MATD01 Fields and Groups

Assignment 1

Solutions

1. (a) R is easily seen to be a rational vector subspace of $\mathbb{C}$. Thus to show that R is a subring it is enough to check that the numbers α^m ($m \geq 0$) are in R (as a product of two elements of R is a $\mathbb{Q}$-linear combination of the α^m ($m \geq 0$)). This can be checked by induction on m: clearly $\alpha^0 = 1 \in R$, and if $\alpha^m \in R$, i.e. if α^m is a $\mathbb{Q}$-linear combination of $1, \alpha, \ldots, \alpha^{n-1}$, then α^{m+1} is a $\mathbb{Q}$-linear combination of $\alpha, \ldots, \alpha^n$. Since $f(\alpha) = 0$ for some $f(x) \in \mathbb{Q}[x]$ of degree n, α^n is a $\mathbb{Q}$-linear combination of $1, \alpha, \ldots, \alpha^{n-1}$. Hence

$$\alpha^{m+1} \in \mathrm{span}_{\mathbb{Q}}\{\alpha, \ldots, \alpha^n\} \subset \mathrm{span}_{\mathbb{Q}}\{1, \alpha, \ldots, \alpha^{n-1}\} = R.$$

(Here $\mathrm{span}_{\mathbb{Q}}(S)$ means the $\mathbb{Q}$-span of S, i.e. the set of all linear combinations of the elements of S with coefficients in $\mathbb{Q}$.)

(b) We have $(a + b\sqrt{2})^{-1} = \frac{a-b\sqrt{2}}{a^2-2b^2}$. (Note that if $a + b\sqrt{2} \neq 0$ with $a, b \in \mathbb{Q}$ then a or b must be nonzero, and hence $a - b\sqrt{2}$ is also nonzero (as $\sqrt{2}$ is irrational). Hence $a^2 - 2b^2 = (a + b\sqrt{2})(a - b\sqrt{2}) \neq 0$.)

2. Let F be a finite integral domain and $a \in F - \{0\}$. The elements a^n ($n \geq 0$) cannot all be distinct. Thus we have $a^n = a^m$ for some integers $n > m \geq 0$. Since F is an integral domain and $a^m \neq 0$, cancellation property implies that $a^{n-m} = 1$.

3. For and $a \in R$ and $n \in \mathbb{Z}_{\geq 0}$ let us write na for $a + a + \ldots + a$ with n appearances of a (this can be generalized to the negative integers too by $(-n)a := -(na)$ but that's not necessary for this question). By distributivity $(m1_R)(n1_R) = (mn)1_R$. Now suppose R is an integral domain of positive characteristic k. Then $k > 1$ (why?). Suppose k is not prime. Then $k = nm$ for some $k > n, m > 1$. We have $(m1_R)(n1_R) = (mn)1_R = 0$, so that (since R is an integral domain) we must have $n1_R = 0$ or $m1_R = 0$. Either way this contradicts the defining property of k.

4. (a) We leave it to the reader to verify the three requirements (respecting addition and multiplication, and sending $1 \mapsto 1$).

(b) The identity and σ are ring homomorphisms $R \to \mathbb{C}$. To see that these are the only ones, let $\phi : R \to \mathbb{C}$ be a ring homomorphism. We leave it to the reader to check that the only ring map $\mathbb{Q} \to \mathbb{C}$ is the identity. Thus $\phi|_{\mathbb{Q}}$ (= the restriction of ϕ to $\mathbb{Q} \subset R$) is the identity, and we have $\phi(a + b\sqrt{2}) = a + b\phi(\sqrt{2})$ for any $a, b \in \mathbb{Q}$. We have $\sqrt{2}^2 = 2$, so that $\phi(\sqrt{2})^2 = \phi(2) = 2$. Thus $\phi(\sqrt{2}) = \pm\sqrt{2}$. In the $+$ case we have $\phi = \mathrm{Id}$ and in the minus case $\phi = \sigma$.

5. First let us make a general observation. Let R be an arbitrary ring, $a \in R$ and n a positive integer. Note that $na = n(1_R a) = (n1_R)a$ by distributivity. Now if $n = p$ is the characteristic of R, we have $pa = p(1_R a) = (p1_R)a = 0a = 0$. More generally, if n is divisible by the characteristic p of R, we have $na = (n/p)(pa) = (n/p)0 = 0$.

Back to the question, by distributivity we have

$$(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}.$$

Since p is prime, for any $0 < k < p$ the number $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ is divisible by p (as its numerator is divisible by p and the denominator is not). Thus by our earlier observation (since R has characteristic p) we have

$$\sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p.$$

This shows that the Frobenius respects addition. That it respects multiplication and identity is clear.

6. Define $\phi : \mathbb{Z} \to R$ by $\phi(n) = n1_R$ (notation as in the solution to Problem 3). We leave it to the reader to check that ϕ is a ring homomorphism (from group theory we know this is a group map; using distributivity one can check that it also respects multiplication).

Given any ring map $\psi : \mathbb{Z} \to R$, we have $\psi(1) = 1_R$. Now being a group map we must have $\psi(n) = n\psi(1) = n1_R$, so that $\psi = \phi$.

7. The subsets given in Parts (a)-(c) are ideals; we leave the verifications to the reader. The subset I given in Part (d) is not an ideal, since $x^2 \in I$ but $x \cdot x^2 = x^3$ is not in I.