MATH 403 Winter 2018
Homework 5
Winter 2018

1. **Problem 5.1** Let R be a commutative ring with identity. Then the map $R[x] \to R[x]$ that sends $r(x) \in R[x]$ to $r(x+1)$ is a ring isomorphism (What is its inverse?). Hence if $R = F$ is a field, a polynomial $f \in F[x]$ is irreducible if and only if $f(x+1)$ is irreducible. Now to prove Φ_p is irreducible in $\mathbf{Q}[x]$, it is equivalent to show that

$$\Phi_p(x+1) = x^{p-1} + \binom{p}{1} + \cdots + p$$

is irreducible. This can be done by applying Eisenstien's criterion with prime p.

2. **Problem 5.2** Suppose there are finitely many irreducible polynomials $\{p_1, \cdots, p_n(x)\}$ in $F[x]$. Consider the polynomial

$$F = \prod_{i=1}^{n} p_i(x) + 1.$$

Since F is a field, $F[x]$ is a principal ideal domain and in particular a unique factoriztion domain. Hence there exist finitely many p_i's such that, after rearranging,

$$F = \epsilon \prod_{i=1}^{l} p_i(x)$$

where $\epsilon \in F$. Then

$$p_1 | F = \prod_{i=1}^{n} p_i(x) + 1.$$

We also have $p_1(x) | \prod_{i=1}^{n} p_i(x)$ so that

$$p_1(x) | 1$$

which is impossible. Hence there are infinitely many irreducible polynomials in $F[x]$ for any field F.

3. **Problem 5.3** Sine every nonzero number in $\mathbf{Z}/p$ is relatively prime to p, we have that

$$(\mathbf{Z}/p)^{\times} = \{1, \cdots, p-1\}$$

is a group of size $p-1$. Hence these numbers all satisfy $x^{p-1} = 1$. In particular, they satisfy $x^p = x$. The element 0 obviously also satisfies $x^p = x$. We see that the polynomial $x^p - x$ has p distinct roots in $\mathbf{Z}/p$. Now recall that if F is a field and $f(x) \in F[x]$ has a root $\alpha \in F$, then $x - \alpha$ is a linear factor for F. But $x^p - x$ is of degree p so can have at most p linear factors. We get the result.

4. **Problem 5.4** Something stronger is true: The units in $F[x]$ is exactly $F - \{0\}$, namely, nonzero constants. Let me start with a commnet on degrees. If D is an integral domain, then for any polynomials $f, g \in D[x]$, we have

$$\deg(f \cdot g) = \deg f + \deg g.$$

This is not true if D is not an integral domain. For this, if a, b are two non-zero element in D with $a \cdot b = 0$, consider two degree 1 polynomials ax and bx in $D[x]$. Then

$$\deg(ax \cdot bx) = \deg abx^2 = \deg 0 = ?$$

Since F is a field, the above statement is true. If $f \in F[x]$ is not a constant polynomial, then for any other $g \in F[x]$, we have

$$\deg(f \cdot g) = \deg f + \deg g \geq \deg f \geq 1.$$

Hence it is impossible that $f \cdot g = 1$. This shows that if $f \in F[x]$ is a unit, f has to be a constant (non-zero of course). Conversely, since $F \subset F[x]$ is a subring, nonzero elements in F are automatically units in $F[x]$.

5. A polynomial $f = a_N x^N + \cdots a_0$ is of degree smaller than or equal to N if and only if each a_i is 0 or 1. Hence we have 2^{N+1} possibiilities. We have shown in problem 5.2 that there are infinitely many irreducible polynomials in $\mathbf{Z}/2[x]$. Hence if the degree of irreducible polynomials in $\mathbf{Z}/2[x]$ is bounded by an integer N, the size of the set of irreducible polynomials would be bounded by 2^{N+1}, a contradiciton.

6. **Problem 5.6** We may prove by contradiction. Suppose $f \in \mathbf{Q}[x]$ is not irreducible, then by Gauss' lemma, there exists $a, b \in \mathbf{Z}[x]$ such that $f = a \cdot b \in \mathbf{Z}[x]$ with $\deg a, \deg b < \deg f$. Then $f_p = a_p \cdot b_p$ where $(-)_p$ means the image of $- \in \mathbf{Z}[x]$ in $\mathbf{Z}/p[x]$ under the ring map $\mathbf{Z}[x] \to \mathbf{Z}/p[x]$. Then since p does not divide the leading coefficient of f, certainly p does not divide the leading coefficients of a and b. Then

$$\begin{aligned} \deg f &= \deg f_p \\ \deg a &= \deg a_p \\ \deg b &= \deg b_p \end{aligned}$$

We see that $\deg a_p, \deg b_p < f_p$ hence f_p is reducible in $\mathbf{Z}/p[x]$, a contradiciton.