains 0; and given any two elements $f = \sum_i a_{2i}t^{2i} \in S_2$ and $g = \sum_i b_{2i}t^{2i} \in S_2$, we have

$$f - g = \sum_i (a_{2i} - b_{2i})t^{2i} \in S_2$$

and

$$f \cdot g = \sum_i \Big(\sum_{2j+2k=i} a_{2j}b_{2k} \Big) t^i \in S_2,$$

in both cases because the indices that occur on the right are even.

(c) S_3 is an ideal in $\mathbb{Q}[t]$. It is the ideal in $\mathbb{Q}[t]$ generated by t^2, i.e. the subset of all elements in $\mathbb{Q}[t]$ of the form $f \cdot t^2$ for some $f \in \mathbb{Q}[t]]$.

(d) S_4 is not a subring, because $t^2 \cdot t^2$ does not have degree at most 2.

(e) S_5 is the ideal generated by $(t - 1) \in \mathbb{Q}[t]$. Indeed, the division algorithm tells us that 1 is a root of a polynomial if and only if $(t - 1)$ is a factor.

3 H Show that if R is an integral domain, a, b, $c \in R$, and $ab = ac$, and $a \neq 0$, then $b = c$: that is, one may cancel. Is this the same as the statement "multiplication by a is injective"?

Solution: *Very simply, we have $a(b - c) = ab - ac = 0$ and since $a \neq 0$ and R is an integral domain we must have $b - c = 0$, i.e. $b = c$. Yes, this absolutely does mean that multiplication by a, thought of as a map $R \to R$, is injective. These are both very useful ways of thinking about what an integral domain is.*

GKS, 15/3/24