MATH 3032: Abstract Algebra

Assignment 4

due 17 March 2025, end of day

Homework should be submitted as a single PDF attachment to `denisalja@dal.ca`. Please title the file in a useful way, for example `Math3032_HW#_Name.pdf`.

You are encouraged to work with your classmates, but your writing should be your own. If you do work with other people, please acknowledge (by name) whom you worked with. You are expected to think about every problem on every assignment, but you are not expected to solve every problem on every assignment. The purpose of homework assignments is to learn.

1. Let $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ for p a prime, and that $a \not\equiv 0 \pmod{p}$.
   (a) Show that $x^2 - x + a$ is irreducible in $\mathbb{F}_2[x]$.
   (b) Show that $x^3 - x + a$ is irreducible in $\mathbb{F}_3[x]$.

   It turns out (but harder to show) that $x^p - x + a$ is always irreducible in $\mathbb{F}_p[x]$ for any prime p and any $a \not\equiv 0 \pmod{p}$. Polynomials of this shape are called *Artin–Schreier polynomials*.

2. Find all integers n for which $x^3 + nx + 2$ is has a factor in $\mathbb{Q}[x]$. Why are there only finitely many?

3. Prove that the following polynomials are irreducible in $\mathbb{Z}[x]$:
   (a) $x^4 - 4x^3 + 6$.
   (b) $x^6 + 30x^5 - 15x^3 + 6x - 120$.
   (c) $x^4 + 4x^3 + 6x^2 + 2x + 1$. Hint: $x \rightsquigarrow x + 1$.
   (d) $\frac{(x+2)^p - 2^p}{x}$, where p is an odd prime.

4. Prove that $x^2 + y^2 - 1$ is irreducible in $\mathbb{Q}[x, y]$.

5. Prove that $f(x) = x^4 - 4x^2 + 8x + 2$ is irreducible over $\mathbb{Q}(\sqrt{-2})$. Hint: $\mathbb{Q}(\sqrt{-2})$ is the field of fractions of $\mathbb{Z}(\sqrt{-2})$, which is a UFD — why? Conclude that if $f(x)$ factors as linear×cubic, then the corresponding root divides 2 in $\mathbb{Z}(\sqrt{-2})$. But the factors of 2 therein are ± 1, $\pm\sqrt{-2}$, and ± 2 — why? Check these factors to conclude that there are no linear factors. Finally, use a similar argument to rule out a factorization as quadratic×quadratic.

6. (a) Show that in $(\mathbb{Z}/6\mathbb{Z})[x]$, we have a nontrivial factorization

$$x = (3x + 2)(2x + 3).$$

   Conclude that x is not irreducible in $(\mathbb{Z}/6\mathbb{Z})[x]$.
   (b) What happens when you reduce this factorization mod 2? What happens when you reduce it mod 3?

(c) Recall the Chinese Remainder Theorem: there is a ring isomorphism $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Use this to show that $(\mathbb{Z}/6\mathbb{Z})[x] \cong (\mathbb{Z}/2\mathbb{Z})[x] \times (\mathbb{Z}/3\mathbb{Z})[x]$. Use this to find all factorizations of x as a product of two factors in $(\mathbb{Z}/6\mathbb{Z})[x]$.

7. Recall that the nth *cyclotomic polynomial* is $\mathrm{cyc}_n(x) := \frac{x^n-1}{x-1} = x^{n-1} + x^{n-2} + \cdots + x + 1$. We showed in class that if n is prime, then $\mathrm{cyc}_n(x)$ is irreducible over $\mathbb{Q}$.

(a) Show that if r and s are relatively prime integers, then $\mathrm{cyc}_r(x)$ and $\mathrm{cyc}_s(x)$ have no common factors in $\mathbb{Q}[x]$. Hint: use Gauss's lemma to convert the problem to $\mathbb{Z}$. Hint: what is $\mathrm{cyc}_n(1)$?

(b) Suppose that $n = rs$. Show that $\mathrm{cyc}_n(x) = \mathrm{cyc}_r(x^s)\,\mathrm{cyc}_s(x)$. Conclude that $\mathrm{cyc}_r(x)$ and $\mathrm{cyc}_s(x)$ are both factors of $\mathrm{cyc}_n(x)$. Conclude that if r and s are relatively prime, then $\mathrm{cyc}_r(x)\,\mathrm{cyc}_s(x)$ is a factor of $\mathrm{cyc}_n(x)$. What is $\frac{\mathrm{cyc}_n(x)}{\mathrm{cyc}_r(x)\,\mathrm{cyc}_s(x)}$?

(c) Conclude that to understand how to factor arbitrary cyclotomic polynomials, it suffices to understand how to factor $\mathrm{cyc}_{p^\ell}(x)$. This is irreducible if $\ell = 1$. Suppose that $\ell = k+1$, and use the previous question to factor $\mathrm{cyc}_{p^{k+1}}(x) = \mathrm{cyc}_{p^k}(x)\,\mathrm{cyc}_p(x^{p^k})$. So by induction conclude that it suffices to understand how to factor $\mathrm{cyc}_p(x^{p^k}) = \frac{x^{p^{k+1}}-1}{x^{p^k}-1}$.

(d) Set

$$f(x) := \mathrm{cyc}_p((x+1)^{p^k}) = \frac{(x+1)^{p^{k+1}} - 1}{(x+1)^{p^k} - 1}.$$

Compute the constant term $f(0)$ of f. Hint: use L'Hôpital's rule.

(e) Show that if $0 < i < p^{k+1}$, then $\binom{p^{k+1}}{i}$ is divisible by p. Conclude that

$$f(x) = \frac{x^{p^{k+1}} + [\text{divisible by p}]}{x^{p^k} + [\text{divisible by p}]}.$$

Conclude that $f(x) = x^{p^k(p-1)} + [\text{divisible by p}]$. Hint: consider the ring map $\mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$.

(f) Conclude that Eisenstein's criterion applies to $f(x)$. Conclude that $\mathrm{cyc}_p(x^{p^k})$ is irreducible over $\mathbb{Q}$.