Math 463/563 - Homework 4

6.2 Define $\phi\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ by $\phi(1) = (1,1)$. It's straightforward to check that ϕ is injective and surjective, so it's an isomorphism. However $\mathbb{Z}/8\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ since the former has an element of order 8 while the latter does not.

6.4 (a) The elements consists of $0, 1, \alpha, \alpha+1$. Note that $\alpha(\alpha+1) = 1$ so every nonzero element is invertible. Hence this ring is a field with four elements, $\mathbb{F}_4$.

(b) Note $(\alpha+1)^2 = \alpha^2 + 1 = 0$. So letting $x = \alpha + 1$, we get that the ring is isomorphic to $\mathbb{F}_2[x]/(x^2)$.

(c) Since α and $\alpha+1$ are both idempotents, we have $\mathbb{F}_2[\alpha] \cong \alpha\mathbb{F}_2[\alpha] \times (\alpha+1)\mathbb{F}_2[\alpha]$. Listing out the elements gives $\alpha\mathbb{F}_2[\alpha] \cong \mathbb{F}_2$ and $(\alpha+1)\mathbb{F}_2[\alpha] \cong \mathbb{F}_2$. Hence $\mathbb{F}_2[\alpha] \cong \mathbb{F}_2 \times \mathbb{F}_2$.

6.8 (a) We showed in 3.13 that $IJ \subseteq I \cap J$. To show $I \cap J \subseteq IJ$, suppose $x \in I \cap J$. Write $x = a + b$ where $a \in I$ and $b \in J$. Since $x, b \in J$, we have $a \in J$ also, and similarly $b \in I$. Let $1 = i + j$ for some $i \in I, j \in J$. Then $x = i(a+b) + (a+b)j \in IJ$.

(b) Let $a = a_I + a_J$ and $b = b_I + b_J$ where $a_I, b_I \in I$ and $a_J, b_J \in J$. Let $x = a_J + b_I$. It's straightforward to check that $x - a \in I$ and $x - b \in J$.

(c) Define $\varphi\colon R \to R/I \times R/J$ by the usual quotient maps. The kernel is $I \cap J = IJ = 0$ by hypothesis and (b) shows that φ is surjective.

(d) Let $i \in I, j \in J$ be the unique elements such that $i + j = 1$. The idempotents are i and j.

7.1 Suppose R is an integral domain of order n. Let $x \in R$ be a nonzero element and consider the sequence $x, x^2, x^3, \ldots$. Since R is finite, there is some distinct positive integers $i \langle j$ such that $x^i = x^j$. Hence $x^i(x^{j-i} - 1) = 0$. Since R is a domain and x is nonzero, we must have $x^{j-i} = 1$. Thus x is invertible and so R is a field.

7.5 Addition: If $a/b, c/d \in S^{-1}R$ define $a/b + c/d = (ad + bc)/bd$ which is an element of $S^{-1}R$ since S is multiplicatively closed. To show it's well defined, suppose $a'/b' = a/b$ and $c/d = c'/d'$. Then $a'/b' + c'/d' = (a'd' + b'c')/b'd'$. But then $0 = (ab' - a'b)dd' + (cd' - c'd)bb' = (ad + bc)(b'd') - (a'd' + b'c')(bd)$ implies $(ad + bc)/bd = (a'd' + b'c')/b'd'$. Commutativity and associativity follow from that of R. Identity is $0/a$ for any $a \in S$. Inverse of a/b is $(-a)/b$. Multiplication: Define $a/b \cdot c/d = ac/bd$. To show this is well defined, again suppose $a'/b' = a/b, c'/d' = c/d$. Then $ac/bd = a'c'/b'd'$ since $acb'd' - a'c'bd = ab'cd' - a'bc'd = 0$. It is associative since R is and a/a for any $a \in S$ is the multiplicative identity. Distributive law: Follows directly from the distributive law of R.

8.1 Let $f \in \mathbb{Z}[x]$ and (f) be a principal ideal. Suppose $\deg f = 0$, so $f \in \mathbb{Z}$. Then (f, x) is a proper ideal which properly contains (f). Hence (f) is not maximal. Suppose $\deg f \geq 1$. Let $p \in \mathbb{Z}$ be a prime which does not divide any of the coefficients of f. Clearly $(f) \neq (f, p)$ since $p \notin (f)$. Moreover $(f, p) \neq \mathbb{Z}[x]$ since $\mathbb{Z}[x]/(f, p) \cong \mathbb{F}_p[x]/(f)$ which is a vector space over $\mathbb{F}_p$ of dimension $\deg f$. Hence (f) is not maximal. There are no maximal principal ideals.

8.3 Since $\mathbb{F}_2$ is a field, it suffices to check that $x^3 + x + 1$ is irreducible. This can be done by listing out all degree 1 and 2 polynomials and observing that none of them multiply out to equal $x^3 + x + 1$.

On the otherhand, over $\mathbb{F}_3$, it factors as $x^3+x+1 = (x+2)(x^2+x+2)$. Hence $\mathbb{F}_3[x]/(x^3+x+1)$ is not a field, e.g., $x+2$ is not invertible.

8.4 Maximal ideals in $\mathbb{R}[x]$ correspond to irreducible polynomials. Irreducible polynomials over $\mathbb{R}$ are either linear or quadratic with two complex conjugate roots. If we consier the upper half plane as $\mathbb{C}$ minus complex numbers with negative imaginary component, then we get a bijection as follows: Send any linear polynomial $x-a$ to a lying on the real axis. Send any quadratic polynomial to the root with positive imaginary component. It's clear this gives a bijection between maximal ideals and the upper half plan.

Part B: 563 Students Only

2.2 Since s sends each element $x \in X$ to sx, ρ_s sends e_x to e_{sx} for basis elements (e_x) in V. Thus $\mathrm{Tr}(\rho_s) = \#\{e_x \mid e_x = e_{sx}\} = \#\{x \mid x = sx\}$. So $\chi_{X(s)}$ is the number of elements in X fixed by s.

2.3 Existence: Set $\rho'_s = (\rho_s^t)^{-1}$. It suffices to show that $\langle \rho_s e_j, \rho'_s e_i \rangle = \langle e_j, e_i \rangle$ for basis elements e_j, e'_i. Let $\rho_s = r_{ij}(s)$ and $\rho'_s = r'_{ij}(s)$. Then

$$\begin{aligned}
\langle \rho_s e_j, \rho'_s e'_i \rangle &= \sum_{l,k} r_{lj}(s) r'_{ki}(s) \langle e_l, e'_k \rangle \\
&= \sum_{l,k} r_{lj}(s) r'_{ki}(s) \delta_{kl} \\
&= \sum_{k} r_{kj}(s) r'_{ki}(s) \\
&= \sum_{k} r^t_{jk}(s) r'_{kj}(s) \\
&= (\rho_s^t \rho'_s)_{ji} = \delta_{ij}.
\end{aligned}$$

Uniqueness: The previous calculation shows that ρ' must satisfy $(\rho_s^t \rho'_s) = \mathrm{Id}$ so there is only one solution.