MATH 113 - HOMEWORK 6

Due in class on Tuesday August 7, 2018

- All rings are assumed to be commutative and contain 1_R.

1. *Fermat's little theorem*

(a) Prove that $x^p - x = 0$ for all $x \in \mathbf{Z}/p\mathbf{Z}$, p a prime [Hint: Consider the order of the group $(\mathbf{Z}/p\mathbf{Z})^\times$].

(b) For each $n = 4, 6$, find $a \in \mathbf{Z}/n\mathbf{Z}$ such that $a^n \neq a$.

Note Part (b) might make you wonder if there's a converse to Fermat's little theorem i.e. is it true that if $x^p - x = 0$ for all $x \in \mathbf{Z}/n\mathbf{Z}$ then n is prime. Unfortunately, this is false (although, if you try small values of n, you'll be inclined to think otherwise). Any value of n for which this "converse" is false is called a *Carmichael number* and there are infinitely many of them. The smallest counterexample is $n = 561 = 3 \cdot 11 \cdot 17$.

2. Determine all irreducible polynomials of degree 2, 3 in $(\mathbf{Z}/2\mathbf{Z})[x]$.

3. *An integral domain that isn't a UFD.*

Consider the subring $\mathbf{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} : a, b \in \mathbf{Z}\} \subseteq \mathbf{C}$. You may assume it's an integral domain (do you see why?).

(a) Define the function $N : \mathbf{Z}[\sqrt{-5}] \longrightarrow \mathbf{Z}$ by $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Show that N satisfies the following three properties:

(1) (Non-negativity) $N(x) \geq 0$ for all $x \in \mathbf{Z}[\sqrt{-5}]$

(2) (Positive-Definiteness) $N(x) = 0$ iff $x = 0$

(3) (Multiplicativity) $N(xy) = N(x)N(y)$ for all $x, y \in \mathbf{Z}[\sqrt{-5}]$

Any function satisfying such properties is called a **norm**.

(b) Prove that $x \in \mathbf{Z}[\sqrt{-5}]$ is a unit iff $N(x) = 1$. Use this to list all the units in $\mathbf{Z}[\sqrt{-5}]$.

(c) Use the multiplicativity of the norm and part **(b)** to show that $2, 3, 1 \pm \sqrt{-5}$ are irreducible.

(d) Using the factorization $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ prove that $\mathbf{Z}[\sqrt{-5}]$ is not a UFD.

Note One can generalize this to prove that $\mathbf{Z}[\sqrt{-n}]$ is **NOT** a UFD for $n \geq 3$ square-free. On the other hand, $\mathbf{Z}[\sqrt{-2}]$ and $\mathbf{Z}[\sqrt{-1}]$ are PIDs (they are also Euclidean) and thus **are** UFDs. The analogous question about $\mathbf{Z}[\sqrt{n}]$ for $n \geq 2$ is a lot harder. For example, there are non-trivial units in $\mathbf{Z}[\sqrt{5}]$ (compare to part (b)). Indeed, notice that $2 - \sqrt{5}$ is a unit in $\mathbf{Z}[\sqrt{5}]$ because $(2 - \sqrt{5})(2 + \sqrt{5}) = -1$!

4. *Prime and Maximal ideals*: For each of the following ideals, determine whether they are prime, maximal or neither

(a) $(x^4 + 3x^2 + 1) \subseteq \mathbf{C}[x]$

(b) $(x^5 + 30x^3 - 48x^2 + 6x + 12) \subseteq \mathbf{Q}[x]$

(c) $(x - 1) \subseteq \mathbf{R}[x, y]$

(d) $(4, 2x - 1) \subseteq \mathbf{Z}[x]$

5. *Irreducible Elements*

(a) Prove that if R is an integral domain and (a) is a nonzero prime ideal, then a is an irreducible element.

(b) Show that $\mathbf{Z}[\sqrt{-5}]$ contains an irreducible element a such that (a) is not prime [so the converse to **(a)** is false].

(c) Prove that if R is a PID and a is irreducible, then (a) is maximal.

Note If R is a UFD, then $x \in R$ is prime iff irreducible. This is why prime and irreducible are used interchangeably in $\mathbf{Z}$, $K[x]$.

6. *Manipulating Ideals.*

(a) Find a ring homomorphism $f : R \longrightarrow S$ and an ideal I of R, such that $f(I)$ is NOT an ideal of S. [Thus, we usually consider $(f(I))$, the *ideal generated by the image of I*]

(b) Let $f : R \longrightarrow S$ be a ring homomorphism and $I \subseteq S$ an ideal. Prove that $f^{-1}(I)$ is an ideal. Moreover, if I is prime prove that $f^{-1}(I)$ is prime.

7. *Products of Rings*

Throughout this question, R, S will denote arbitrary rings.

(a) Prove that if R, S are non-trivial, then $R \times S$ is never an integral domain.

(b) Let $I \subseteq R, J \subseteq S$ be ideals. Prove that $I \times J$ is an ideal of $R \times S$.

(c) Prove that $(R \times S)/(I \times J) \cong (R/I) \times (S/J)$ [Hint: One can take a "product" of homomorphisms..].

(d) Find all prime ideals of $\mathbf{Z} \times \mathbf{Z}$. Which of these are maximal?