
620-321 Algebra, Semester 1, 2009

Answers to Problem Sheet 2

---

1. Let R be a ring, $I \lhd R$ an ideal and $r, r', s \in R$. Suppose that $r + I = r' + I$. Then $r' = r + i$ for some $i \in I$, and

$$\begin{aligned}(r' + I)(s + I) = r's + I = (r + i)s + I = rs + is + I &= rs + I \qquad \text{(since } is \in I \text{ as } I \text{ is an ideal)}\\ &= (r + I)(s + I)\end{aligned}$$

Multiplication is therefore independent of the coset representative chosen. Similarly for addition.

4. Same as last week!

5. The given map (let's call it φ) is a homomorphism since

$$\begin{aligned}\varphi(m)\varphi(n) &= (1 + 1 + \cdots + 1)(1 + 1 + \cdots + 1) && (m \text{ and } n \text{ times respectively})\\ &= 1 + 1 + \cdots + 1 && (mn \text{ times})\\ &= \varphi(mn)\end{aligned}$$

and

$$\begin{aligned}\varphi(m) + \varphi(n) &= (1 + 1 + \cdots + 1) + (1 + 1 + \cdots + 1) && (m \text{ and } n \text{ times respectively})\\ &= 1 + 1 + \cdots + 1 && (m + n \text{ times})\\ &= \varphi(m + n)\end{aligned}$$

By the definition of the characteristic n, we have that $n \in \ker\varphi$. If φ is injective, then $n = 0$ and $\ker\varphi = \{0\}$. If $\ker\varphi \neq \{0\}$, then n is the smallest positive integer in $\ker\varphi$. Since $\ker\varphi$ is an ideal in $\mathbb{Z}$, it follows that $\ker\varphi = (n)$. By the first isomorphism theorem, $\operatorname{im}\varphi$ is isomorphic to $\mathbb{Z}/(n)$. Suppose R is an integral domain with non-zero characteristic. Then if $\varphi(nm) = 0$ where $1 < m, n \in \mathbb{Z}$, we must have either $\varphi(m) = 0$ or $\varphi(n) = 0$. Thus the least integer n such that $\varphi(n) = 0$ must be a prime.

6. Let F be a field. The homomorphism $\varphi : \mathbb{Z} \to F$ defined by $1_{\mathbb{Z}} \to 1_F$ is either injective or has kernel (p) where p is a prime, by the previous exercise. In the later case its image is $\mathbb{Z}_p = \mathbb{Z}/(p)$. If φ is injective, then F contains a copy of $\mathbb{Z}$ and hence the inverses of non-zero integers and hence a copy of $\mathbb{Q}$. In either case this is the smallest subfield of F containing 1_F.

7. $q(x) = x^2 - x - 3, \;\; r(x) = x + 3$

8. There exist (unique) $q, r \in F[x]$ s.t. $f(x) = q(x)(x-a)+r(x)$ with $\deg(r) = 0$. Since $\deg(r) = 0$ we have $r(x) = c$ for some $c \in F$.

   Suppose $f(a) = 0$. Then,

$$0 = f(a) = q(a)(a - a) + c = q(a).0 + c = c \quad \text{(since } F \text{ is an integral domain).}$$

   Therefore $f(x) = q(x)(x - a)$.

   The converse follows immediately from the fact that $F[x]$ is an integral domain.

9. Since $x^2 - 2$ has no roots in $\mathbb{Q}$, it has no linear factors in $\mathbb{Q}[x]$. If $x^2 - 2$ factored as a product of two non-unit polynomials in $\mathbb{Q}[x]$ one (both) of them would be linear. In $\mathbb{R}[x]$, $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$, and neither factor is a unit.

10. (a) First note that if $b \neq 0$ and $c \neq 0$, then $bd \neq 0$ since D is an integral domain. Now suppose that $(a, b) \sim (\alpha, \beta)$ and $(c, d) \sim (\gamma, \delta)$. We need to show that $(ad + bc, bd) \sim (\alpha\delta + \beta\gamma, \beta\delta)$ and $(ac, bd) \sim (\alpha\gamma, \beta\delta)$.

$$\begin{aligned}
(ad + bc)\beta\delta &= a\beta d\delta + b\beta c\delta \\
&= \alpha b d\delta + b\beta d\gamma && \text{(since } a\beta = b\alpha \text{ and } c\delta = d\gamma\text{)} \\
&= (\alpha\delta + \beta\gamma)bd \\
&\Longrightarrow (ad + bc, bd) \sim (\alpha\delta + \beta\gamma, \beta\delta)
\end{aligned}$$

and

$$\begin{aligned}
&ac\beta\gamma = \alpha\gamma bd && \text{(since } a\beta = b\alpha \text{ and } c\delta = d\gamma\text{)} \\
&\Longrightarrow (ac, bd) \sim ((\alpha\gamma, \beta\delta)
\end{aligned}$$

11. Notice that $2 \not| (1 \pm \sqrt{-5})$, since $|2|^2 = 4$ does not divide $|(1 \pm \sqrt{-5})|^2 = 6$. Therefore, 2 is not prime because $2|(1-\sqrt{-5})(1+\sqrt{-5})$. If $2 = (a+b\sqrt{-5})(x+y\sqrt{-5})$ then $4 = (a^2+5b^2)(x^2+5y^2)$. Since a, b, x, y are integers, this is only possible if one of the factors is ± 1.