MATH 521A: Abstract Algebra
Homework 6 Solutions

1. Let R, S, T be rings, with S, T both subrings of R. Suppose that S has the special property that for every $s \in S$ and every $r \in R$, we have both $sr \in S$ and $rs \in S$. Set $S+T = \{s+t : s \in S, t \in T\}$, a subset of R. Prove that $S+T$ is a subring of R.

   First, $0_R \in S$ and $0_R \in T$ (since S, T are subrings), so $0_R = 0_R + 0_R \in S+T$. Second, let $x, x' \in S+T$. Then there are s, t, s', t' with $s, s' \in S$, $t, t' \in T$, and $x = s+t, x' = s+t'$. Now, we calculate $x - x' = (s+t) - (s'+t') = (s-s') + (t-t')$. Since $s - s' \in S$ and $t - t' \in T$, we have $x - x' \in S+T$. Lastly, we calculate $xx' = (s+t)(s'+t') = (ss' + st' + ts') + tt'$. Since S is a ring, $ss' \in S$. Similarly, since T is a ring, $tt' \in T$. By our special property, both st' and ts' are in S, so the sum $ss' + st' + ts' \in S$. Hence $xx' \in S+T$.

2. Consider the polynomial ring $\mathbb{Z}_9[x]$, and the nine elements $\{3x+0, 3x+1, \ldots, 3x+8\}$. Determine which are units and which are zero divisors.

   Let's first find units, by calculating $(a+3x)(b_0+b_1x+\cdots+b_nx^n) = 1$. Looking at the constant term, we have $ab_0 \equiv 1 \pmod 9$, so a is a unit modulo 9. This limits us to $a \in \{1, 2, 4, 5, 7, 8\}$. A bit of trial and error shows that all six are units: $(1+3x)(1+6x) \equiv (2+3x)(5+6x) \equiv (4+3x)(7+6x) \equiv (5+3x)(2+6x) \equiv (7+3x)(4+3x) \equiv (8+3x)(8+6x) \equiv 1 \pmod 9$.

   Now we look for zero divisors, by calculating $(a+3x)(b_0+b_1x+\cdots+b_nx^n) = 0$. Looking at the constant term, we have $ab_0 \equiv 0 \pmod 9$, so a is a zero divisor modulo 9. This limits us to $a \in \{0, 3, 6\}$. All three are zero divisors, as $(a+3x)(3) \equiv 3a + 0x \equiv 0 \pmod 9$.

3. Consider the polynomial ring $\mathbb{Z}_9[x]$, and the nine elements $\{0x+3, 1x+3, \ldots, 8x+3\}$. Determine which are units and which are zero divisors.

   For all nine elements, the constant term is 3; the argument in the preceding problem shows that none of these can be units, but some might be zero divisors. We have $(0x+3)(3) \equiv (3x+3)(3) \equiv (6x+3)(3) \equiv 0 \pmod 9$, so these three are zero divisors. We now prove that the remaining six are neither units nor zero divisors.

   Calculate $(3+ax)(b_0+b_1x+\cdots+b_nx^n) = 0$, and look at the x^{n+1} term. We must have $ab_n \equiv 0 \pmod 9$, so a must be a zero divisor modulo 9. However, none of $\{1, 2, 4, 5, 7, 8\}$ are zero divisors modulo 9, so none of $\{1x+3, 2x+3, 4x+3, 5x+3, 7x+3, 8x+3\}$ are zero divisors in $\mathbb{Z}_9[x]$.

4. Let R be a ring, and $k \in \mathbb{N}$. Define $x^kR[x] = \{x^kf(x) : f(x) \in R[x]\}$. Prove that $x^kR[x]$ is a subring of $R[x]$.

   Certainly $x^kR[x]$ is a subset of $R[x]$, being polynomials (whose lowest-degree term is at least of degree k). First, $0 = x^k0$, so the zero polynomial $0 \in x^kR[x]$. Now, let $x^kf(x), x^kg(x) \in x^kR[x]$. We have $x^kf(x) - x^kg(x) = x^k(f(x) - g(x))$. Since $f(x) - g(x) \in R[x]$, $x^kf(x) - x^kg(x) \in x^kR[x]$. Lastly, we have $x^kf(x)x^kg(x) = x^k(f(x)x^kg(x))$. Since $f(x)x^kg(x) \in R[x]$, we have $x^kf(x)x^kg(x) \in x^kR[x]$.

5. Let F be a field. Determine explicitly which elements of $F[x]$ are in the subring $x^3F[x] + x^5F[x]$. (refer to exercises 1,4)

Exercises 1 and 4 prove that this object is a subring (provided we check the special property for either $x^3F[x]$ or $x^5F[x]$, which is not too hard to do). Suppose $a(x) = a_0 + a_1x + \cdots + a_kx^k \in x^3F[x] + x^5F[x]$. Then there are polynomials $b(x), c(x) \in F[x]$ with $a(x) = x^3b(x) + x^5c(x) = (b_0x^3 + b_1x^4 + \cdots + b_mx^{3+m}) + (c_0x^5 + c_1x^6 + \cdots + c_nx^{5+n}) = b_0x^3 + b_1x^4 + \cdots$. Note that this proves that $a_0 = a_1 = a_2 = 0$, so in particular $a(x) \in x^3F[x]$. Hence $x^3F[x] + x^5F[x] \subseteq x^3F[x]$. But also $x^3F[x] \subseteq x^3F[x] + x^5F[x]$, because for each $x^3f(x) \in x^3F[x]$, we can write $x^3f(x) = x^3f(x) + x^50 \in x^3F[x] + x^5F[x]$. Hence in fact $x^3F[x] + x^5F[x] = x^3F[x]$.

6. Working in $\mathbb{Q}[x]$, find $\gcd(a(x), b(x))$, for $a(x) = x^3 + x^2 + x + 1$, $b(x) = x^4 - 2x^2 - 3x - 2$.

$$\begin{aligned} x^4 - 2x^2 - 3x - 2 &= (x-1)(x^3 + x^2 + x + 1) + (-2x^2 - 3x - 1) \\ x^3 + x^2 + x + 1 &= \left(-\frac{1}{2}x + \frac{1}{4}\right)(-2x^2 - 3x - 1) + \left(\frac{5}{4}x + \frac{5}{4}\right) \\ -2x^2 - 3x - 1 &= \left(-\frac{8}{5}x - \frac{4}{5}\right)\left(\frac{5}{4}x + \frac{5}{4}\right) + 0 \end{aligned}$$

Hence $\gcd(a, b)$ is the monic multiple of $\frac{5}{4}x + \frac{5}{4}$, namely $x + 1$.

7. Working in $\mathbb{Z}_2[x]$, find $\gcd(a(x), b(x))$, for $a(x) = x^3 + x^2 + x + 1$, $b(x) = x^4 - 2x^2 - 3x - 2$.

We first note that $b(x) = x^4 + x$, and calculate:

$$\begin{aligned} x^4 + x &= (x+1)(x^3 + x^2 + x + 1) + (x+1) \\ x^3 + x^2 + x + 1 &= (x^2 + 1)(x + 1) + 0 \end{aligned}$$

Hence $\gcd(a, b) = x + 1$, which is already monic.

8. Working in $\mathbb{Z}_5[x]$, find $\gcd(a(x), b(x))$, for $a(x) = x^3 + x^2 + x + 1$, $b(x) = x^4 - 2x^2 - 3x - 2$.

$$\begin{aligned} x^4 - 2x^2 - 3x - 2 &= (x-1)(x^3 + x^2 + x + 1) + (3x^2 + 2x - 1) \\ x^3 + x^2 + x + 1 &= (2x - 1)(3x^2 + 2x - 1) + 0 \end{aligned}$$

Hence $\gcd(a, b)$ is the monic multiple of $3x^2 + 2x - 1$, namely $2(3x^2 + 2x - 1) = x^2 + 4x + 3$.

9. Working in $\mathbb{Q}[x]$, let $a(x) = x^2 - 5x + 6$, $b(x) = x^3 - x^2 - 2x$. Find $u(x), v(x)$ such that $\gcd(a(x), b(x)) = a(x)u(x) + b(x)v(x)$.

$$\begin{aligned} x^3 - x^2 - 2x &= (x+4)(x^2 - 5x + 6) + (12x - 24) \\ x^2 - 5x + 6 &= \left(\frac{1}{12}x - \frac{1}{4}\right)(12x - 24) \end{aligned}$$

We solve for $12x - 24$, getting $12x - 24 = (x^3 - x^2 - 2x) + (-x - 4)(x^2 - 5x + 6)$. Now we normalize, to make the gcd monic, by multiplying by $\frac{1}{12}$, getting $x - 2 = (\frac{1}{12})(x^3 - x^2 - 2x) + (\frac{-1}{12}x - \frac{1}{3})(x^2 - 5x + 6)$. Hence the desired polynomials are $u(x) = \frac{-1}{12}x - \frac{1}{3}$ and $v(x) = \frac{1}{12}$.

10. Working in $\mathbb{Z}_3[x]$, let $a(x) = x^2 - 5x + 6$, $b(x) = x^3 - x^2 - 2x$. Find $u(x), v(x)$ such that $\gcd(a(x), b(x)) = a(x)u(x) + b(x)v(x)$.

Note that $a(x) = x^2 + x$ and $b(x) = x^3 + 2x^2 + x = (x^2 + x)(x + 1)$. Hence $\gcd(a, b) = x^2 + x$, and $x^2 + x = 1(x^2 + x) + 0(x^3 + 2x^2 + x)$, so we can take $u(x) = 1$, $v(x) = 0$.