Homework 5, Math 401

due on February 17, 2020

Before you start, please read the syllabus carefully.

1. Prove that given an integer $n = \prod_{1 \leq i \leq k}(p_i)^{r_i}$ where $p_i$ are different primes, then
   \[ \mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}. \]

2. In the above question, if $n = p_1p_2$, determine the isomorphism map $\phi : \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \rightarrow \mathbb{Z}_{p_1p_2}$.

3. Prove that the two definitions of $I = \langle \alpha_1, \cdots, \alpha_n \rangle$ are the same:
   1) the minimal ideal contain $\alpha_i$ for all $i$;
   2) the set $\{ \sum_{1 \leq i \leq n} r_i \alpha_i \mid r_i \in R \}$.
   \textbf{Answer:} It suffices to show that the two sets are the same. Denote the set defined by 1) to be $I_1$, and $I_2$ for the set defined by 2). The set $I_1$ is the minimal ideal contain $\alpha_i$ for all $i$, then for all $r_i \in R$, we have $r_i \alpha_i \in I_1$, thus $\sum_i r_i \alpha_i \in I_1$ since $I_1$ is an ideal. So we show that $I_2 \subseteq I_1$. On the other hand, we see that $I_2$ is an ideal, since $r(\sum_i \alpha_i r_i) = \sum_i (rr_i)\alpha_i \in I_2$ for all $r, r_i \in R$, and $\sum_i r_i \alpha_i + \sum_i r_i' \alpha_i = \sum_i (r_i + r_i')\alpha_i \in I_2$ for all $r, r_i, r_i' \in R$. So $I_1 = I_2$.

4. Given an irreducible polynomial $f(x) \in \mathbb{F}[x]$. Prove that $\mathbb{F}[x]/(f(x))$ is a field.

5. Given $f(x) = x^2 + 5$, determine whether $f(x)$ is irreducible in
   \begin{enumerate}[(a)]
   \item $\mathbb{Z}_3[x]$
   \item $\mathbb{Z}_5[x]$
   \item $\mathbb{Z}_7[x]$
   \end{enumerate}

6. Prove that $\mathbb{Z}_3[x]/(x^2 + 5) \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$.
   \textbf{Answer:} $f(x) = x^2 + 5 = (x + 2)(x + 1) \in \mathbb{Z}_3[x]$. Since $x + 2$ and $x + 1$ is relatively prime in $\mathbb{Z}_3[x]$, by Chinese Remainder Theorem, we have
   \[ \mathbb{Z}_3[x]/(f(x)) = \mathbb{Z}_3[x]/\langle(x + 2)(x + 1) \rangle \simeq \mathbb{Z}_3[x]/(x + 2) \times \mathbb{Z}_3[x]/(x + 1). \]

   Finally since $\mathbb{Z}_3[x]/(x + 2) \simeq \mathbb{Z}_3$ and $\mathbb{Z}_3[x]/(x + 1) \simeq \mathbb{Z}_3$, we have $\mathbb{Z}_3[x]/(x^2 + 5) \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$.

7. We have learnt that $F = \mathbb{Q}[\sqrt{2}]$ is a field extension of $\mathbb{Q}$. Determine whether $x^2 + 5 \in F[x]$ is irreducible.

8. Prove by induction that it follows from Fundamental Theorem of Algebra that every $f(x) \in \mathbb{C}[x]$ can be written into a product of linear polynomials in $\mathbb{C}[x]$. 