Problem Set 3

As in lectures, by rings we shall mean a commutative ring with identity, unless otherwise specified. Textbook questions are from "Galois Theory" (2nd edition) by Joseph Rotman.

1. Textbook exercise 44. [*The product is from $i = 1$ to n, a_i's are not necessarily distinct.*]

2. (a) Textbook exercise 46.

   (b) Compute the number of elements in the field $\mathbb{Z}_2[x]/I$.

   [Note that this gives you another kind of example of **finite fields**. The ones that we have already seen are : $\mathbb{Z}_p$ where p is a prime.]

3. Show that if m, n are coprime then $\mathbb{Z}_{mn}$ is isomorphic to $\mathbb{Z}_m \oplus \mathbb{Z}_n$ as rings.

   Hints : Consider the map $\phi : \mathbb{Z} \to \mathbb{Z}_m \oplus \mathbb{Z}_n$ given by $\phi(a) = ([a]_m, [a]_n)$ and try to use first isomorphism theorem. The Chinese Remainder Theorem may come in handy.

   We have been seeing in the lectures, how many concepts/theorems from Number Theory holds in Polynomial rings as well. The next two questions are similar and about proving the Chinese remainder Theorem for polynomials. A more general version of CRT in any ring is true and is given as a bonus problem in the next page.

4. Let K be a field and let $f(x),\ g(x) \in K[x]$ be **relatively prime**. Show that for any $r(x), s(x) \in K[x]$ the system of equations :

$$\begin{aligned} y &\equiv r(x) \quad \mod\ (f(x)) \\ y &\equiv s(x) \quad \mod\ (g(x)) \end{aligned}$$

   has a solution in $K[x]$, which is unique modulo $f(x)g(x)$.

   Note : This means first you've to find a polynomial $h(x) \in K[x]$ which satisfy the congruences. Here modulo means the same thing, you can think of it as :
   $a(x) \equiv b(x) \mod (f(x))$ if $f(x) \mid a(x) - b(x)$ or, if $a(x) - b(x) \in (f(x))$, the ideal generated by $f(x)$.

   Hint : Go back to the proof of CRT in Number Theory for coprime numbers and see if you can imitate the proof.

5. Now using Q.4 show that the following similar result as Q.3 is true for polynomials :
   Let K be a field and let $f(x),\ g(x) \in K[x]$ be relatively prime. Then, as rings

$$\frac{K[x]}{(f(x)g(x))} \cong \frac{K[x]}{(f(x))} \oplus \frac{K[x]}{(g(x))}$$

Bonus problem in next page!

Policy : Solving this question will get you a 2% course bonus, even if this PS is dropped while calculating your final grade. Of course, the maximum possible course grade is 100. Note that this question will be marked either 0 or 2, no partial marks. I encourage all of you to try it, but just to save time, please do not submit a partial answer or one that you're completely uncertain of.

Bonus Problem (2%)

Let R be a ring. For two ideals I, J of R define $I + J := \{i + j \mid i \in I,\ j \in J\}$.
I and J are called coprime if $I + J = R$. Show that, if I and J are coprime ideals of R, then

$$\frac{R}{I \cap J} \cong \frac{R}{I} \oplus \frac{R}{J}$$

Note : The surjectivity of the map is essentially CRT, which you'll need to prove.