Math146 - PS3 due 2025-02-07

George McNinch

2025-02-07

In these exercises, you may use without proof that the real number $\sqrt{p}$ – a root of $T^2 - p$ – is not in $\mathbf{Q}$ for a prime number p.

Also, we are going to write $\mathbf{F}_p$ for the field $\mathbf{Z}/p\mathbf{Z}$ of order p.

---

1. Let R be a principal ideal domain (PID) and let $p \in R$ be irreducible. Let $I = \langle p^2 \rangle$ be the principal ideal generated by p^2.

   (a) Show that there is a surjective ring homomorphism $R/I \to R/\langle p \rangle$.

   (b) Show that the element $u = 1 + p + I \in R/I$ is a unit in R/I. Can you give an expression for the inverse u^{-1}?

2. Let R be a PID and let $a_1, a_2, \cdots, a_n \in R$ be elements which are not all 0 for some $n \in \mathbf{Z}_{>0}$.

   A *greatest common divisor* for the elements $a_1, a_2, \cdots, a_n$ is an element $d \in R$ with the properties: (i) $d \mid a_i$ for each $1 \le i \le n$, and (2) if $e \in R$ and $e \mid a_i$ for $1 \le i \le n$, then $e \mid d$.

   (a) Prove that a greatest common divisor d of the a_i exists and show that

   $$d = \sum_{i=1}^{n} x_i a_i$$

   for some elements $x_i \in R$ ($1 \le i \le n$).

   (b) If d and d' are two gcds of the a_i, show that d and d' are associates.

   (c) Suppose that $a, b, c \in R$ and that $(a, b) \neq (0, 0)$. Prove that $\gcd(\gcd(a, b), c) = \gcd(a, b, c)$.

   Hint: To prove (a) and (b), imitate the proof given in the notes for the case $n = 2$.

3. Let F be a field and let $a, b \in F$ with $a \neq b$. Prove that

   $$F[T]/\langle (T-a)(T-b) \rangle \simeq F \times F.$$

   Hint: Define a mapping $\phi : F[T] \to F \times F$ by the rule

   $$\phi(f) = (f(a), f(b)).$$

   Show that ϕ is onto and find $\ker \phi$.

4. Give an example of a *reducible* polynomial $f \in \mathbf{Q}[T]$ of degree 4 that has no roots in $\mathbf{Q}$.

5. Decide whether each of the following polynomials is irreducible. If the polynomial is irreducible, provide confirmation. If the polynomial is not irreducible, exhibit a factorization as a product of irreducible polynomials.

   (a) $T^2 - 3 \in \mathbf{F}_7[T]$.

   (b) $T^3 + T + 1 \in \mathbf{F}_2[T]$.

   (c) $T^3 + T + 1 \in \mathbf{F}_3[T]$.