Math 151 Spring 2004

Test 3 - Solutions

1. Find the greatest common divisor of $f(x) = 6x^2 + 4x - 2$ and $g(x) = 3x^3 - 4x^2 - 2x + 1$ over R.
   $3x^3 - 4x^2 - 2x + 1 = (6x^2 + 4x - 2)(\frac{1}{2}x - 1) + (3x - 1)$
   $6x^2 + 4x - 2 = (3x - 1)(2x + 2)$
   so $gcd(f(x), g(x))$ *is the multiple of* $3x - 1$ *that is monic, i.e.* $x - \frac{1}{3}$.

2. Is $x^3 - 2$ irreducible

   (a) over $\mathbb{Q}$?
   Yes because it does not have rational roots.

   (b) over $\mathbb{Z}_5$?
   No: $x^3 - 2 \equiv x^3 - 27 = (x - 3)(x^2 + 3x + 9) \equiv (x + 2)(x^2 + 3x + 4)$ *(mod 5).*
   Or, could find the root $x = 3$*, and then* $x^3 - 2$ *factors as* $(x - 3)g(x)$ *for some polynomial* $g(x) \in \mathbb{Z}_5[x]$.

3. Can a field have exactly

   (a) 1 element?
   No because the multiplicative identity must be different from the additive identity, so a field has at least 2 elements.

   (b) 2 elements?
   Yes. $\mathbb{Z}_2$ *is a field.*

4. Is the union of 2 ideals always an ideal? Prove or give a counterexample.
   No. Counterexample: Ring $R = \mathbb{Z}$*, ideals* $I = 2\mathbb{Z}$ *and* $J = 3\mathbb{Z}$*. The union* $I \cup J$ *is not an ideal because e.g. it is not closed under addition:* $2 \in I$*, so* $2 \in I \cup J$*;* $3 \in J$*, so* $3 \in I \cup J$*; but* $2 + 3 = 5 \notin I \cup J$ *because* $5 \notin I$ *and* $5 \notin J$.

5. Find the multiplicative inverse of $[x]$ in $\mathbb{Z}_3 \, / < x^2 + x + 2 >$.
   $x^2 + x + 2 = x(x + 1) + 2$
   $x = 2(2x)$ *(modulo 3!)*
   So $2 = (x^2 + x + 2) - x(x + 1)$
   $2 = (x^2 + x + 2) + x(2x + 2)$
   Multiply both sides by 2:
   $1 = (x^2 + x + 2)2 + x(x + 1)$
   Therefore $x(x + 1) \equiv 1$ *(mod* $x^2 + x + 2$*)*
   i.e. $[x]^{-1} = [x + 1]$.

6. Let R and S be rings, and let $f : R \to S$ be an onto ring homomorphism. Prove that if R is commutative then so is S.
   Let $a, b \in S$*. Since* f *is onto, there exist* $x, y \in R$ *such that* $a = f(x)$ *and* $b = f(y)$*.*
   Then $ab = f(x)f(y) = f(xy) = f(yx) = f(y)f(x) = ba$*, so* S *is commutative.*

Optional: Is $\mathbb{Z}[x]/ < x^2 + 2 >$ a field?

No. Every congruence class has a unique representative of the form $ax + b$*. The class of* x *has no inverse because* $x(ax+b) = ax^2+bx = ax^2+2a+bx-2a = a(x^2+2)+bx-2a \equiv bx - 2a \not\equiv 1$ *(mod* $x^2 + 2$*) for any* a *and* b.