Problem 1 (20pts) Complete the following definitions:

(a–4pts) Let $R$ be a UFD and $B \subseteq R$ be a nonempty set. We say $h \in R$ is a highest common factor of $B$ if...

Solution. ... $h \mid b$ for all $b \in B$ and if $g \mid b$ for all $b \in B$ then $g \mid h$. \hfill \Box

(b–4pts) Let $R$ be a UFD and $f \in R[x] - \{0\}$. We say that $h \in R$ is a highest common factor of $f$ if...

Solution. ... $h$ is a highest common factor of the non-zero coefficients of $f$. \hfill \Box

(c–4pts) Let $R$ be a UFD and $f \in R[x] - \{0\}$. We say that $f$ is primitive if...

Solution. ... 1 is a highest common factor of $f$. \hfill \Box

(d–4pts) Let $L : K$ be a field extension. We say that $L : K$ is finite if...

Solution. ... the $K$-vector space $L$ is finite dimensional (as a $K$-vector space, of course). \hfill \Box

(e–4pts) Let $L : K$ be a field extension. We say that $L : K$ is an algebraic extension if...

Solution. ... every $\alpha \in L$ is algebraic over $K$, that is, if for each $\alpha \in L$, there is $f \in K[x]$ such that $f(\alpha) = 0$. \hfill \Box

Problem 2 (10pts) Consider the polynomial $f(x) = x^3 + 10x^2 + 15x + 10$.

(a–5pts) Decide if $f(x)$ is irreducible over $\mathbb{Q}[x]$.

Solution. Eisenstein’s Criterion states that if $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ and $p$ is prime such that

\begin{enumerate}
  \item $p \nmid a_n$
  \item $p \mid a_i$ for $i = 0, \ldots, a_{n-1}$
  \item $p^2 \nmid a_0$
\end{enumerate}

then $f$ is irreducible. Using the prime $p = 5$, we conclude that $f(x) = x^3 + 10x^2 + 15x + 10$ is irreducible. \hfill \Box
(b–5pts) Factor $f(x)$ into a product of irreducibles over $\mathbb{Z}_3[x]$.

**Solution.** We have that $f(x) = x^3 + x^2 + 1$ in $\mathbb{Z}_3[x]$, so that obviously $x = 1$ is a root and thus $x - 1$ divides $f$. Doing long division, we find:

\[
\begin{array}{cccc}
& & x & + 2 \\
\text{x - 1)} & x^3 & + x^2 & + 1 \\
& - x^3 & - x^2 & \\
\hline
& & 2 x^2 & \\
& & - 2 x^2 & + 2 x \\
\hline
& & & 2 x + 1 \\
& & & - 2 x + 2 \\
\hline
& & & 3 
\end{array}
\]

Thus $x^3 + x^2 + 1 = (x - 1)(x^2 + 2x + 2) + 3 = (x - 1)(x^2 + 2x + 2)$ (remember that we are working modulo 3). The first of these polynomials is irreducible over $\mathbb{Z}_3$ because it is linear; the latter is irreducible as we can easily check by looking for roots (recall that a quadratic is irreducible over $\mathbb{Z}$ if and only if it has no roots over $\mathbb{Z}$)

\[
\begin{align*}
x = 0 & \implies (0)^2 + 2 \cdot 0 + 2 \neq 0 \\
x = 1 & \implies (1)^2 + 2 \cdot 1 + 2 = 5 \neq 0 \\
x = 2 & \implies (2)^2 + 2 \cdot 2 + 2 = 10 \neq 0.
\end{align*}
\]

So $x^3 + x + 1 = (x - 1)(x^2 + 2x + 2)$ is a factorization of $f(x)$ into irreducibles as required.

---

**Problem 3** (15pts) Prove that if $R$ is a UFD, $p \in R$ is irreducible, and $q \in R$ is associated to $p$, then $q$ is prime.

**Solution.** In a UFD, all irreducibles are prime, thus it is enough to show that $q$ is irreducible. So suppose that $q = ab$; we must show that $a$ or $b$ is a unit. But $p$ and $q$ are associates, so there exists a unit $u \in R$ such that $p = uq$. Then $p = uab = (ua)b$ and since $p$ is irreducible, either $ua$ or $b$ is a unit. Of course, if $ua$ is a unit then so is $u^{-1}ua = a$, so we conclude that either $a$ or $b$ is a unit, that is, that $q$ is irreducible.

**Problem 4** (15pts) Suppose that $R$ is a PID and $r \in R$ is irreducible. Prove that $(r)$, the ideal generated by $r$, is a maximal ideal.

**Solution.** Note that given $a, b \in R$, $(a) \subseteq (b)$ if and only if $b \mid a$ (this could be assumed without proof in the answer, but for completeness sake—if there is $t \in R$ such that $bt = a$, then

\[
(a) = \{ra \mid r \in R\} = \{rtb \mid r \in R\} \subseteq \{rb \mid r \in R\} = (b);
\]

conversely, if $(a) \subseteq (b)$, then $a \in (b)$, that is, there is $t \in R$ such that $a = bt$.

To prove that $(r)$ is maximal, it is enough to show that if $M \subseteq R$ is an ideal and $(r) \subseteq M$, then $M = R$. But $R$ is a PID, so if $(r) \subseteq M$, there is $s \in R$ such that $M = (s)$, and $(r) \subseteq (s)$ implies that $s \mid r$ but $r \nmid s$ (if $r \mid s$, then $(s) \subseteq (r) \subseteq (s)$ a contradiction). Of course $r$ is irreducible, so $s$ or $t$ is a unit. If $t$ is a unit, then $t^{-1}r = s$, that is $r \mid s$, a contradiction. Thus $s$ must be a unit, whence $(s) = R$ as required.
Problem 5 (15pts) Suppose that $L : K$ is a field extension and $\alpha, \beta \in L$. If there is $f(x) \in K[x]$ such that $f(\alpha) = \beta$, prove that $K(\alpha) = K(\alpha, \beta)$.

Solution. Recall that $K(\alpha)$ is the smallest field containing $K$ and $\alpha$. Of course $K(\alpha, \beta)$ contains $K$ and $\alpha$ (it is the the smallest field containing $K$, $\alpha$, and $\beta$) and thus $K(\alpha) \subseteq K(\alpha, \beta)$.

So we are done if we can show $K(\alpha, \beta) \subseteq K(\alpha)$, and this will follow if $\beta \in K(\alpha)$ (since $K(\alpha, \beta)$ is the smallest field containing $K$, $\alpha$, and $\beta$ and we already already know that $K$ and $\alpha$ are in $K(\alpha)$).

By hypothesis, there is $f(x) \in K[x]$ such that $f(\alpha) = \beta$. Write $f(x) = \sum_{i=0}^{n} k_i x^i$ where $k_0, \ldots, k_n \in K$. Then

$$\beta = f(\alpha) = \sum_{i=0}^{n} k_i \alpha^i.$$  

But $K(\alpha)$ is a field, and is thus closed under multiplication and addition, that is,

$$\beta = f(\alpha) = \sum_{i=0}^{n} k_i \alpha^i = f(\alpha) \in K(\alpha)$$

because $\alpha, k_0, \ldots, k_n \in K(\alpha)$. This completes the proof. \qed