HONORS ALGEBRA: SOLUTIONS TO HOMEWORK 12

4.4, Q9. Define $U_p = \{x : x \in \mathbb{Z}_p \setminus \{0\}\}$ and $V_p = \{x^2 : x \in \mathbb{Z}_p \setminus \{0\}\}$. Then U_p is a multiplicative group, as we have seen earlier in the course. We define the map $\varphi : U_p \to V_p$ by putting $\varphi(x) = x^2$. This defines a group homomorphism (again, we have seen this earlier in the course) which is evidently surjective. Using the field property of $\mathbb{Z}_p$, we find that $\ker(\varphi) = \{x \in U_p : x^2 = 1\} = \{+1, -1\}$. To see this, observe that if $x^2 = 1$, then $(x+1)(x-1) = 0$, so the integral domain property of $\mathbb{Z}_p$ shows that $x + 1 = 0$ or $x - 1 = 0$. We thus deduce from the First Homomorphism Theorem that $V_p \cong U_p/\ker(\varphi) = U_p/\{+1, -1\}$. Then V_p is a subgroup of U_p of order $|U_p|/2 = (p-1)/2$. Thus V_p is a normal subgroup of U_p with two cosets V_p and aV_p, for some $a \in U_p$. Since no element of aV_p lies in V_p, none of these elements are quadratic residues modulo p, and we have $|aV_p| = |V_p| = (p-1)/2$ quadratic non-residues modulo p. The remaining elements of U_p lie in V_p and are quadratic residues modulo p, the number of which is $|V_p| = (p-1)/2$.

4.4, Q10. The set R is a subset of the ring of real numbers. Thus, to show that R is a ring, it suffices to check that it is a subring of $\mathbb{R}$. Plainly $0 \in R$, so R is nonempty. Also, if $a_i, b_i \in \mathbb{Z}$ $(i = 1, 2)$, then $(a_1 + \sqrt{m}b_1) \pm (a_2 + \sqrt{m}b_2) = (a_1 \pm a_2) + \sqrt{m}(b_1 \pm b_2) \in R$, and also $(a_1 + \sqrt{m}b_1)(a_2 + \sqrt{m}b_2) = (a_1a_2 + mb_1b_2) + \sqrt{m}(a_1b_2 + a_2b_1) \in R$, so R does indeed form a subring of $\mathbb{R}$, and is hence a ring.

4.4, Q11. We have that $0 \in I_p$, so I_p is not empty. Also, whenever a_i, b_i are integers divisible by p for $i = 1, 2$, say $a_i = pc_i$ and $b_i = pd_i$, then $(a_1 + \sqrt{m}b_1) \pm (a_2 + \sqrt{m}b_2) = p(c_1 \pm c_2) + \sqrt{m}p(d_1 \pm d_2) \in I_p$, so that I_p forms an additive subgroup of R. Moreover, whenever $u, v \in \mathbb{Z}$, we have $(u + \sqrt{m}v)(a_1 + \sqrt{m}b_1) = (u + \sqrt{m}v)(pc_1 + \sqrt{m}pd_1) = p(uc_1 + mvd_1) + \sqrt{m}p(ud_1 + vc_1) \in I_p$. Thus, since I_p is commutative, it follows that I_p is an ideal of R.

4.4, Q12. Consider the quotient ring R/I_p. This consists of the cosets $u+\sqrt{m}v+I_p$, with $0 \le u, v < p$. This is a commutative ring with unit $1 + I_p$. Suppose now that $\alpha = u + \sqrt{m}v + I \ne I$, so that $u + \sqrt{m}v + I$ is not the zero element in R/I_p. We claim that α has a multiplicative inverse in R/I_p, so that R/I_p is a division ring and hence a field. To see this, observe that when m is a quadratic non-residue modulo p, and v is non-zero in $\mathbb{Z}_p$, one has $u^2 - mv^2 = v^2((uv^{-1})^2 - m)$, and so $u^2 - mv^2$ is divisible by p if and only if u and v are both divisible by p. When u and v are not both divisible by p, therefore, the integer $u^2 - mv^2$ has a multiplicative inverse modulo p, say w. We now have $(w(u - \sqrt{m}v) + I)\alpha = w(u - \sqrt{m}v)(u + \sqrt{m}v) + I = w(u^2 - mv^2) + I = 1 + I$, so that $w(u - \sqrt{m}v) + I$ is a multiplicative inverse of α. It follows that R/I_p is a field, and hence that I_p is a maximal ideal (Theorem 4.4.3).

4.4, Q13. Since I_p is a maximal ideal of R, it follows that R/I_p is a field. Moreover, when $a_i, b_i \in \mathbb{Z}$, one has $a_1 + \sqrt{m}b_1 + I_p = a_2 + \sqrt{m}b_2 + I_p$ if and only if $(a_1 - a_2) + \sqrt{m}(b_1 - b_2) \in I_p$. But when $c, d \in \mathbb{Z}$, if one has $c + \sqrt{m}d \in I_p$, then $c + \sqrt{m}d = u + \sqrt{m}v$ for some $u, v \in \mathbb{Z}$ with $p|u$ and $p|v$. Thus $(c-u)^2 = m(v-d)^2$, which shows that $u^2 \equiv mv^2 \pmod{p}$. This is possible when m is a quadratic non-residue only when $p|u$ and $p|v$. Hence $a_1 \equiv a_2 \pmod{p}$ and $b_1 \equiv b_2 \pmod{p}$. Then the distinct cosets of I_p in R are given by $a + \sqrt{m}b + I_p$, with $0 \le a, b < p$, and thus the field R/I_p has p^2 elements.

4.5, Q3. (a) By using the division algorithm, we obtain

$$x^3 - 6x + 7 = (x^2 - 4x + 10)(x + 4) - 33,$$

so the greatest common divisor of $x^3 - 6x + 7$ and $x + 4$ divides 33 and hence is 1.
(b) Likewise,

$$2x^7 - 4x^5 + 2 = (2x^5 - 2x^3 - 2x)(x^2 - 1) - 2x + 2,$$

and

$$x^2 - 1 = \Big(-\frac{1}{2}x + \frac{1}{2}\Big)(-2x - 2) + 0,$$

so the greatest common divisor of $2x^7 - 4x^5 + 2$ and $x^2 - 1$ divides $2x - 2$ and hence is $x - 1$.
(c) Similarly,

$$x^6 + x^4 + x + 1 = \Big(\frac{1}{3}x^4 + \frac{2}{9}x^2 - \frac{2}{27})(3x^2 + 1) + x + \frac{29}{27},$$

and

$$3x^2 + 1 = \Big(3x - \frac{29}{9}\Big)\Big(x + \frac{29}{27}\Big) + \frac{1084}{243},$$

so the greatest common divisor of $x^6 + x^4 + x + 1$ and $3x^2 + 1$ divides $\frac{1084}{243}$ and hence is 1.
(d) Finally,

$$x^7 - x^4 + x^3 - 1 = (x^4 + 1)(x^3 - 1),$$

so the greatest common divisor of $x^7 - x^4 + x^3 - 1$ and $x^3 - 1$ divides $x^3 - 1$ and hence is $x^3 - 1$.

4.5, Q5. In all cases we find that $d(x) = (a(x), b(x))$ divides any element of I, so that $I \subseteq (d(x))$. Moreover, since there exist $f, g \in \mathbb{Q}[x]$ such that $d(x) = a(x)f(x) + b(x)g(x)$, we see that $(d(x)) \subseteq I$. Thus $I = d(x) = (a(x), b(x))$.
(a) We have $d(x) = (a(x), b(x)) = 1$.
(b) We have $d(x) = (a(x), b(x)) = x - 1$.
(c) We have $d(x) = (a(x), b(x)) = 1$.
(d) We have $d(x) = (a(x), b(x)) = x^3 - 1$.

4.5, Q12. If $f(x)$ and $g(x)$ are relatively prime in $F[x]$, then (Theorem 4.5.7) there are polynomials $a(x), b(x) \in F[x]$ for which $af + bg = 1$. Since $F \subseteq K$, this last relation holds also in $K[x]$, and thus any common divisor $d \in K[x]$ of f and g must divide 1. It follows that the greatest common divisor of f and g in $K[x]$ is a monic constant polynomial, namely 1, and hence f and g are also relatively prime in $K[x]$.

4.5, Q18. Suppose that all irreducible polynomials in $F[x]$ have degree bounded by N. Since F is finite, this implies that there are just finitely many irreducible polynomials, and we may label these $p_1, \ldots, p_n$ for some natural number n. Now consider the polynomial $P(x) = p_1(x)p_2(x) \cdots p_n(x) + 1$. We see that $(P(x), p_i(x)) = 1$ for each i, so that $P(x)$ is not divisible by any irreducible polynomial. But Theorem 4.5.12 shows that $P(x)$ is either irreducible, or the product of irreducible polynomials. Then $P(x)$ must be irreducible, yet is not one of the (exhaustive) list of irreducible polynomials in $F[x]$. This yields a contradiction which forces us to conclude that there are irreducible polynomials of arbitrarily large degree.