Homework 11 Partial Solutions

Problem 3.3. $C_0 = 1101000$, so $g(x) = 1 + x + x^3$. Then $n = 7$, and $r = 3$ (the degree of $g(x)$). Hence $n - r - 1 = 3$, and a basis is given by $\{g(x), xg(x), x^2g(x), x^3g(x)\}$. □

Problem 3.5. We have $< a >= \{ra | r \in R\}$. Let x, y be any two elements of $< a >$. Then $x = r_x a$, and $y = r_y a$ for some elements r_x, r_y of R, and $x - y = (r_x - r_y)a \in < a >$ since $r_x - r_y \in R$.
Similarly, for any $z = r_z a \in < a >$, and any $r \in R$, we get $rz = r(r_z a) = (rr_z)a \in < a >$. □

Problem 3.5. Let I be an arbitrary ideal of $\mathbb{Z}$. If $I =< 0 >$, then it is obviously principal. Otherwise, it must contain a positive integer (note than $x \in I \Rightarrow (-1)x \in I$), and, by the well-ordering principle, I contains a least positive integer. Call this integer c. Then we claim $I =< c >$. Suppose the claim is false, and let $x \in I$ such that c does not divide x. Assume w.l.o.g. that x is positive. Then $c = qx + r$ with $0 < r \leq c - 1$. But then $r = c - qx \in I$ since $c \in I$ and $x \in I$, and $r > 0$, contradicting the minimality of c in I. Remark: the notations $< y >$ and $\mathbb{Z}y$ both signify $\{zy | z \in \mathbb{Z}\}$, i.e. the set of all integer multiples of y. □