MATH 347 Homework #4 sketch of solutions

Note Title

#1 Let $p(x)$, $g(x)$, $f(x)$ be polynomials. Suppose $f(x) \mid p(x)$ and $f(x) \mid g(x)$. Prove that for any polynomials $a(x)$, $b(x)$, $f(x) \mid (a(x)p(x) + b(x)g(x))$.

Since $f(x) \mid p(x)$ and $f(x) \mid g(x)$ there are polynomials $q_1(x), q_2(x)$ so that $p(x) = q_1(x) f(x)$, $g(x) = q_2(x) f(x)$. Then

$a(x)p(x) + b(x)g(x) = a(x)q_1(x)f(x) + b(x)q_2(x)f(x) = \big(a(x)q_1(x) + b(x)q_2(x)\big)f(x)$

$\Rightarrow f(x) \mid a(x)p(x) + b(x)g(x)$.

#2 A subset $I \subseteq \mathbb{Z}$ is an ideal iff (i) $a \in I$ and $b \in I \Rightarrow a+b \in I$. and $a \in I$, $d \in \mathbb{Z} \Rightarrow ad \in I$.

Prove that for any ideal I there is an integer $a \geq 0$ so that

$$I = \{ax \mid x \in \mathbb{Z}\} = a\mathbb{Z}.$$

If $I = \{0\}$, we may take $a = 0$. Next suppose $I \neq \{0\}$.

Consider $S = \{n \in I \mid n > 0\}$. To apply Well-Ordering Principle, we need to argue that $S \neq \emptyset$. Since $I \neq \{0\}$, there is $x \in I$ with $x \neq 0$. If $x > 0$, $x \in S$ and $S \neq \emptyset$. If $x < 0$, $(-1)\cdot x > 0$ and $(-1)\cdot x \in I$ since I is an ideal in $\mathbb{Z}$. Now, by well-ordering, we know that $a = \min(S)$ exists. We next argue that $I = \{ax \mid x \in \mathbb{Z}\}$.

Since $a \in I$, $ax \in I$ for all $x \in \mathbb{Z}$. $\Rightarrow \{ax \mid x \in \mathbb{Z}\} \subseteq I$.

Conversely, suppose $y \in I$. By the division algorithm there are $q, r \in \mathbb{Z}$ so that $y = qa + r$ and $0 \leq r < a$. Since $a \in I$, $(-q)a \in I$.

$\Rightarrow r = y + (-q)a \in I$. If $r > 0$, $r \in S$. Since $r < a = \min S$, this cannot happen. $\Rightarrow r = 0 \Rightarrow y = qa$ for some $q \in \mathbb{Z}$.

$\Rightarrow y \in \{ax \mid x \in \mathbb{Z}\}$. Since y is arbitrary, $I \subseteq \{ax \mid x \in \mathbb{Z}\}$.

Therefore $I = \{ax \mid x \in \mathbb{Z}\}$.

#3 (a) Prove that for any $a, b \in \mathbb{Z}$ the set

$$(a,b) := \{ au + bv \mid u, v \in \mathbb{Z} \}$$

is an ideal.

Proof: $\forall x \in \mathbb{Z}$, $\forall u, v \in \mathbb{Z}$, $(au+bv)x = a\cdot(ux) + b(vx) \in (a,b)$

$\forall u_1, u_2, v_1, v_2 \in \mathbb{Z}$ $\quad (au_1 + bv_1) + (au_2 + bv_2) = a(u_1+u_2) + b(v_1+v_2) \in (a,b)$.

Therefore (a,b) is an ideal.

(b) Prove that $(a,b) = \{ dx \mid x \in \mathbb{Z} \} = d\mathbb{Z}$ where $d = \gcd(a,b)$.

Since (a,b) is an ideal by (a) above, $(a,b) = d\mathbb{Z}$ for some $d \in \mathbb{Z}$ by #2. Since $a \in (a,b) = d\mathbb{Z}$, $a = dx$ for some $x \in \mathbb{Z}$. $\Rightarrow d \mid a$. Similarly, $d \mid b$. Thus d is a divisor of a & b. Since $d \cdot 1 \in d\mathbb{Z} = (a,b)$, there are integers u_0, v_0 so that $d = u_0 a + v_0 b$. So if $c \mid a$ and $c \mid b$, then $c \mid u_0 a + v_0 b \Rightarrow c \mid d$. $\Rightarrow d$ is the greatest common divisor of a & b.

#4 Prove that if p is a prime number then $\sqrt[3]{p}$ is irrational.

Suppose $\sqrt[3]{p} = a/b$ where $a, b \in \mathbb{Z}$, $b \neq 0$. We may assume $\gcd(a,b) = 1$ (if not, reduce the fraction). Then $b^3 p = a^3$. $\Rightarrow p \mid a^3$. Since p is prime $p \mid a^3 \Rightarrow p \mid a$, ie. $a = qp$ for some $q \in \mathbb{Z}$ $\Rightarrow b^3 p = (qp)^3$ $\Rightarrow b^3 = q^3 p^2$. $\Rightarrow p \mid b^3$. Since p is prime $p \mid b^3 \Rightarrow p \mid b$. But $p \mid b$ and $p \mid a$ contradicts $\gcd(a,b) = 1$. Therefore no such a and b may exist.

#5 Do there exist integers x and y so that $13x + 17y = 132$?

Since 13 and 17 are both primes, $\gcd(13,17) = 1$. $\Rightarrow \exists u, v \in \mathbb{Z}$ so that $13u + 17v = 1$. $\Rightarrow 132 = 1 \cdot 132 = (13u + 17v)132 = 13\cdot(u \cdot 132) + 17(v \cdot 132)$

Let $x = 132u$, $y = 132v$.