Math247 January 08 Solutions

Jon Woolf

January 25, 2008

SECTION A

1. There is a finite field of size n if and only if $n = p^k$ where $p \in \mathbf{N}$ is a prime and $k \in \mathbf{N}$.

(i) There is a field with 19 elements, namely $\mathbf{Z}/19\mathbf{Z}$.

(ii) There is no field with 54 elements because $54 = 2 \times 27$ is not prime.

(iii) There is a field with 9 elements because $9 = 3^2$ is a prime power. To find it we need to find an irreducible polynomial f of degree 2 in the ring $(\mathbf{Z}/3\mathbf{Z})[x]$. The quotient $(\mathbf{Z}/3\mathbf{Z})[x]/\langle f \rangle$ will then be a field with 9 elements. Take $f = x^2 + 1$; this is irreducible because there are no roots in $\mathbf{Z}/3\mathbf{Z}$ since $f(0) = 1, f(1) = 2$ and $f(2) = 2$.

2. To decide whether the abelian groups

$$A = \langle a, b \mid 4a + 6b, 3a + 3b \rangle \quad \text{and} \quad B = \langle a, b, c \mid a + 3c, b - 4c, 2b - 2c \rangle$$

are isomorphic or not we write the relations in matrix form and reduce them to diagonal matrices using invertible integral row and column operations.

First A:

$$\begin{pmatrix} 4 & 6 \\ 3 & 3 \end{pmatrix} \overset{C_2 - C_1}{\longrightarrow} \begin{pmatrix} 4 & 2 \\ 3 & 0 \end{pmatrix} \overset{C_1 \leftrightarrow C_2}{\longrightarrow} \begin{pmatrix} 2 & 4 \\ 0 & 3 \end{pmatrix} \overset{C_2 - 2C_1}{\longrightarrow} \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$$

So $A \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$.

Then B:

$$\begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & -4 \\ 0 & 2 & -2 \end{pmatrix} \overset{C_3 - 3C_1}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -4 \\ 0 & 2 & -2 \end{pmatrix}$$

$$\overset{C_3 + 4C_2}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 6 \end{pmatrix} \overset{R_3 - 2R_2}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

So $B \cong \mathbf{Z}/6\mathbf{Z}$.

Finally we note that $\mathbf{Z}/6\mathbf{Z} \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$ so that A and B are isomorphic.

3. A unit in a commutative ring R with a 1 is an element $r \in R$ for which there exists a multiplicative inverse $s \in R$ with $rs = 1$.

(i) 3 is a unit in $\mathbf{Q}$ because $3 \times \frac{1}{3} = 1$.

(ii) 3 is not a unit in $\mathbf{Z}/6\mathbf{Z}$ because it is a zero-divisor: $2 \times 3 = 0$.

(iii) 3 is a unit in $\mathbf{Z}/8\mathbf{Z}$ because $3 \times 3 = 1$.

(iv) x^2 is not a unit in $\mathbf{Z}[x]$ because the degree of $x^2 f$ is ≥ 2 for any $f \neq 0$.

(v) $1 - i$ is not a unit in $\mathbf{Z}[i]$ because the only units are the elements $\pm 1, \pm i$ which have complex norm 1.

4. An *irreducible* element of R is a non-zero non-unit $r \in R$ such that if $r = st$ then either s or t is unit.

(i) $f = x^3 + x + 1$ is irreducible in $(\mathbf{Z}/5\mathbf{Z})[x]$ because it has no roots: $f(0) = 1, f(1) = 3, f(2) = 1, f(3) = 1$ and $f(4) = 4$. (If a cubic factorises then it must have at least one linear factor, i.e. at least one root.)

(ii) $f = x^3 + x + 1$ is irreducible in $\mathbf{Q}[x]$ if it is irreducible in $\mathbf{Z}[x]$ (by Gauss's lemma). We can check that f has no integer roots because $f(n) \geq 1$ for $n \geq 0$ and $f(n) \leq -1$ for $n < 0$. So f is irreducible in $\mathbf{Z}[x]$ and thence in $\mathbf{Q}[x]$.

(ii) $f = x^3 + x + 1$ is not irreducible in $\mathbf{R}[x]$ because $f(-1) = -1$ and $f(0) = 1$ so, by the intermediate value theorem, there must be a root in $(-1, 0)$ and thus a factor.

5. A homomorphism $\theta : \mathbf{Z}/12\mathbf{Z} \to \mathbf{Z}/12\mathbf{Z}$ is determined uniquely by specifying $\theta(1)$. Moreover we can specify any $\theta(1) = k \in \mathbf{Z}/12\mathbf{Z}$: the resulting map $\theta(n) = kn$ is a homomorphism because

$$\theta(m+n) = k(m+n) = km + kn = \theta(m) + \theta(n).$$

So there are 12 homomorphisms: $\theta(n) = kn$ for $k = 0, 1, 2, \ldots, 11$. These are clearly all different since the image of 1 is different in each case.

Here is a list of the kernels and images:

θ	$\ker\theta$	$\operatorname{im}\theta$
$n \mapsto 0$	$\{0,1,2,3,4,5,6,7,8,9,10,11\}$	$\{0\}$
$n \mapsto n$	$\{0\}$	$\{0,1,2,3,4,5,6,7,8,9,10,11\}$
$n \mapsto 2n$	$\{0,6\}$	$\{0,2,4,6,8,10\}$
$n \mapsto 3n$	$\{0,4,8\}$	$\{0,3,6,9\}$
$n \mapsto 4n$	$\{0,3,6,9\}$	$\{0,4,8\}$
$n \mapsto 5n$	$\{0\}$	$\{0,1,2,3,4,5,6,7,8,9,10,11\}$
$n \mapsto 6n$	$\{0,2,4,6,8,10\}$	$\{0,6\}$
$n \mapsto 7n$	$\{0\}$	$\{0,1,2,3,4,5,6,7,8,9,10,11\}$
$n \mapsto 8n$	$\{0,3,6,9\}$	$\{0,4,8\}$
$n \mapsto 9n$	$\{0,4,8\}$	$\{0,3,6,9\}$
$n \mapsto 10n$	$\{0,6\}$	$\{0,2,4,6,8,10\}$
$n \mapsto 11n$	$\{0\}$	$\{0,1,2,3,4,5,6,7,8,9,10,11\}$

(Note that, as Lagrange's theorem guarantees, the kernel and image always have size dividing 12 and, as the first isomorphism theorem guarantees, the product of their sizes is always 12.)

From the table there are 4 isomorphisms $\theta(n) = kn$ for $k = 1, 5, 7$ and 11, i.e. for those values of k which are coprime to 12.

6. We use the Euclidean algorithm. Let $\alpha = 2 - 5i$ and $\beta = 2 + 2i$ and consider the augmented matrix

$$\left(\begin{array}{cc|c} 1 & 0 & 2-5i \\ 0 & 1 & 2+2i \end{array}\right) \xrightarrow{R_1+iR_2} \left(\begin{array}{cc|c} 1 & i & -3i \\ 0 & 1 & 2+2i \end{array}\right)$$
$$\xrightarrow{R_1+R_2} \left(\begin{array}{cc|c} 1 & 1+i & 2-i \\ 0 & 1 & 2+2i \end{array}\right)$$
$$\xrightarrow{R_2-iR_1} \left(\begin{array}{cc|c} 1 & 1+i & 2-i \\ -i & 2-i & 1 \end{array}\right)$$

Since we clearly obtain a 0 in the top right entry at the next stage

$$\gcd(2-5i, 2+2i) = 1 = (2-i)\beta - i\alpha.$$

(It would also be possible, and admissible, to find the gcd by using the norm: $N(2-5i) = 29$ and $N(2+2i) = 8$ and since these have no common factors $\gcd(2-5i, 2+2i) = 1$. However we would then need to use the Euclidean algorithm to write the gcd as a linear combination of $2-5i$ and $2+2i$.)

SECTION B

7. A homomorphism of abelian groups is a map $\theta : A \to B$ such that $\theta(a + a') = \theta(a) + \theta(a')$ for all $a, a' \in A$.

A homomorphism of rings is a map $\theta : R \to S$ such that $\theta(r+r') = \theta(r)+\theta(r')$ and $\theta(rr') = \theta(r)\theta(r')$ for all $r, r' \in R$. Furthermore we require that $\theta(1) = 1$. (In particular it is a homomorphism of the underlying additive abelian groups.)

(i) $\varphi : \mathbf{Z} \to \mathbf{Z} : m \mapsto 2m$ is a homomorphism of abelian groups because $\varphi(m + n) = 2(m + n) = 2m + 2n = \varphi(m) + \varphi(n)$. It is not a ring homomorphism because, e.g. $\varphi(2 \cdot 3) = 12 \neq 4 \cdot 6 = \varphi(2)\varphi(3)$.

(ii) $\varphi : \mathbf{Z} \to \mathbf{Z} : m \mapsto m^3$ is not a homomorphism of abelian groups, and therefore not a ring homomorphism either. This is because, e.g. $\varphi(1+1) = 2^3 = 8 \neq 1 + 1 = \varphi(1) + \varphi(1)$.

(iii) $\varphi : (\mathbf{Z}/3\mathbf{Z})[x] \to (\mathbf{Z}/3\mathbf{Z})[x] : f \mapsto f^3$ is a homomorphism of rings, and therefore a homomorphism of abelian groups too. This is because, $\varphi(a+b) = (a+b)^3 = a^3+3a^2b+3ab^2+b^3 = a^3+b^3 = \varphi(a)+\varphi(b)$ and $\varphi(ab) = (ab)^3 = a^3b^3 = \varphi(a)\varphi(b)$.

(iv) $\varphi : \mathbf{Z}[x] \to \mathbf{C} : f \mapsto f(1 + i)$ is a homomorphism of rings, and therefore a homomorphism of abelian groups too. This is easy to check, or we can quote the result that evaluation maps of this kind are always homomorphisms.

8. A *prime ideal* I of a ring R is an ideal (an additive subgroup closed under multiplication by an arbitrary element of R) with the additional property that $rs \in I$ implies either $r \in I$ or $s \in I$.

(i) $6\mathbf{Z}$ is an ideal in $\mathbf{Z}$ but it is not prime, e.g. $2 \cdot 3 = 6 \in 6\mathbf{Z}$ but neither 2 nor 3 is in $6\mathbf{Z}$.

(ii) $13\mathbf{Z}$ is a prime ideal in $\mathbf{Z}$: if $mn \in 13\mathbf{Z}$ then $13|mn$ so $13|m$ or $13|n$ (because 13 is prime), i.e. either $m \in 13\mathbf{Z}$ or $n \in 13\mathbf{Z}$.

(iii) $I = \{f \in \mathbf{Q}[x] \mid f(8) = 0\}$ is a prime ideal in $\mathbf{Q}[x]$: if $fg \in I$ then $0 = (fg)(8) = f(8)g(8)$ so either $f(8) = 0$ or $g(8) = 0$, i.e. either $f \in I$ or $g \in I$.

(iv) $I = \langle x^2 + 1\rangle$ is not a prime ideal in $\mathbf{C}[x]$ because, e.g. $(x + i)(x - i) = x^2 + 1 \in I$ but neither of $x \pm i$ is in I as they are not multiples of $x^2 + 1$.

9.

(i) The possible tables of factors, p-primary and Smith Normal Form decompositions for an abelian group of size $45 = 3^2 \times 5$ are listed below. There are two possible tables, and so two isomorphism classes of abelian groups of size 45.

Table of factors	P-primary decomp	SNF decomp
$\begin{array}{c\|c\|c\|c} 0 & 2 & 3 & 5 \\ \hline\hline & & 9 & 5 \end{array}$	$\mathbf{Z}/9\mathbf{Z} \oplus \mathbf{Z}/5\mathbf{Z}$	$\mathbf{Z}/45\mathbf{Z}$
$\begin{array}{c\|c\|c\|c} 0 & 2 & 3 & 5 \\ \hline\hline & & 3 & 5 \\ & & 3 & \end{array}$	$\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/5\mathbf{Z}$	$\mathbf{Z}/15\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$

(ii) The possible tables of factors, p-primary and Smith Normal Form decompositions for an abelian group of size $72 = 3^2 \times 2^3$ are listed below. There are six possible tables, and so six isomorphism classes of abelian groups of size 72.

Table of factors	P-primary decomp	SNF decomp
$\begin{array}{c\|c\|c} 0 & 2 & 3 \\ \hline & 8 & 9 \end{array}$	$\mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/9\mathbf{Z}$	$\mathbf{Z}/72\mathbf{Z}$
$\begin{array}{c\|c\|c} 0 & 2 & 3 \\ \hline & 4 & 9 \\ & 2 & \end{array}$	$\mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/9\mathbf{Z}$	$\mathbf{Z}/36\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$
$\begin{array}{c\|c\|c} 0 & 2 & 3 \\ \hline & 2 & 9 \\ & 2 & \\ & 2 & \end{array}$	$\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/9\mathbf{Z}$	$\mathbf{Z}/18\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$
$\begin{array}{c\|c\|c} 0 & 2 & 3 \\ \hline & 8 & 3 \\ & & 3 \end{array}$	$\mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$	$\mathbf{Z}/24\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$
$\begin{array}{c\|c\|c} 0 & 2 & 3 \\ \hline & 4 & 3 \\ & 2 & 3 \end{array}$	$\mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$	$\mathbf{Z}/12\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$
$\begin{array}{c\|c\|c} 0 & 2 & 3 \\ \hline & 2 & 3 \\ & 2 & 3 \\ & 2 & \end{array}$	$\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$	$\mathbf{Z}/6\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$

10. We can easily check that $f = x^4 + x + 1$ has no roots in $\mathbf{Z}/2\mathbf{Z}$ since $f(0) = 1 = f(1)$ so the only possible factorisation is of the form

$$f = (x^2 + ax + 1)(x^2 + bx + 1) = x^4 + (a + b)x^3 + abx^2 + (a + b)x + 1.$$

This is impossible as comparing coefficients of x and x^3 gives $0 = a + b = 1$. Hence f is irreducible in $R = (\mathbf{Z}/2\mathbf{Z})[x]$.

(i) The number of elements in the quotient ring R/I where $I = \langle f \rangle$ is $2^4 = 16$ and the number of elements in the group of units $(R/I)^*$ is $16 - 1 = 15$. The possible orders of elements in $(R/I)^*$ are the divisors of 15 namely $1, 3, 5$ and 15.

(ii) It is clear that $x \neq 1$ and $x^3 \neq 1$. Since $x^5 = x^4 \cdot x = (x + 1)x = x^2 + x \neq 1$ we deduce that x must have the only other possible order, namely 15.

(iii) The element 1 has order 1. The element $x^5 = x^2 + x$ has order 3: certainly $(x^5)^3 = x^{15} = 1$ and since x^3 and $(x^3)^3 = x^9$ are not 1 this shows x^3 has order 5. A similar argument shows x^5 has order 3. Finally x has order 15.

11. (i) Bézout's theorem for the ring $\mathbf{Q}[x]$ states that if $f, g \in \mathbf{Q}[x]$ then we can find $a, b \in \mathbf{Q}[x]$ with

$$af + bg = \gcd(f, g).$$

Elements of the quotient are represented by polynomials $g \in \mathbf{Q}[x]$ with $\deg g < \deg f$. If f is irreducible in $\mathbf{Q}[x]$ and $g \neq 0$ then $\gcd(f, g) = 1$ for any such g. By Bézout's theorem we can find $a, b \in \mathbf{Q}[x]$ with

$$af + bg = 1.$$

Hence $bg = 1 \in \mathbf{Q}[x]/\langle f \rangle$ so that (the class of) b is a multiplicative inverse for (the class of) g. Since every element of the quotient has a multiplicative inverse $\mathbf{Q}[x]/\langle f \rangle$ is a field.

(ii)

(a) We apply the Euclidean algorithm to $f = x^3 + x + 1$ and $g = x^2 + 1$. The first step is

$$f = xg + 1$$

so we see that $f - xg = 1$, i.e. $xg = 1$ in $\mathbf{Q}[x]/\langle x^3 + x + 1 \rangle$.

(b) We apply the Euclidean algorithm to $f = x^3 + x^2 + 1$ and $g = x^2 + 1$. We get

$$\begin{aligned} f &= (x+1)g - x \\ g &= (-x)(-x) + 1 \end{aligned}$$

Rearranging we have

$$1 = g - (-x)(-x) = g + x(f - (x+1)g) = xf - (x^2 + x - 1))g$$

so the multiplicative inverse of (the class of) g in $\mathbf{Q}[x]/\langle x^3 + x^2 + 1 \rangle$ is (the class of) $1 - x - x^2$.