Submit problems 1, 3 and 9 by Thursday, August 10. Concepts covered: Polynomial rings over fields. Reading: Rotman section on Polynomial Rings over Fields.

1. Let A be your student id. If $17 \nmid A$ let $a = A$ otherwise let a be the smallest prime greater than A. Find the multiplicative inverse of $[a]$ in $\mathbb{Z}/17\mathbb{Z}$.

2. Show that $p(x) = x^2 + 1$ is irreducible in $\mathbb{R}[x]$. Show that $\mathbb{C} \cong \mathbb{R}[x]/(p)$. Factorize p in $\mathbb{C}[x]$.

3. Let R be a ring.
   (a) Show that $R^R = \{f : R \to R\}$, the set of functions from R to R is a ring. If R is an integral domain is R^R also a domain?

   (b) Show that the map $\Phi : R[x] \to R^R$ which sends a formal polynomial to the function associated to the polynomial is a ring homomorphism.

   (c) If R is a finite field prove that Φ is not injective. Demonstrate a non-trivial element in $\ker \Phi$.

   (d) If R is an infinite field prove that Φ is injective.

   (e) If $R = \mathbb{Z}/2\mathbb{Z}$ find $\ker \Phi$ and show that $R[x]/\ker \Phi \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

   (f) (**Bonus**) Prove an analogous statement for $\mathbb{Z}/p\mathbb{Z}$ for $p > 2$.

4. Let F be a field. $p \in F[x]$ is called irreducible if $\deg p > 0$ and p can not be factored as $p = fg$ where $\deg f > 0$ and $\deg g > 0$. Prove that (p) is a prime ideal if and only if p is irreducible, hence show that $E = F[x]/(p)$ is a field. Show that if $\deg p = 1$ then p is irreducible and $F[x]/(p) \cong F$.

5. Let F be a field and $a, b \in F[x]$ non-zero polynomials. The greatest common divisor, gcd of a and b a monic polynomial d which divides both a and b and any polynomial which divides a and b also divides d.
   (a) Show that the gcd exists and can be expressed as $d = ap + bq$ for some $p, q \in F[x]$. Show that d is unique.

   (b) Prove that if a is irreducible then $\gcd(a, b) = 1$.

6. Prove that there are domains R containing a pair of elements having no gcd. (Problem 40, page 30 Rotman)

7. Problem 43, page 31 Rotman.

8. Problem 44, page 31 Rotman.

9. Problem 45, page 31 Rotman.

10. Problem 46, page 31 Rotman.

11. Problem 47, page 31 Rotman.

12. Problem 48, page 31 Rotman.

43. In the ring $R = \mathbb{Z}[x]$, show that x and 2 are relatively prime, but there are no polynomials $f(x)$ and $g(x) \in \mathbb{Z}[x]$ with $1 = xf(x) + 2g(x)$.

44. Let $f(x) = \prod(x - a_i) \in F[x]$, where F is a field and $a_i \in F$ for all i. Show that $f(x)$ has ***no repeated roots*** [i.e., $f(x)$ is not a multiple of $(x - a)^2$ for any $a \in F$] if and only if $(f(x), f'(x)) = 1$, where $f'(x)$ is the derivative of $f(x)$.

45. Find the gcd of $x^3 - 2x^2 + 1$ and $x^2 - x - 3$ in $\mathbb{Q}[x]$ and express it as a linear combination.

46. Prove that $\mathbb{Z}_2[x]/I$ is a field, where $p(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$ and $I = (p(x))$.

47. If R is a ring and $a \in R$, let $e_a : R[x] \to R$ be evaluation at a. Prove that $\ker e_a$ consists of all the polynomials over R having a as a root, and so $\ker e_a = (x - a)$, the principal ideal generated by $x - a$.

48. Let F be a field, and let $f(x), g(x) \in F[x]$. Prove that if $\partial(f) \leq \partial(g) = n$ and if $f(a) = g(a)$ for $n + 1$ elements $a \in F$, then $f(x) = g(x)$.

Prime Ideals and Maximal Ideals

The notion of prime number can be generalized to polynomials.

Definition. Let F be a field. A nonzero polynomial $p(x) \in F[x]$ is ***irreducible***[4] ***over*** F if $\partial(p) \geq 1$ and there is no factorization $p(x) = f(x)g(x)$ in $F[x]$ with $\partial(f) < \partial(p)$ and $\partial(g) < \partial(p)$.

Notice that irreducibility does depend on the coefficient field F. For example, $x^2 + 1$ is irreducible over $\mathbb{R}$, but it factors over $\mathbb{C}$. It is easy to see that linear polynomials (degree 1) are irreducible over any field F for which they are defined. It follows from Corollary 21 that irreducible polynomials of degree ≥ 2 over a field F have no roots in F. The converse is false, however, for $f(x) = x^4 + 2x^2 + 1 = (x^2 + 1)^2$ factors over $\mathbb{R}$, but it has no real roots.

[4]This notion can be generalized to any ring R. A nonzero element $r \in R$ is called ***irreducible*** if r is not a unit and, in every factorization $r = st$ in R, either s or t is a unit. If F is a field and $R = F[x]$, then this notion coincides with our definition of irreducible polynomial. In $\mathbb{Z}[x]$, however, $2x + 2 = 2(x + 1)$ is not irreducible, yet it does not factor into polynomials each of which has smaller degree.