MAT 612
04/25/10

HW #6 Solutions[1]

9.3.1 Arguing by contradiction, suppose R is a UFD. Since $p(x) = a(x)b(x)$ in $F[x]$, and $p \in R[x]$, Gauss' Lemma implies $\exists \beta \in F$ such that βa and $\beta^{-1}b$ are in $R[x]$. Since b is monic, $\beta^{-1} \in R$, hence $a = \beta^{-1}(\beta a) \in R[x]$, a contradiction. We don't need the assumption that a and b have smaller degree than p. For the second part, note that $(x+\sqrt{2})(x+\sqrt{2}) = x^2 + 2\sqrt{2}x + 8$. The latter polynomial lies in $\mathbb{Z}[2\sqrt{2}]$, and is monic. But $\sqrt{2} \notin \mathbb{Z}[2\sqrt{2}]$. (If it were, then $\sqrt{2} = a + 2b\sqrt{2}$ for some $a, b \in \mathbb{Z}$, and then $\sqrt{2} = \frac{a}{1-2b} \in \mathbb{Q}$, contradiction.) Thus $x + \sqrt{2} \notin \mathbb{Z}[2\sqrt{2}]$, and $x + \sqrt{2}$ is monic. By the first part, $\mathbb{Z}[2\sqrt{2}]$ is not a UFD. Note: $2\sqrt{2}$ is irreducible in $\mathbb{Z}[2\sqrt{2}]$ (exercise), so 8 has two distinct factorizations into irreducibles in $\mathbb{Z}[2\sqrt{2}]$: $8 = 2^3 = (2\sqrt{2})^2$.

9.4.2 (a) $x^4 - 4x^3 + 6$ is irreducible in $\mathbb{Z}[x]$ by Eisenstein with $p = 2$. (b) $x^6 + 30x^5 - 15x^3 + 6x - 120$ is irreducible in $\mathbb{Z}[x]$ by Eisenstein with $p = 3$. (c) If $p(x) = x^4 + 4x^3 + 6x^2 + 2x + 1$, then $p(x-1) = x^4 - 2x + 2$, which is irreducible by Eisenstein with $p = 2$. If $p(x) = a(x)b(x)$, then $p(x-1) = a(x-1)b(x-1)$. Since $a(x)$ is a unit if and only if $a(x-1)$ is a unit, and similarly for b, it follows that $p(x)$ is irreducible in $\mathbb{Z}[x]$. (d) $f(x) = \frac{(x-2)^p - 2^p}{x} = x^{p-1} + \sum_{k=1}^{p-1} \binom{p}{k} 2^k x^{p-k-1}$. Eisenstein's criterion applies: p divides $\binom{p}{k}$, hence $\binom{p}{k} 2^k$ for each $1 \le k \le p-1$, and p^2 does not divide $\binom{p}{p-1} 2^{p-1} = p = 2^{p-1}$ because p is odd by assumption. Hence f is irreducible.

9.4.6(a) From 9.4.1(b), the prime factorization of $x^3 + x + 1$ over $\mathbb{F}_3$ is $(x-1)(x^2+x-1)$. In particular, $p(x) = x^2 + x - 1$ is irreducible over $\mathbb{F}_3[x]$. Let $F = \mathbb{F}_3[x]/(p(x))$. Since $p(x)$ is prime in the PID $\mathbb{F}_3[x]$, $(p(x))$ is a maximal ideal, hence F is a field. Note that $\mathrm{char}(F) = 3$, and the natural map $\mathbb{F}_3 \to F$ is injective. The element $\alpha \in F$ represented by x satisfies $p(\alpha) = 0$, hence α is algebraic over $\mathbb{F}_3$, and $m_\alpha^{\mathbb{F}_3}(x) = p(x)$, since p is monic and irreducible over $\mathbb{F}_3$. Hence $|F : \mathbb{F}_3| = \deg(p) = 2$, so $|F| = |\mathbb{F}_3|^2 = 9$. (Note: the elements of F have the form $a + b\alpha$ for $a, b \in \mathbb{F}_3$, and $\alpha^2 = 1 - \alpha$.)

9.4.7 Define $f : \mathbb{R}[x] \to \mathbb{C}$ by $f(p(x)) = p(i)$. Then f is onto because every element of $\mathbb{C}$ can be expressed in the form $a + bi$ for $a, b \in \mathbb{R}$. The kernel of f is the principal ideal generated by the minimal polynomial of i over $\mathbb{R}$, which is clearly equal to $x^2 + 1$. Thus $\mathbb{R}[x]/(x^2+1)$ is isomorphic to $\mathbb{C}$.

13.1.1 $p(x) = x^3 + 9x + 6$ is irreducible over $\mathbb{Z}[x]$ by Eisenstein's Criterion, with $p = 3$. Then $p(x)$ is irreducible in $\mathbb{Q}[x]$ by Gauss' Lemma. Let θ be a root of $p(x)$, and let $\beta = 1 + \theta$.Since $\beta \in \mathbb{Q}[\theta]$, which has degree three over $\mathbb{Q}$, β must be a root of a cubic polynomial in $\mathbb{Q}[x]$. We have $\beta^2 = 1 + 2\theta + \theta^2$ and $\beta^3 = 1 + 3\theta + 3\theta^2 + \theta^3 = 1 + 3\theta + 3\theta^2 + (-6 - 9\theta) = -5 - 6\theta + 3\theta^2$. A little linear algebra reveals that $\beta^3 - 3\beta^2 + 12\beta - 4 = 0$. Then $\beta(\beta^2 - 3\beta + 12) = 4$. Thus $(1+\theta)^{-1} = \beta^{-1} = \frac{1}{4}(\beta^2 - 3\beta + 12) = \frac{5}{2} - \frac{1}{4}\theta + \frac{1}{4}\theta^2$.

[1] exercises from Dummit and Foote, *Abstract Algebra*, 3rd ed.

13.1.2 $p(x) = x^3 - 2x - 2$ is irreducible over $\mathbb{Q}$ by Gauss' Lemma and the Eisenstein Criterion with $p = 2$. Let $p(\theta) = 0$. Then $\theta^3 = 2+2\theta$ so $(1+\theta)(1+\theta+\theta^2) = 1+2\theta+2\theta^2+\theta^3 = 3+4\theta+2\theta^2$.

As in 13.1.1, we set $\beta = 1 + \theta + \theta^2$ and compute (using *Mathematica* to some extent) $\beta^2 = 5 + 8\theta + 5\theta^2$, and $\beta^3 = 31 + 49\theta + 28\theta^2$. We then find that $\beta^3 - 7\beta^2 + 7\beta - 3 = 0$. Then $\beta(\beta^2 - 7\beta + 7) = 3$, so $\beta^{-1} = \frac{1}{3}(\beta^2 - 7\beta + 7) = \frac{1}{3}(5 + \theta - 2\theta^2)$ Then $\frac{1+\theta}{1+\theta+\theta^2} = (1 + \theta)(\frac{1}{3}(5 + \theta - 2\theta^2)) = \frac{1}{3}(1 + 2\theta - \theta^2) = \frac{1}{3} + \frac{2}{3}\theta - \frac{1}{3}\theta^2$.

13.2.2 As shown above in 9.4.6(a), $h(x)$ is irreducible over $\mathbb{F}_3$. Similarly, since $g(0) = 1$ and $g(1) = 1$ in $\mathbb{F}_2$, g is irreducible over $\mathbb{F}_2$, $g(0) = -1, g(1) = 1, g(2) = 2$ in $\mathbb{F}_3$, so g is irreducible over $\mathbb{F}_3$, and $h(0) = 1$ and $h(1) = 1$ in $\mathbb{F}_2$, so $h(x)$ is irreducible over $\mathbb{F}_2$. Then $F = \mathbb{F}_3[x]/(g(x))$ is a field with $3^2 = 9$ elements, as shown above, and, similarly, $\mathbb{F}_3[x]/(h(x))$ is a field with $3^3 = 27$ elements, $K = \mathbb{F}_2[x]/(g(x))$ is a field with $2^2 = 4$ elements, and $\mathbb{F}_2[x]/(h(x))$ is a field with $2^3 = 8$ elements. Here are the multiplication tables - let α denote the image of x in K and F, respectively.

K	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

F	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
2	0	2	1	2α	α	$2+2\alpha$	$2+\alpha$	$1+2\alpha$	$1+\alpha$
α	0	α	2α	$1+2\alpha$	$2+\alpha$	1	$2+2\alpha$	$1+\alpha$	2
2α	0	2α	α	$2+\alpha$	$1+2\alpha$	2	$1+\alpha$	$2+2\alpha$	1
$1+\alpha$	0	$1+\alpha$	$2+2\alpha$	1	2	$2+\alpha$	α	2α	$1+2\alpha$
$1+2\alpha$	0	$1+2\alpha$	$2+\alpha$	$2+2\alpha$	$1+\alpha$	α	2	1	2α
$2+\alpha$	0	$2+\alpha$	$1+2\alpha$	$1+\alpha$	$2+2\alpha$	2α	1	2	α
$2+2\alpha$	0	$2+2\alpha$	$1+\alpha$	2	1	$1+2\alpha$	2α	α	$2+\alpha$

We can see that $K^\times$ is cyclic of order three, generated by α, and $F^\times$ is cyclic of order 8. Looking at the diagonal entries, we see that 2 has order 2, so $1 + 2\alpha$ has order 4, and thus α has order 8, so α generates $F^\times$. ($1 + \alpha = \alpha^{-1}, 2 + 2\alpha = \alpha^3$, and $2\alpha = \alpha^5$ also generate $F^\times$.)