Math 236
Fall 2008
Dr. Seelinger

Solutions for §§5.2 and 5.3

Section 5.2

Problem 7. Consider $R = \mathbb{Q}[x]/(x^2-3)$. Each element of R can be written in the form $[ax+b]$. (Why?) Determine the rules for addition and multiplication of congruence classes.

First, note that by Corollary 5.5 that every congruence class in $R = \mathbb{Q}[x]/(x^2-3)$ has a unique representative of degree 1 or less (including the zero polynomial). Therefore every element of $R = \mathbb{Q}[x]/(x^2-3)$ can be written in the form $[ax+b]$ where $a, b \in \mathbb{Q}$. Let $[ax+b], [cx+d] \in R$. Then, by Theorem 5.6,

$$[ax+b] + [cx+d] = [(a+c)x + (b+d)]$$

and

$$[ax+b][cx+d] = [acx^2 + (ad+bc)x + bd] = [ac(3) + (ad+bc)x + bd] = [(ad+bc)x + (3ac+bd)].$$

Problem 14: In each part explain why $[f(x)]$ is a unit in $F[x]/(p(x))$ and find its inverse.
(a) $[f(x)] = [2x-3] \in \mathbb{Q}[x]/(x^2-2)$.

When we divide x^2-2 by $2x-3$ we get a quotient of $\frac{x}{2} + \frac{3}{4}$ and a remainder of $\frac{1}{4}$. Therefore, we get

$$(x^2-2) = \left(\frac{x}{2} + \frac{3}{4}\right)(2x-3) + \frac{1}{4} \Rightarrow 4(x^2-2) + (-2x-3)(2x-3) = 1.$$

If we reduce this equation modulo x^2-2, we get $[2x-3][-2x-3] = [1]$, hence $[2x-3]$ is a unit in $\mathbb{Q}[x]/(x^2-2)$ and $[2x-3]^{-1} = [-2x-3]$.

(b) $[f(x)] = [x^2+x+1] \in \mathbb{Z}_3[x]/(x^2+1)$.

We use the Euclidean Algorithm to get the gcd of $f(x)$ and $p(x) = x^2+1$. So, when we divide $p(x)$ by $f(x)$ we get $q_1(x) = 1$ and $r_1(x) = 2x$. Now we divide $f(x)$ by $r_1(x)$ and get $q_2(x) = 2x+2$ and $r_2(x) = 1$. Hence $\gcd(f(x), p(x)) = 1$, so by Theorem 5.9, $[f(x)]$ is a unit in $\mathbb{Z}_2[x]/(x^2+1)$. Furthermore,

$$f(x) = (2x+2)(2x) + 1 \Rightarrow 1 = f(x) + (x+1)(2x) = f(x) + (x+1)(p(x) - f(x)).$$

Hence, when we reduce the above equation modulo $p(x)$ we get $[1] = [f(x)][2x]$ so $[f(x)]^{-1} = [2x]$.

(c) $[f(x)] = [x^2+x+1] \in \mathbb{Z}_2[x]/(x^3+x+1)$.

We again use the Euclidean Algorithm to find the gcd of $f(x)$ and $p(x) = x^3+x+1$. So we divide $p(x) = x^3+x+1$ by $f(x)$ and get $q_1(x) = x+1$ and $r_1(x) = x$. Next, we divide $f(x)$ by $r_1(x)$ and get $q_2(x) = x+1$ and $r_2(x) = 1$. Therefore, $\gcd(f(x), p(x)) = 1$ so by Theorem 5.9, $[f(x)]$ is a unit in $\mathbb{Z}_2[x]/(x^3+x+1)$. Also, we have

$$1 + (x+1)(x) = f(x) \Rightarrow 1 = f(x) + (x+1)(x) = f(x) + (x+1)(p(x) + (x+1)f(x))$$

$$\Rightarrow 1 = (x+1)p(x) + x^2 f(x).$$

When we reduce this modulo $p(x)$ we get $[1] = [f(x)][x^2]$, so $[f(x)]^{-1} = [x^2]$.

Section 5.3

Problem 5(a). Verify that $\mathbb{Q}(\sqrt{3}) = \{r + s\sqrt{3} : r, s \in \mathbb{Q}\}$ is a subfield of of $\mathbb{R}$.
(b). Show that $\mathbb{Q}(\sqrt{3})$ is isomorphic to $\mathbb{Q}[x]/(x^2 - 3)$.

(a) First we check that $\mathbb{Q}(\sqrt{3})$ is a subring of $\mathbb{R}$. Note that $0 = 0 + 0\sqrt{3} \in \mathbb{Q}(\sqrt{3})$. Also, if $a + b\sqrt{3}, c + d\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ we have $(a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c) + (b + d)\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ and $(a+b\sqrt{3})(c+d\sqrt{3}) = (ac+3bd)+(ad+bc)\sqrt{3} \in \mathbb{Q}(\sqrt{3})$. Finally, $-(a+b\sqrt{3}) = -a+(-b)\sqrt{3} \in \mathbb{Q}(\sqrt{3})$, so by Theorem 3.2, $\mathbb{Q}(\sqrt{3})$ is a subring of $\mathbb{R}$. Since $\mathbb{R}$ is commutative, so is $\mathbb{Q}(\sqrt{3})$. Also $1 = 1 + 0\sqrt{3} \in \mathbb{Q}(\sqrt{3})$, so it is a commutative ring with identity. Finally, for any $a + b\sqrt{3} \neq 0$ we have

$$(a + b\sqrt{3})^{-1} = \left(\frac{a}{a^2 - 3b^2}\right) + \left(\frac{-b}{a^2 - 3b^2}\right)\sqrt{3} \in \mathbb{Q}(\sqrt{3}).$$

Since every non-zero element of $\mathbb{Q}(\sqrt{3})$ has a multiplicative inverse since $a^2 - 3b^2 \neq 0$ for any rational numbers a and b.

(b) Let us define a function $\phi : \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}[x]/(x^2 - 3)$ by letting $\phi(a + b\sqrt{3}) = [a + bx]$ for any $a, b \in \mathbb{Q}$. We need to show that ϕ is an isomorphism. We first show properties (H1) and (H2). Let $a + b\sqrt{3}, c + d\sqrt{3} \in \mathbb{Q}(\sqrt{3})$. Then

$$\phi((a + b\sqrt{3}) + (c + d\sqrt{3})) = \phi((a + c) + (b + d)\sqrt{3}) = [(a + c) + (b + d)x]$$

$$= [a + bx] + [c + dx] = \phi(a + b\sqrt{3}) + \phi(c + d\sqrt{3})$$

So (H1) holds. Also,

$$\phi((a + b\sqrt{3})(c + d\sqrt{3})) = \phi((ac + 3bd) + (ad + bc)\sqrt{3}) = [(ac + 3bd) + (ad + bc)x]$$

while

$$phi(a + b\sqrt{3})\phi(c + d\sqrt{3}) = [a + bx][c + dx] = [ac + (ad + bc)x + bdx^2] = [(ac + 3bd) + (ad + bc)x]$$

since $[x^2] = [3]$ in $\mathbb{Q}[x]/(x^2 - 3)$. Therefore, (H2) also holds.

Next, assume $\phi(a + b\sqrt{3}) = \phi(c + d\sqrt{3}) \Rightarrow [a + bx] = [c + dx]$. By Corollary 5.5, there is a unique polynomial of degree 1 or less (including the zero polynomial) for each congruence class modolu $p(x)$. Therefore, $a + bx = c + dx \Rightarrow a = c$ and $b = d$. Hence $a + b\sqrt{3} = c + d\sqrt{3}$ so ϕ is injective.

Now let y be a congruence class in $\mathbb{Q}[x]/(x^2 - 3)$. By Corollary 5.5, $y = [r + sx]$ for some $r, s \in \mathbb{Q}$. So $\phi(r + s\sqrt{3}) = [r + sx] = y$, hence ϕ is surjective. Therefore, ϕ is an isomorphism and hence $\mathbb{Q}(\sqrt{3})$ is isomorphic to $\mathbb{Q}[x]/(x^2 - 3)$. Q.E.D.

Problem 6: Let $p(x)$ be irreducible in $F[x]$. If $[f(x)] \neq [0_F]$ in $F[x]/(p(x))$ and $h(x) \in F[x]$, prove that there exists $g(x) \in F[x]$ such that $[f(x)][g(x)] = [h(x)]$ in $F[x]/(p(x))$.

Proof. Since $p(x)$ is irreducible in $F[x]$, by Theorem 5.10 we have $F[x]/(p(x))$ is a field. Therefore, since $[f(x)] \neq [0_F]$, there exists an element $[f_0(x)] = [f(x)]^{-1} \in F[x]/(p(x))$. So let $[g(x)] = [f(x)]^{-1}[h(x)]$. Then

$$[f(x)][g(x)] = [f(x)]([f(x)]^{-1}[h(x)]) = ([f(x)][f(x)]^{-1})[h(x)] = [h(x)].$$

Hence $g(x) = f_0(x)h(x) \in F[x]$ works. Q.E.D.

Problem 9(a): Show that $\mathbb{Z}_2[x]/(x^3 + x + 1)$ is a field.
(b): Show that the field $\mathbb{Z}_2[x]/(x^3 + x + 1)$ contains all three roots of $x^3 + x + 1$.

(a) By Theorem 5.10 it is sufficient to show that $x^3 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$. But $x^3 + x + 1$ has no roots in $\mathbb{Z}_2$, hence by Corollary 4.18 $x^3 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$. Therefore, by Theorem 5.10, $K = \mathbb{Z}_2[x]/(x^3 + x + 1)$ is a field.

(b) Let $u = [x] \in K = \mathbb{Z}_2[x]/(x^3 + x + 1)$. Then by Theorem 5.11 we know $u \in K$ is a root of $p(x) = x^3 + x + 1 \in \mathbb{Z}_2[x] \subseteq K[x]$. Therefore, by the Factor Theorem, $(x - u)$ is a factor of $x^3 + x + 1$ in $K[x]$. By doing long division, we find that $x^3 + x + 1 = (x - u)(x^2 + ux + (1 + u^2))$. Let $g(x) = x^2 + ux + (1 + u^2)$. In order to finish the problem, we need to show that $g(x)$ has two roots in K. Note that $g(u^2) = 0$ and $g(u^2 + u) = 0$. Therefore, $x^3 + x + 1$ has three roots, $u, u^2, u^2 + u$ in K. By Corollary 4.16 these are all the roots of $x^3 + x + 1$. Q.E.D.