ANSWERS TO SOME OF THE HOMEWORK PROBLEMS

Third problem set

1. By definition $\phi(1) = 1$, hence $\phi(n \cdot 1) = n \cdot \phi(1) = n \cdot 1$ for all $n \in \mathbb{Z}$. For any ring homomorphism ϕ, if u is a unit then $\phi(u^{-1}) = (\phi(u))^{-1}$ (this is another reason why we want to impose the condition $\phi(1) = 1$), hence $\phi(n\cdot 1/m\cdot 1) = \phi((n\cdot 1)(m\cdot 1)^{-1}) = \phi(n\cdot 1)(\phi(m\cdot 1))^{-1} = (n\cdot 1)(m\cdot 1)^{-1}) = n\cdot 1/m\cdot 1$. Since by defintion the prime subfield of F is the set of all elements of the form $a = n\cdot 1/m\cdot 1$, we see that $\phi(a) = a$ for all a in the prime subfield.

2. (i) First $(\phi(\sqrt{2}))^2 = \phi((\sqrt{2})^2) = \phi(2) = 2$, by Problem 1. Thus $\phi(\sqrt{2}) = \pm\sqrt{2}$. If $\phi(\sqrt{2}) = \sqrt{2}$, then again by Problem 1 $\phi(a+b\sqrt{2}) = \phi(a)+\phi(b\sqrt{2}) = \phi(a) + \phi(b)\phi(\sqrt{2}) = a + b\sqrt{2}$ for all $a, b \in \mathbb{Q}$, and hence $\phi = \mathrm{Id}$. Similarly, if $\phi(\sqrt{2}) = -\sqrt{2}$, then $\phi(a + b\sqrt{2}) = \phi(a) + \phi(b\sqrt{2}) = \phi(a) + \phi(b)\phi(\sqrt{2}) = a - b\sqrt{2}$ for all $a, b \in \mathbb{Q}$. Finally, if ϕ is defined by $\phi(a + b\sqrt{2}) = a - b\sqrt{2}$ for all $a, b \in \mathbb{Q}$, then it is easy to see that ϕ is an additive homomorphism and that $\phi(1) = 1$. To see that ϕ preserves multiplication, we compute:

$$\begin{aligned}
\phi(a + b\sqrt{2})\phi(c + d\sqrt{2}) &= (a - b\sqrt{2})(c - d\sqrt{2}) = (ac + 2bd) - (ad + bc)\sqrt{2};\\
\phi((a + b\sqrt{2})(c + d\sqrt{2})) &= \phi((ac + 2bd) + (ad + bc)\sqrt{2})\\
&= (ac + 2bd) - (ad + bc)\sqrt{2}.
\end{aligned}$$

Hence ϕ preserves multiplication and is thus a ring homomorphism. Since clearly $\phi^2 = \mathrm{Id}$, ϕ is an isomorphism with $\phi^{-1} = \phi$.
(ii) Arguing as in (i), $(\phi(\sqrt[3]{2}))^3 = \phi((\sqrt[3]{2})^3) = \phi(2) = 2$, so that $\phi(\sqrt[3]{2})$ is a cube root of 2. This rules out $\phi(\sqrt[3]{2}) = -\sqrt[3]{2}$ since $(-\sqrt[3]{2})^3 = -2$, as well as $\phi(\sqrt[3]{2}) = (\sqrt[3]{2})^2$ since $((\sqrt[3]{2})^2)^3 = 4$. In fact, since $\phi(\sqrt[3]{2}) \in \mathbb{Q}(\sqrt[3]{2})$, it is a real number whose cube is 2 and hence $\phi(\sqrt[3]{2}) = \sqrt[3]{2}$. Thus $\phi((\sqrt[3]{2})^2) = (\sqrt[3]{2})^2$, and again using Problem 1, if $a, b, c \in \mathbb{Q}$,

$$\begin{aligned}
\phi(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) &= \phi(a) + \phi(b)\phi(\sqrt[3]{2}) + \phi(c)\phi((\sqrt[3]{2})^2)\\
&= a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2,
\end{aligned}$$

so that $\phi = \mathrm{Id}$.

3. (a) Not an ideal ($\sqrt{2}\cdot 1 \notin \mathbb{Q}$). (b) Not an ideal ($x \cdot 1 \notin \mathbb{Z}$). (c) Not an ideal ($i \cdot 1 \notin \mathbb{Z}$). (d) An ideal, in fact it is the principal ideal generated by $3 - 2i$. (e) An ideal, in fact it is the principal ideal generated by (x^5).

(f) Not an ideal since e.g. the linear term of 1 is 0 but that of $x \cdot 1$ is not.
(g) Not a subgroup, since for example $2x$ and $-2x+1$ both have leading coefficient divisible by 2, but their sum does not. Hence not an ideal.

4. We already know that $I \cap J$ is an additive subgroup of R. If $r \in I \cap J$ and $s \in R$, then $sr \in I$ since I is an ideal and $sr \in J$ since J is an ideal, hence $sr \in I \cap J$. Clearly any subset of R, and hence any ideal, contained in both I and J is by definition contained in $I \cap J$. But $I \cup J$ is not always an ideal, e.g. $(2) \cup (3) \subseteq \mathbb{Z}$ which is not closed under addition.

5. By Problem 3, Part (b) from the last HW, the sum of two nilpotent elements is nilpotent. Clearly 0 is nilpotent and, by Part (a) of Problem 3, last HW, r nilpotent $\implies$ $-r = (-1) \cdot r$ is nilpotent. Hence $\sqrt{0}$ is an additive subgroup. Again by HW 2, Problem 3, Part (a) it is an ideal. $R = \mathbb{Z}$: $\sqrt{0} = (0)$. $R = \mathbb{Z}/6\mathbb{Z}$: $\sqrt{0} = (0)$. $R = \mathbb{Z}/27\mathbb{Z}$: $\sqrt{0} = (3)$. $R = \mathbb{Z}/18\mathbb{Z}$: $\sqrt{0} = (6)$.

6. (i) Recall that, by definition, $\varphi^{-1}(J) = \{r \in R : \varphi(r) \in J\}$. We know $\varphi^{-1}(J)$ is an additive subgroup of R. If $r \in \varphi^{-1}(J)$ and $s \in R$, then by definition $\varphi(sr) = \varphi(s)\varphi(r) \in J$, since $\varphi(r) \in J$ and J is an ideal in S. Hence $sr \in \varphi^{-1}(J)$ by definition. The last sentence follows since if $i\colon R \to S$ is the inclusion, then $R \cap J = i^{-1}(J)$.
(ii) Again, we know that $\varphi(I)$ is an additive subgroup of S (even if φ is not necessarily surjective). Given $s \in S$ and $\varphi(r) \in \varphi(I)$, since φ is surjective there exists a $t \in R$ with $\varphi(t) = s$. Hence $s\varphi(r) = \varphi(t)\varphi(r) = \varphi(tr)$. Since I is an ideal, $tr \in I$ and hence by definition $s\varphi(r) = \varphi(tr) \in \varphi(I)$. Thus $\varphi(I)$ is an ideal. For an example where φ is not surjective and $\varphi(I)$ is not an ideal, you could take $R = \mathbb{Z}$, $S = \mathbb{Q}$, i the inclusion and I any nonzero ideal. Then $i(I)$ is not an ideal of $\mathbb{Q}$ since, as it is nonzero, it would have to be all of $\mathbb{Q}$ but it is contained in $\mathbb{Z}$.

Fourth problem set

1. Suppose that R is a ring and that every ideal of R is either $\{0\}$ or R, and that $R \neq \{0\}$. Let $r \in R$, $r \neq 0$. Then (r) is an ideal of R and $(r) \neq \{0\}$, hence $(r) = R$. Thus $1 \in (r)$, i.e. there exists $s \in R$ such that $rs = 1$. Hence every nonzero r has a multiplicative inverse. Since $R \neq \{0\}$, R is a field.

2. In any case, $\operatorname{Ker} \rho$ is an ideal of F. Thus either $\operatorname{Ker} \rho = \{0\}$ and ρ is injective, or $\operatorname{Ker} \rho = F$ and hence $\rho(a) = 0$ for all $a \in F$. In particular, $\rho(1) = 0$, hence since $\rho(1) = 1$, $1 = 0$ and $R = \{0\}$.

3. It is easy to check that $I+J$ is an additive subgroup of R. If $r \in I$, $s \in J$, and $t \in R$, then $t(r+s) = tr + ts \in I + J$. Finally, any ideal of R containing both I and J must contain all sums $r+s$ with $r \in I$, $s \in J$, hence contains $I+J$.

4. $I \cdot J$ is closed under addition: given two expressions $\sum_i r_i s_i$, with $r_i \in I$, $s_i \in J$, and $\sum_j t_j w_j$, $t_j \in I$, $w_j \in J$, the sum $\sum_i r_i s_i + \sum_j t_j w_j$ is again a sum of products of elements of R such that the first term is in I and the second is in J, hence is in $I \cdot J$. Clearly $0 = 0 \cdot 0 \in I \cdot J$, and if $\sum_i r_i s_i \in I \cdot J$, then $-\sum_i r_i s_i = \sum_i (-r_i) s_i \in I \cdot J$. Thus $I \cdot J$ is an additive subgroup. Given $r \in R$ and $\sum_i r_i s_i \in I \cdot J$, the product $r\left(\sum_i r_i s_i\right) = \sum_i (r r_i) s_i \in I \cdot J$, because I is an ideal. Hence $I \cdot J$ is an ideal. Clearly $\sum_i r_i s_i \in I$ since $r_i s_i \in I$ for every i (I is an ideal) and $\sum_i r_i s_i \in J$ since $r_i s_i \in J$ for every i (J is an ideal). Hence $I \cdot J \subseteq I \cap J$.

5. $(n) + (m) = (d)$, where $d = \gcd\{n, m\}$. $(n) \cap (m) = (e) = (nm/d)$, where $d = \gcd\{n, m\}$ and hence $e = \operatorname{lcm}\{n, m\}$. $(n) \cdot (m) = (nm)$. So for example if $n = m = 2$, then $(2) \cap (2) = (2)$ but $(2) \cdot (2) = (4)$.

6. Let $f\colon R \to S/J$ be defined by $f(r) = r + J$. Then f is a homomorphism since it is the composition $\pi \circ i$ of two homomorphisms, where i is the inclusion $R \to S$ and $\pi\colon S \to S/J$ is the quotient homomorphism. Moreover $\operatorname{Ker} f = \{r \in R : r \in J\} = R \cap J = I$. Hence there is an induced injective homomorphism, which we will also denote by f, from R/I to S/J. It is surjective $\iff$ for every element $s + J$ of S/J, there exists an $r \in R$ such that $r + J = s + J \iff$ for all $s \in S$, there exists an $r \in R$ such that $r - s \in J$.

7. (i) Clearly $-3 + 2i = i(2 + 3i) \in I$. In fact, I is the set of all multiples $(a + bi)(2 + 3i) = a(2 + 3i) + b(-3 + 2i)$, $a, b \in \mathbb{Z}$. This exactly says that $2 + 3i$ and $-3 + 2i$ generate the additive subgroup I. (ii) Since I contains $2 + 3i$ and $-3 + 2i$, it contains $2 + 3i - (-3 + 2i) = 5 + i$. (iii) By (ii), $a + bi \equiv a - 5b \bmod I$ and we can then apply Problem 6 to see that f is surjective. (iv) $13 = (2 - 3i)(2 + 3i) \in I$. (v) Since $13 \in \mathbb{Z} \cap I$ and $\mathbb{Z} \cap I$ is an ideal in $\mathbb{Z}$, $13\mathbb{Z} \subseteq \mathbb{Z} \cap I$. Conversely, suppose that $(a + bi)(2 + 3i) = a(2 + 3i) + b(-3 + 2i) \in \mathbb{Z}$, where $(a + bi)(2 + 3i)$ is a typical element of I. Then the imaginary part $(3a + 2b)i = 0$, so that $2b = -3a$. Since a and b are relatively prime, $2|a$, say $a = 2k$, and hence $-6k = 2b$ so that $b = -3k$. Then

$$(a+bi)(2+3i) = a(2+3i)+b(-3+2i) = (2a-3b)+(3a+2b)i = 4k+9k = 13k.$$

Hence $\mathbb{Z} \cap I \subseteq 13\mathbb{Z}$ so that $\mathbb{Z} \cap I = 13\mathbb{Z}$. (vi) Again by Problem 6, there is a homomorphism $\mathbb{Z}/13\mathbb{Z} \to \mathbb{Z}[i]/I$ which is injective and surjective, hence a (ring) isomorphism. Since $\mathbb{Z}/13\mathbb{Z}$ is a field, I is a maximal and hence a prime ideal.