

Solutions to exam in algebra: MMG 500 and MVE 150, 2020-03-20.

1a) The operation is associative as $l*(m*n) = l*(m+n-1) = l+(m+n-1) = (l+m-1)+n = (l*m)*n$

b) 1 is a neutral element for the given operation as $m*1 = (m+1)-1 = m$ and $1*m = (1+m)-1 = m$

c) $*$ is an associative operation on \mathbf{Z} with neutral element 1. We have also for any $m \in \mathbf{Z}$ that $2-m$ is inverse to m as $m*(2-m) = (m+(2-m)-1) = 1$ and $(2-m)*m = ((2-m)+m)-1 = 1$. Hence $(\mathbf{Z}, *)$ is a group with 1 as identity.

2. We know by the fundamental theorem for abelian groups that any finite abelian group is isomorphic to a product of cyclic groups of prime power order. As 2020 has prime factorisation $2^2 \times 5 \times 101$ we thus conclude that any abelian group of order 2020 is isomorphic to $\mathbf{Z}_4 \times \mathbf{Z}_5 \times \mathbf{Z}_{101}$ or $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_5 \times \mathbf{Z}_{101}$. As by the above theorem these two groups are non-isomorphic, it follows that there are exactly two isomorphism classes of abelian groups of order 2020. (Remark: One can also represent the two isomorphism classes by \mathbf{Z}_{2020} and $\mathbf{Z}_2 \times \mathbf{Z}_{1010}$.)

3. As $o(N)$ and $o(G/N)$ are relatively prime we may find integers k and m with $1 = o(N)k + o(G/N)m$. Therefore, $Ng = ((Ng)^{o(N)})^k ((Ng)^{o(G/N)})^m$ in G/N by the power laws. Further, $(Ng)^{o(G/N)} = Ne$ for all $Ng \in G/N$ by a corollary of Lagrange's theorem. Hence $Ng = ((Ng)^{o(G/N)})^m = (N(g^{o(G/N)}))^m = (Ne)^m = N$ and $g \in N$ for any $g \in G$ with $g^{o(N)} \in N$.

4. If rs is a zero divisor in R , then $rs \neq 0$ and $(rs)t = 0$ for some $t \neq 0$ in R . If now $st \neq 0$, then r is a zero divisor as $r(st) = 0$ and $r \neq 0$. If instead $st = 0$, then s is a zero divisor as $s \neq 0$ and $t \neq 0$.

5a). This follows from the subring criterion as $(a+b\sqrt{6}i) \pm (c+d\sqrt{6}i) = (a \pm c) + (b \pm d)\sqrt{6}i \in \mathbf{Z}[\sqrt{-6}]$ and $(a+b\sqrt{6}i)(c+d\sqrt{6}i) = (ac-6bd) + (ad+bc)\sqrt{6}i \in \mathbf{Z}[\sqrt{-6}]$ for all a, b, c, d in \mathbf{Z} .

b) Let N be the norm map with $N(a+b\sqrt{6}i) = a^2+6b^2$. This map is multiplicative as $N(a+b\sqrt{6}i) = |a+b\sqrt{6}i|^2$. So if $a+b\sqrt{6}i$ is inverse to $c+d\sqrt{6}i$ in $\mathbf{Z}[\sqrt{-6}]$ then $(a^2+6b^2)(c^2+6d^2) = N((a+b\sqrt{6}i)(c+d\sqrt{6}i)) = N(1) = 1$. But then $a^2+6b^2 = 1$ as $a^2+6b^2 \in \mathbf{N}$ and $c^2+6d^2 \in \mathbf{N}$. We have thus for any unit $a+b\sqrt{6}i$ that $a^2 = 1-6b^2 \in (0, 1] \cap \mathbf{Z} = \{1\}$, which implies that $a = \pm 1$ and $b = 0$. There are therefore just two units in $\mathbf{Z}[\sqrt{-6}]$ given by ± 1 .

c) If $a+b\sqrt{6}i$ and $c+d\sqrt{6}i$ are in $\mathbf{Z}[\sqrt{-6}]$, then $N((a+b\sqrt{6}i)(c+d\sqrt{6}i)) = (a^2+6b^2)(c^2+6d^2)$. Also, if $b \neq 0$ then $a^2+6b^2 \geq 6b^2 \geq 6$ and if $b = 0$ then $a^2+6b^2 = a^2 \geq 4$ if not $a = \pm 1$. We have therefore, if of $a+b\sqrt{6}i$ and $c+d\sqrt{6}i$ are non-units that $a^2+6b^2 \geq 4$, $c^2+6d^2 \geq 4$ and $N((a+b\sqrt{6}i)(c+d\sqrt{6}i)) \geq 16$. The non-units $2, 3, \sqrt{6}i, -\sqrt{6}i$ are thus all irreducible as $N(2) = 4$, $N(3) = 9$ and $N(\sqrt{6}i) = N(-\sqrt{6}i) = 6$. We have thus two different prime factorisations of 6 given by 2×3 and $(\sqrt{6}i)(-\sqrt{6}i)$ in $\mathbf{Z}[\sqrt{-6}]$, where 2 and 3 are not associates to $\pm\sqrt{6}i$. So $\mathbf{Z}[\sqrt{-6}]$ is not a UFD.

6a). If $I \subseteq R$ and $J \subseteq S$ are ideals in the rings R and S , then it follows from the subgroup criterion that $I \times J$ is an additive subgroup of $R \times S$. Further, if $(r, s) \in R \times S$ and $(i, j) \in I \times J$, then $(r, s)(i, j) = (ri, sj)$ and $(i, j)(r, s) = (ir, js)$ are both in $I \times J$, such that $I \times J$ is an ideal of $R \times S$. If we apply this to the two trivial ideals in R and S , then we get four ideals $R \times S, R \times \{0_S\}, \{0_R\} \times S, \{0_R\} \times \{0_S\}$ in $R \times S$ for any two rings and in particular for fields $R = K$ and $S = L$.

b) Let I be an ideal in $K \times L$ for two fields K and L . There are then four cases.

Case 1: There exists $(a, b) \in I$ with $a \neq 0_K$ and $b \neq 0_L$. Then $(a^{-1}, b^{-1})(a, b) = (1_R, 1_S) \in I$ such that $I = K \times L$ as any $(r, s) = (r, s)(1_R, 1_S) \in I$.

Case 2: $I \subseteq K \times \{0_L\}$, but $I \neq \{0_K\} \times \{0_L\}$. We have then that $(a, 0) \in I$ for some $a \neq 0$ and hence that $(a^{-1}, 0)(a, 0) = (1_R, 0_L) \in I$. But then $I = K \times \{0_L\}$ as any element $(r, 0) \in K \times \{0_L\}$ lies in I as $(r, 0) = (r, 0)(1_R, 0_L) \in I$.

Case 3: $I \subseteq \{0_K\} \times L$, but $I \neq \{0_K\} \times \{0_L\}$. Then $(0_R, 1_L) \in I$ and $I = \{0_K\} \times L$ by the same arguments as in case 2.

Case 4: $I = \{0_K\} \times \{0_L\}$.

There are thus no other ideals in $K \times L$ than $K \times L, K \times \{0_L\}, \{0_K\} \times L$ and $\{0_K\} \times \{0_L\}$ if K and L are fields.