HW 14

1

Let R be a ring with abelian group A. Define a map $\varphi : R \to End(A)$ which maps r to multiplication by r, i.e. let $\varphi(r) = \varphi_r$ where $\varphi_r(a) = ra$.

φ is a ring homomorphism. It preserves addition: this is equivalent to $\varphi_{r+s} = \varphi_r + \varphi_s$, or $\forall a \in A, (r+s)a = ra + sa$, which follows from the distributive law in R.

Similarly, φ preserves multiplication means $\varphi_r \varphi_s = \varphi_{rs}$ where the product on the left denotes function composition in $End(A)$. This means $\forall a \in A, r(sa) = (rs)a$ which follows from associativity of multiplication in R.

We show that φ is injective by showing its kernel is $\{0\}$. Suppose $\varphi(r) = 0$, that is $ra = 0$ for all $a \in R$. In particular, for $a = 1$ we have $r1 = 0$, which means $r = 0$.

7.4.12

Let $r \in IJ$. Then $r = \sum_{p=0,q=0}^{p=P,q=Q} i_p j_q$ for some $i \in I, j \in J$. Since I, J are f.g., each $i_p = \sum_r \alpha_{p,r} a_r$ and each $j_q = \sum_s \beta_{q,s} b_s$ hence $r = \sum_{p=0,q=0}^{p=P,q=Q} (\sum_r \alpha_{p,r} a_r)(\sum_s \beta_{q,s} b_s)$ which is a linear combination of the $\{a_i b_j\}$.

7.4.15a

For $p, q \in \mathbb{F}_2[x]$ let $p \sim q$ if $\overline{p} = \overline{q}$, that is $p - q \in \mathbb{F}_2[x]$.

Since $x^2 \sim x + 1$, if p q for some q of degree 1 or lower. Proof: otherwise, if q have minimal degree; we can rewrite the highest-order term to get a polynomial of lower degree, a contradiction.

By enumerating possible values of coefficients those polynomials are $\{0, 1, x, x + 1\}$. None of these are equivalent to each other as their difference is nonzero and are degree 1 polynomials.

7.4.15b

As this is a commutative group of order 4, all of whose nonidentity elements have order 2, it is isomorphic to V_4.

7.4.15c

$\overline{E}$ is multiplicatively generated by x, since the powers are $x, x^2 = x+1, x(x+1) = x^2+x = x+x+1 = 1, x$. Hence every nonzero element of $\overline{E}$ has a multiplicative inverse.

4

Define the n ideals $R_i = (x - x_i)$ for $x_i \in F$, where $F[x]$ is the ambient ring.

These are pairwise comaximal. Proof: letting the ideals be $R_i = (x - x_i)$ and $R_j = (x - x_j)$, it suffices to show $1 \in R_i + R_j$, since then $F[x] = (1) \subseteq R_i + R_j$. In fact, let $k = (x_j - x_i)^{-1}$, which exists since $x_j - x_i \neq 0$, we have $1 = k(x - x_i) + (-k)(x - x_j) \in R_i + R_j$.

Let the ring homomorphism $\varphi_i : F[x] \to F[x]/(x - x_i)$ be the map $p \mapsto p + (x - x_i)$. By the euclidean algorithm on polynomials, $p(x) = q(x) + r(x)(x - x_i)$ where q is constant; substituting $x = x_i$ we get $q = p(x_i) = y_i$.

By the Chinese Remainder Theorem, the map $p \mapsto (p+R_1, \dots, p+R_n)$ is a surjective ring homomorphism with domain $F[x]$, kernel $R_1 \cdots R_n$ and range (and codomain) $F[x]/R1 \times \cdots \times F[x]/R_n$. Let $Y = (y_1 + R_1, \dots y_n + R_n)$, and find the unique inverse of Y under this ring homomorphism, which by construction can be represented as $p + R_1 \cdots R_n$ where we have $p(x_i) = y_i$ for all i. Furthermore, since $R_1 \cdots R_n$ is generated by the degree n polynomial $(x - x_1) \cdots (x - x_n)$, there is a unique representative p of degree $n - 1$ or lower.

5a

We consider $R = \mathbb{Z}, a = 2$ then $Z[1/2] = \mathbb{Z}[x]/(2x - 1)$. The map i is given by $i : z \mapsto z + (2x - 1)$ and it is injective. Suppose $i(z_1) = i(z_2)$; then $z_2 - z_1 = p(x)(2x - 1)$ for some $p(x) \in \mathbb{Z}[x]$. Since the LHS is a polynomial of degree 0 or $-\infty$ and the RHS is a product of $p(x)$ and $2x - 1$ which is degree 1, by the additivity of degree under product in $Z[x]$ we have $p(x) = 0$ (it has degree $-\infty$), hence $z_1 = z_2$. (Note: additivity of degree holds because $\mathbb{Z}$ is an integral domain, I'm not sure what happens for general rings).

If we take $R = \mathbb{Z}, a = 0$ then $Z[1/0]$ is $\mathbb{Z}[x]/(-1)$. Since $(-1) = (1) = \mathbb{Z}[x]$, this is the quotient by the whole ring, which results in a ring of size 1 (where $0 = 1$), hence the map is not injective (it maps an infinite set to a single element).

5b

When $a = 0$ we have $R[1/0] = R[x]/(-1)$ and again $R[1/a]$ is isomorphic to the zero ring.

Suppose $R[1/a]$ is the zero ring, that is $0 = 1$ in $R[1/a]$. This means $1 = p(x)(ax - 1)$ as an equation in $R[x]$. Hence $R[1/a]$ is the zero ring $\iff$ $ax - 1$ is a unit in $R[x]$. However, I can't find a simpler characterisation of this condition.