Math 306, Spring 2012
Homework 2 Solutions

(1) (5 pts) Suppose that R is an integral domain that is not a field. Prove that $R[x]$ is not a principal ideal domain. (Hint: Let $c \in R$ be nonzero and noninvertible and consider $I = (c, x)$.)

Solution: Suppose that c is nonzero and noninvertible in R and let $I = (c, x)$. Suppose that I is principal, i.e. there is $d \in I$ such that $I = (d)$. Therefore $c \in (d)$ and $x \in (d)$. In other words, we have $d|c$ and $d|x$. Since $d|x$, then d is a unit or $d = ux$, where u is a unit. Since d also divides c, it must follow that d is a unit. Hence $I = R[x]$. Therefore there are $p, q \in R[x]$ such that $cp + qx = 1$. Since the degree of qx is at least 1, it follows that $cp_0 = 1$, where $p_0 \in R$ is the constant term of p. Therefore c is a unit, a contradiction.

(2) (5 pts) Prove that every quotient of a principal ideal domain is also a principal ideal domain. (Hint: Let H be an ideal of R/I and prove that $J = \{a \in R\colon a + I \in H\}$ is an ideal of R and hence principal.)

Solution: Let R be a principal ideal domain and let I be an ideal of R. Let H be an ideal in R/I. Consider the set $J = \{a \in R\colon a + I \in H\}$. Since H is nonempty, it must contain $0 + I$, so $0 \in J$. Suppose that $a, b \in J$. Then $a + I, b + I \in H$. Therefore $a - b + I = (a + I) - (b + I) \in H$, so $a - b \in J$. If $a \in J$ and $r \in R$, then $a + I \in H$, so $ra + I = (r + I)(a + I) \in H$ and $ar + I = (r + I)(a + I) \in H$, so $ra, ar \in J$. Therefore J is an ideal in R. Since R is principal, there is some $j \in R$ such that $J = (j)$. We claim that $H = (j + I)$. Clearly $(j + I) \subseteq H$. If $a + I \in H$, then $a \in J$, so $a = rj$ for some $r \in R$. Therefore $a + I = (r + I)(j + I)$, so $a + I \in (j + I)$. Hence H is principal and R/I is a PID.

(3) Let $\mathbb{Q}_{(2)}$ be the set of rationals of the form r/s, where $r \in \mathbb{Z}$ and s is a positive odd integer.
- (a) (3 pts) Prove that $\mathbb{Q}_{(2)}$ is a subring of $\mathbb{Q}$.
- (b) (3 pts) Find the set of units $U(\mathbb{Q}_{(2)})$.
- (c) (5 pts) Prove that $\mathbb{Q}_{(2)}$ is a principal ideal domain. (Hint: Let I be an ideal of $\mathbb{Q}_{(2)}$ and let 2^n be the smallest power of 2 that lies in I; prove that $I = (2^n)$ by showing that $(2^n) \subseteq I$ and $I \subseteq (2^n)$.)

Solution:
- (a) Certainly $0/1 \in \mathbb{Q}_{(2)}$, so $\mathbb{Q}_{(2)}$ is nonempty. Suppose that $a/b, c/d \in \mathbb{Q}_{(2)}$, where b and d are positive odd integers. Then $a/b - c/d = (ad - bc)/bd$ is also in $\mathbb{Q}_{(2)}$ since bd is a positive odd integer. Also we have $(a/b)(c/d) = (ac)/(bd)$ which clearly belongs to $\mathbb{Q}_{(2)}$. Hence $\mathbb{Q}_{(2)}$ is a subring of $\mathbb{Q}$.
- (b) The group of units is given by $U(\mathbb{Q}_{(2)}) = \{p/q\colon p \text{ is odd and } q \text{ is positive odd}\}$.
- (c) Let I be an ideal of $\mathbb{Q}_{(2)}$. If I is trivial, then $I = (0)$ so is principal. If I is not trivial, then there is some $p/q \in I$ where q is a positive odd integer. We can express $p/q = 2^a m/q$, where $a \in \mathbb{Z}_{\geq 0}$ and m is odd. Since $2^a m/q \in I$, we must have $2^a = (2^a m/q)(q/m) =\in I$. Therefore I contains some power of 2. Let 2^n be the smallest power of 2 that lies in I. We claim that $I = (2^n)$. Clearly $(2^n) \subseteq I$. Suppose that $2^b r/s \in I$, where $b \in \mathbb{Z}_{\geq 0}$ and r and s are odd. Then $2^b \in I$, so $b \geq n$. Therefore $2^b r/s = (2^n)(2^{b-n} r/s)$, so $2^b r/s \in (2^n)$. Hence I is principal, so $\mathbb{Q}_{(2)}$ is a PID.

(4) (4 pts/part) For each of the following pairs of polynomials f and g, find the quotient and remainder upon dividing g by f in the polynomial ring $K[t]$, where K is a field.
- (a) $g = t^7 - t^3 + 5$ and $f = t^3 + 1$ in $\mathbb{Q}[t]$;
- (b) $g = t^3 + 2t^2 - t + 1$ and $f = t + 2$ in $\mathbb{Z}_3[t]$.

Solution:
- (a) $g = (t^4 - t - 1)f + (t + 6)$
- (b) $g = (t^2 - 1)f + 0$

(5) (4 pts/part) For each of the pairs above, find the highest common factor and express it in the form $af + bg$ for some $a, b \in K[t]$ (see Theorem 2.9 on page 35). You may leave a and b in unexpanded form. Recall that we defined the highest common factor to be monic.

Solution:

(a) $1 = \frac{1}{215}(t^2 - 6t + 36)(t^7 - t^3 + 5) - \frac{1}{215}((t^2 - 6t + 36)(t^4 - t - 1) + 1)(t^3 + 1)$
$= \frac{1}{215}(t^2 - 6t + 36)(t^7 - t^3 + 5) - \frac{1}{215}(t^6 - 6t^5 + 36t^4 - t^3 + 5t^2 - 30t - 35)(t^3 + 1)$

(b) $t + 2 = 1 \cdot (t + 2) + 0 \cdot (t^3 + 2t^2 - t + 1)$

(6) (a) (5 pts) List all the irreducible monic quadratic polynomials $t^2 + at + b$ in $\mathbb{Z}_5[t]$.
(b) (3 pts) In each of these cases, compute $a^2 - 4b$. Formulate a conjecture but do not prove it.

Solution:

polynomial	t^2+2	t^2+3	t^2+t+1	t^2+t+2	t^2+2t+3	t^2+2t+4	t^2+3t+3	t^2+3t+4	t^2+4t+1	t^2+4t+2
a^2-4b	2	3	2	3	2	3	2	3	2	3

Conjecture: a monic quadratic polynomial in $\mathbb{Z}_5[x]$ is irreducible iff $a^2 - 4b$ equals 2 or 3.

(7) (5 pts) List all irreducible cubic polynomials in $\mathbb{Z}_2[t]$.

Solution: The only ones are $t^3 + t + 1$ and $t^3 + t^2 + 1$.