Algebra II: Tutorial 1

January 26, 2022

1. If R is an integral domain, then either $\mathrm{char}(R)$ is equal to zero or a prime number.

   Solution. Since $\mathrm{char}(R) \in \mathbb{N}$, $\mathrm{char}(R) = 0$ or $\mathrm{char}(R) > 0$. In the first case, there is nothing to prove. Suppose that $\mathrm{char}(R) = n > 0$, and that n is not prime, i.e. there exist integers $1 < n_1, n_2 < n$ such that $n = n_1 n_2$. Then, $n \cdot 1_R = (n_1 n_2) \cdot 1_R = (n_1 \cdot 1_R)(n_2 \cdot 1_R) = 0$, using the fact that $(R, +)$ is associative. Since R is an integral domain, this implies that either $n_1 \cdot 1_R = 0$ or $n_2 \cdot 1_R = 0$, which contradicts the assumption that n is the characteristic of R. Our assumption must be false, and n must be prime.

2. If R is an integral domain and a, b are non-zero, then $(a) = (b)$ if and only if $a = ub$ where $u \in R^\times$.

   Solution. Suppose that $a = ub$ with $u \in R^\times$. Then, $a \in (b)$ and $b \in (a)$, and so $(a) = (b)$. Suppose now that $(a) = (b)$. In particular, $a \in (b)$ and $b \in (a)$. In other words, $a = ub$ for some $u \in R$ and $b = ra$ for some $r \in R$. In particular, $(1 - ur)a = 0$. Since R is assumed integral and a assumed non-zero, $1 = ur$, which implies that both u and r are units. ■

3. Every Euclidean domain is a PID.

   Solution. Suppose that (R, v) is a Euclidean domain, and consider any non-zero ideal I in R. Then, the set $\{v(g) \mid g \in I, g \neq 0\} \subset \mathbb{N}$ admits a minimal element. Let $f \in I$ be any non-zero element in I realising that minimal value. Then, for any other $g \in I$, there exists elements $q, r \in R$ such that $f = qg + r$, where either $r = 0$ or $r \neq 0$, in which case $v(r)$ is well-defined and $v(r) < v(f)$. Note that $f \in I$ and $g \in I$ imply that $r \in I$, and the minimality assumption on f implies that $r = 0$, i.e. $g \in (f)$. Since g is an arbitrary element in I, we get $I = (f)$, which proves that R is a PID. ■

Problem 1 (Ideal correspondence)**.** Let R, S be commutative rings, with additive identities 0_R and 0_S respectively. Suppose that $f : R \to S$ is a surjective ring homomorphism.

1. Show that if I is an ideal of R, then $f(I) = \{f(r) \mid r \in I\}$ is an ideal of S.

2. Show that if J is an ideal of S, then $f^{-1}(J) = \{r \in R \mid f(r) \in J\}$ is an ideal of R containing $\mathrm{Ker}(f)$, the kernel of f.

3. Deduce that there is a one-to-one correspondence between ideals of S and ideals of R containing $\mathrm{Ker}(f)$.

4. Show that this correspondence descends to a bijection between prime (resp. maximal) ideal of S and prime (resp, maximal) ideals of R containing $\mathrm{Ker}(f)$.

Solution. Throughout the solutions, denote by 0_R and 1_R (respectively 0_S and 1_S) the additive and multiplicative identity elements in R (resp. in S).
1. Since $f(0_R) = 0_S$, $0_S \in f(I)$. If $s_1 = f(r_1) \in f(I)$, then $-1_S \cdot s_1 = f(-1_R)f(r_1) = f(-r_1) \in f(I)$. If $s_1, s_2 \in f(I)$, say $s_1 = f(r_1), s_2 = f(r_2)$, then $s_1+s_2 = f(r_1+r_2) \in f(I)$. Finally, if $s \in S$ and $s_1 \in f(I)$, say $s_1 = f(r_1)$, then $s \cdot s_1 = s \cdot f(r_1)$. By assumption, f is surjective, and so there exists $r \in R$ such that $f(r) = s$. Then, $s \cdot f(r_1) = f(rr_1) \in f(I)$, which concludes the proof that $f(I)$ is an ideal.
2. That $(f^{-1}(J), +)$ is an abelian subgroup of $(R, +)$ is immediate from the properties of f. Suppose that $r_1 \in f^{-1}(J)$, and $r \in R$. Then $f(r \cdot r_1) = f(r)f(r_1) \in J$, which implies that $r \cdot r_1 \in f^{-1}(J)$. Finally, notice that $\mathrm{Ker}(f) = f^{-1}(0)$, so $f^{-1}(J)$ necessarily contains $\mathrm{Ker}(f)$.
3. Suppose that I is an ideal of R containing $\mathrm{Ker}(f)$. Then, $f(I) = \{f(r) \mid r \in R\}$, and

$$\begin{aligned} f^{-1}(f(I)) &= \{r \in R \mid f(r) \in f(I)\} \\ &= \{r \in R \mid f(r) = f(y) \text{ for } y \in I\} \\ &= \{r \in R \mid r - y \in \mathrm{Ker}(f)\} \\ &= I + \mathrm{Ker}(f) = I. \end{aligned}$$

where in the last line we have used the fact that I contains $\mathrm{Ker}(f)$ by assumption.
Suppose now that J is an ideal of R. Then, $f(f^{-1}(J)) = \{f(r) \mid r \in f^{-1}(J)\} = \{f(r) \mid f(r) \in J\} = J$, where in the last equality we have used the assumption that f is surjective. This concludes our claim.
4. We prove the equivalence for prime ideals, the corresponding one for maximal ideals being straightforward. Suppose that I is a prime ideal in R containing $\mathrm{Ker}(f)$. Take $s_1, s_2 \in S$ such that $s_1s_2 \in f(I)$, say $s_1s_2 = f(r)$ for some $r \in I$. Since f is surjective, there exist $r_1, r_2 \in R$ such that $f(r_1) = s_1$ and $f(r_2) = s_2$. Therefore, $s_1s_2 = f(r_1r_2) = f(r)$, which implies that $r_1r_2 - r \in\mathrm{Ker}(f) \subset I$; in particular $r_1r_2 \in I$. By assumption, I is a prime ideal, so either r_1 or r_2 belongs to R, implying either s_1 or s_2 belongs to $f(I)$, proving our claim. Conversely, suppose that J is a prime ideal in S. Take $r_1, r_2 \in R$ such that $r_1r_2 \in f^{-1}(J)$. By definition, $f(r_1r_2) = f(r_1)f(r_2) \in J$. Since J is prime, either $f(r_1)$ or $f(r_2)$ belongs to J, and so either r_1 or r_2 belongs to $f^{-1}(J)$. ■