MATH 521A: Abstract Algebra

Homework 9 Solutions

1. Find the equivalence classes, and rules for addition and multiplication, in $\mathbb{Q}[x]/(x^2-2)$.

   The equivalence classes are $[ax+b]$, for every $a, b \in \mathbb{Q}$. We have $[ax+b]+[cx+d] = [(a+c)x+(b+d)]$, and $[ax+b][cx+d] = [(ad+bc)x+(2ac+bd)]$.

2. Find the equivalence classes, and rules for addition and multiplication, in $\mathbb{Q}[x]/(x^2)$.

   The equivalence classes are $[ax+b]$, for every $a, b \in \mathbb{Q}$. We have $[ax+b]+[cx+d] = [(a+c)x+(b+d)]$, and $[ax+b][cx+d] = [(ad+bc)x+bd]$.

3. Find the equivalence classes, and rules for addition and multiplication, in $\mathbb{Q}[x]/(x^2+1)$.

   The equivalence classes are $[ax+b]$, for every $a, b \in \mathbb{Q}$. We have $[ax+b]+[cx+d] = [(a+c)x+(b+d)]$, and $[ax+b][cx+d] = [(ad+bc)x+(-ac+bd)]$.

4. For exercises 1-3, find all the units and zero divisors.

   In problems $1, 3$, the rings are actually fields since x^2-2 and x^2+1 are both irreducible over $\mathbb{Q}$ (using the rational root test). Hence every element, except $[0x+0]$, is a unit, and there are no zero divisors. In problem 2, the nonzero elements $[ax]$ are all zero divisors, for any nonzero $a \in \mathbb{Q}$, because $[ax][x] = [0]$. All other nonzero elements may be written as $[ax+b]$ with $b \neq 0$ and a arbitrary. We have $[ax+b][-\frac{a}{b^2}x+\frac{1}{b}] = [1]$, so $[ax+b]$ is a unit.

5. For exercises 1-3, find the inverse of $[3x-2]$ (in each respective ring).

   Exercise 1: Suppose $[3x-2][ax+b] = [1]$. We multiply and get the system of equations $\{3b-2a = 0, -2b+6a = 1\}$, which we solve. Hence $[3x-2][\frac{1}{14}(3x+2)] = [1]$.
   Exercise 2: As above, $[3x-2][-\frac{3}{4}x-\frac{1}{2}] = [1]$.
   Exercise 3: Suppose again $[3x-2][ax+b] = [1]$. This time we get $\{3b-2a = 0, -2b-3a = 1\}$, which we solve and conclude $[3x-2][\frac{1}{13}(-3x-2)] = [1]$.

6. Find a zero divisor in $\mathbb{Z}_2[x]/(x^4+x^2+1)$.

   Note that $[x^4+x^2+1] = [0]$, so what we're looking for is a nontrivial divisor of x^4+x^2+1, over $\mathbb{Z}_2$. This has no roots, but fortunately we can factor $x^4+x^2+1 = (x^2+x+1)^2$. Hence $[x^2+x+1]$ is a zero divisor, as are it multiples $[x^3+x^2+x]$ and $[x^3+1]$.

7. If $f(x) \in F[x]$ has degree n, prove that there is an extension field E of F so that $f(x)$ splits. That is, $f(x) = c_0(x-c_1)(x-c_2)\cdots(x-c_n)$ for some (not necessarily distinct) $c_i \in E$. Prove that the degree of E over F is at most $n!$.

   We prove this by induction on n. If $n = 1$ then $f(x)$ already splits in F, and $[F:F] = 1 = 1!$. This completes the base case.

   We first assume that $f(x)$ is irreducible. Set $G = F[x]/(f(x))$. G contains a root r of f, so by the root theorem, in $G[x]$, we have $f(x) = (x-r)g(x)$, for some polynomial $g(x)$ of degree $n-1$. We have $[G:F] = n$. By the inductive hypothesis, there is some extension field E of G in which $g(x)$ splits, with $[E:G] \leq (n-1)!$. We have $[E:F] = [E:G][G:F] \leq (n-1)!n = n!$.

   We now assume that $f(x)$ is reducible, i.e. $f(x) = g(x)h(x)$. Suppose $\deg(g) = k$ and $\deg(h) = n-k$, both positive integers. We apply the inductive hypothesis to find an extension field G of F so that $g(x)$ splits. Hence, in $G[x]$, we have $f(x) = (\text{linear factors})h(x)$. Now we apply the inductive hypothesis again to find an extension field E of G so that $h(x)$ splits. We have $[E:F] = [E:G][G:F] \leq k!(n-k)!$. But we know that the binomial coefficient $\frac{n!}{k!(n-k)!}$ is an integer, so in particular $k!(n-k)! \leq n!$.

8. Let $f(x) = x^3 + x + 1$, and set $E = \mathbb{Z}_2[x]/(x^3 + x + 1)$. Prove that $f(x)$ splits in E. That is, find three distinct roots of $f(x)$ in E.

Since $f(x)$ has no roots in $\mathbb{Z}_2$, and is of degree 3, it is irreducible. Hence we know already that $[x]$ is a root, i.e. $[x]^3 + [x] + [1] = [0]$. A bit of trial and error (not too much, since there are only eight ring elements) finds the other roots $[x^2]$ and $[x^2 + x]$. We verify: $f(x^2) = x^6 + x^2 + 1$, and $x^6 = (x^3)^2 = (x+1)^2 = x^2 + 1$. Hence $f(x^2) = 0$. Also, $f(x^2 + x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. We have $x^6 = x^2 + 1, x^5 = x^2 + x + 1, x^4 = x^2 + x, x^3 = x + 1$. Plugging all of these in, and summing in $\mathbb{Z}_2$, gives $f(x^2 + x) = 0$.

9. Find a field with eight elements, and give the addition and multiplication table.

We need some irreducible third-degree polynomial in $\mathbb{Z}_2[x]$. Fortunately there are two: $p(x) = x^3 + x + 1$ and $q(x) = x^3 + x^2 + 1$. Hence we have our choice of $\mathbb{Z}_2[x]/(p(x))$ or $\mathbb{Z}_2[x]/(q(x))$. These are isomorphic, because there is a unique field with p^k elements, for every prime p and every $k \in \mathbb{N}$. Below is the answer with $p(x)$.

$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

$\times$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

10. Prove that:
(a) $2\cos\frac{2\pi}{5} = e^{2\pi i/5} + e^{-2\pi i/5}$ satisfies $x^2 + x - 1 = 0$; and
(b) $2\cos\frac{2\pi}{7} = e^{2\pi i/7} + e^{-2\pi i/7}$ satisfies $x^3 + x^2 - 2x - 1 = 0$.

(a) We plug in, expand, and simplify to get $e^{2\pi i/5} + e^{4\pi i/5} + e^{6\pi i/5} + e^{8\pi i/5} + e^{10\pi i/5}$. This is the sum of the five complex fifth roots of unity, which is zero by symmetry.
(b) We plug in, expand, and simplify to get $e^{2\pi i/7} + e^{4\pi i/7} + e^{6\pi i/7} + e^{8\pi i/7} + e^{10\pi i/7} + e^{12\pi i/7} + e^{14\pi i/7}$. This is the sum of the seven complex seventh roots of unity, which is again zero.

11. Use Problem 10 to prove that the regular pentagon is constructible with straightedge and compass, while the regular septagon (seven edges) is not.

First, the regular pentagon (resp. septagon) is constructible exactly when $2\cos\frac{2\pi}{5}$ (resp. $2\cos\frac{2\pi}{7}$) is, since this translates easily to the edge lengths. Polynomial $x^2 + x - 1$ has no rational roots (by the rational root test) and hence is irreducible over $\mathbb{Q}$ since it is of degree 2. Set $E = \mathbb{Q}[x]/(x^2 + x - 1)$. We have $[E : \mathbb{Q}] = 2$, since $x^2 + x - 1$ is degree 2, and the desired $2\cos\frac{2\pi}{5}$ lies in E. Hence we may construct the pentagon.

Polynomial $x^3 + x^2 - 2x - 1$ also has no rational roots, and also is irreducible over $\mathbb{Q}$ since it is of degree 3. Since 3 is not a power of 2, no root of $x^3 + x^2 - 2x - 1$ is constructible, and in particular the septagon is not constructible.