# Basic Algebra 1
# Solutions to Practice Final

Bahare Mirza

December 10, 2012

**(1)** We want to compute the reduced residue of $3^{N+1}$ where $N =$ some big power of 10. Note that the following works as long as the power of 10 is bigger than 0, and not just in the particular case of our interest!

First step is to observe that $3^3 = 27 \equiv 1 \pmod{13}$. Secondly, we have $N \equiv 1 (\text{mod } 3)$, and hence $N+1 \equiv 2$, and so $N+1 = 3k+2$ for some integer $k$.

From these two facts we get

$$\begin{aligned} 3^{N+1} &= 3^{3k+2} \\ &= (3^3)^k 3^2 \\ &\equiv (1)^k 3^2 \\ &\equiv 9, \end{aligned}$$

where all congruences are modulo 3.

**(2)** Take $R = \mathbb{Z}[x]$. Then the ideal $I = (2, x)$ is not principal and the quotient $R/I$ is $\mathbb{Z}/2\mathbb{Z}$.

**(3)** a) If $p$ is of the form $3m+1$ then

$$\begin{aligned} x^p - x &= x(x^{p-1} - 1) \\ &= x(x^{3m} - 1) \\ &= x((x^3)^m - 1) \\ &= x(x^3 - 1)((x^3)^{m-1} + (x^3)^{m-2} + \cdots + x^3 + 1). \end{aligned}$$

Hence $x^3 - 1 | x^p - x$, and $gcd(x^3 - 1, x^p - x) = x^3 - 1$.

b)For this case we use the fact that $gcd(x^3 - 1, x^p - x)$ in the ring $\mathbb{Z}/p\mathbb{Z}[x]$, is a polynomial of degree $d$ equal to the number of distinvt roots of $x^3 - 1$ in $\mathbb{Z}/p\mathbb{Z}$ (proved in exercise 10 part (c) of assignment 3.)

We show that $x^3 - 1$ has only one root in $\mathbb{Z}/p\mathbb{Z}$;

If $a$ is such a root then we have $a^3 = 1$. But $a \in \mathbb{Z}/p\mathbb{Z}$ and hence $a^p = a$ by Fermat's Little Theorem, so

$$\begin{aligned} a &= a^p \\ &= a^{3m+2} \\ &= (a^3)^m a^2 \\ &= (1)^m a^2 = a^2. \end{aligned}$$

So $a(a-1) = a^2 - a = 0$ and hence, as $\mathbb{Z}/p\mathbb{Z}$ is a field and has no zero-divisors, $a$ is either 0 or 1. But $a$ can not be zero, as $a^3 = 1$, so $a = 1$ is the only option, that is the only root of $x^3 - 1$. This shows that $d = 1$.

Now $x-1|x^3-1 = (x-1)(x^2+x+1)$ and $x-1|x^p-x = x(x-1)(x^{p-2}+\cdots+1)$, so $x - 1|gcd(x^3 - 1, x^p - x)$. Since the latter has degree 1 we get

$$x - 1 = gcd(x^3 - 1, x^p - x)$$

**(4)** Any element of order $t$ of the group $G$ is in fact a root of the polynomial $x^t - 1$, as the group operation on $G$ is multiplication in $F$ and the identity is just 1. But $x^t - 1$ is a polynomial of degree $t \geq 1$ in $F[x]$ and hence has at most $t$ roots. This implies that $G$ has at most $t$ elements of order $t$.

**(5)** Fermat's Little Theorem states that for every prime number $p$ and every integer $a \not\equiv 0 \bmod p$, we have

$$a^{p-1} \equiv 1 \quad mod \quad p.$$

Lagrange's Theorem says that for every finite group $G$ and each of its subgroupe $H$ we have

$$|H||G|.$$

The proof of Fermat's Little Theorem using Lagrange's Theorem goes as follows; Take $G = \mathbb{Z}/p\mathbb{Z}^\times$, the group operation being multiplication in $\mathbb{Z}/p\mathbb{Z}$. Such $a$ as in the assumption of FLT gives an element of $G$. Further take $H$ to be the cyclic subgroup generated by $a$. Then $|H| = ord(a)$ and by Lagrange's Theorem $ord(a) = |H|$ divides $|G| = p - 1$. So $p - 1 = k \times ord(a)$ for some integer $k$. Now we have

$$\begin{aligned} a^{p-1} &= a^{k \times ord(a)} \\ &= (a^{ord(a)})^k \\ &\equiv (1)^k \\ &= 1. \end{aligned}$$

This proves FLT.

**(6)** To prove that $1+\sqrt{-11}$ is irreducible we use the norm function $f : \mathbb{Z}[\sqrt{-11}] \to \mathbb{Z}$, introduced in the solution of exercise 1 of assignment 2. We saw that this function is "mutiplicative":

$$f((a+b\sqrt{-11})(c+d\sqrt{-11})) = f(a+b\sqrt{-11})f(c+d\sqrt{-11}).$$

Now assume $1+\sqrt{-11} = (a+b\sqrt{-11})(c+d\sqrt{-11})$. We will prove that either $a+b\sqrt{-11}$ or $c+d\sqrt{-11}$ is equal to one or minus one.

By multiplicity of the norm function we get

$$\begin{aligned} 12 &= f(1+\sqrt{-11}) \\ &= f((a+b\sqrt{-11})(c+d\sqrt{-11})) \\ &= f(a+b\sqrt{-11})f(c+d\sqrt{-11}) \\ &= (a^2+11b^2)(c^2+11d^2). \end{aligned}$$

So $f(a+b\sqrt{-11})$ and $f(c+d\sqrt{-11})$ will have to be one of the following numbers

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12.$$

Now we show that $\mathbb{Z}[\sqrt{-11}]$ has no elements of norm $\pm 2, \pm 3, \pm 6$. In fact, $a^2 + 11b^2 = f(a+b\sqrt{-11})$ is always positive since $a^2$ and $b^2$ are positive and if $b$ is non-zero then $a^2+11b^2 \geq 11$, and so we cannot get any of the 6 numbers above. On the other hand $2, 3$ and $6$ are not perfect sqaures so cannot equal $a^2$.

So we have proved that $f(a+b\sqrt{-11})$ is $1, 4$ or $12$. But $4$ cannot occur as otherwise $f(c+d\sqrt{-11}) = 3$ which is impossible.

Now if $f(a+b\sqrt{-11}) = 1$ then we should have $b = 0$ and $a = \pm 1$, and so $a+b\sqrt{-11} = \pm 1$.

On the other hand, if $f(a+b\sqrt{-11}) = 12$ then $f(c+d\sqrt{-11}) = 1$ and so $c+d\sqrt{-11} = \pm 1$.

This shows that $1+\sqrt{-11}$ is irreducible.

Now we show the ideal $(3, 1+\sqrt{-11})$ is not principal;

If there was an element $\alpha$ such that $(\alpha) = (3, 1+\sqrt{-11})$ then we shold have $3 = \alpha\beta$ and $1+\sqrt{-11} = \alpha\gamma$ for some $\beta, \gamma \in \mathbb{Z}[\sqrt{-11}]$. But then we should have

$$9 = f(3) = f(\alpha)f(\beta)$$

and

$$12 = f(1+\sqrt{-11}) = f(\alpha)f(\gamma).$$

So $f(\alpha)$ should devide $gcd(9, 12) = 3$ and hence should equal 1 or 3. But we've already seen that our ring has no elements of norm 3, so $f(\alpha) = 1$ which implies $\alpha = \pm 1$ in which case the ideal generated by $\alpha$ is the whole ring. But $(3, 1+\sqrt{-11})$ is not the whole ring (it does not contain 1, for example.) This is a contradiction and proves that $(3, 1+\sqrt{-11})$ is not principal.

Now define a map

$$\phi : \mathbb{Z}[\sqrt{-11}] \to \mathbb{Z}/3\mathbb{Z}$$

which sends $a+b\sqrt{-11}$ to the class $[a-b]$ of $a-b$ in $\mathbb{Z}/3\mathbb{Z}$. We show first that this map is a ring homomorphism;

- $\phi(1) = [1]$
- $$\begin{aligned}\phi((a+b\sqrt{-11})+(c+d\sqrt{-11})) &= \phi(a+c+(b+d)\sqrt{-11}) \\ &= [a+c-(b+d)] \\ &= [a-b]+[c-d] \\ &= \phi(a+b\sqrt{-11})+\phi(c+d\sqrt{-11})\end{aligned}$$
- $$\begin{aligned}\phi((a+b\sqrt{-11})(c+d\sqrt{-11})) &= \phi(ac-11bd+(ad+bc)\sqrt{-11}) \\ &= [ac-11bd-(ad+bc)] \\ &= [ac+bd-ad-bc] \\ &= [(a-b)(c-d)] \\ &= \phi(a+b\sqrt{-11})\phi(c+d\sqrt{-11}).\end{aligned}$$

Second we show it is surjective; in fact image of $\{0,1,2\}$ as a subset of $\mathbb{Z}[\sqrt{-11}]$ is the whole ring $\mathbb{Z}/3\mathbb{Z}$ and so $\phi$ is surjective.

Next we see that $(3, 1+\sqrt{-11})$ is in the kernel; in fact $\phi(3) = [3-0] = [3] = [0]$ and $\phi(1+\sqrt{-11} = [1-1] = [0]$.

Further if $a+b\sqrt{-11}$ is in $Ker(\phi)$, then $[a-b] = 0$ and hence $a = b+3k$ for some integer $k$. We have

$$a+b\sqrt{-11} = 3k+b+b\sqrt{-11} = 3k+b(1+\sqrt{-11}) \in (3, 1+\sqrt{-11}).$$

This shows that $Ker\phi = (3, 1+\sqrt{-11})$.

Now by the First Isomorphism Theorem we have

$$\mathbb{Z}[\sqrt{-11}]/Ker(\phi) \cong Im(\phi).$$

By the obove observation this formula reads

$$\mathbb{Z}[\sqrt{-11}]/(3, 1+\sqrt{-11}) \cong \mathbb{Z}/3\mathbb{Z}.$$

**(7)** For a $2\times 2$ matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $a, b, c, d, \in \{0,1\}$ to be invertible we should have $ad-bc = det(A) \neq 0 \in \mathbb{Z}/2\mathbb{Z}$. So we shold have $ad-bc \equiv 1 \mod 2$. This happens when (1) $ad = 1$ and $bc = 0$ or when (2) $ad = 0$ and $bc = 1$.

In the first case we have

$$\begin{bmatrix} 1,0 \\ 0,1 \end{bmatrix}, \begin{bmatrix} 1,1 \\ 0,1 \end{bmatrix}, \begin{bmatrix} 1,0 \\ 1,1 \end{bmatrix}.$$

And in the second case

$$\begin{bmatrix}0,1\\1,0\end{bmatrix}, \begin{bmatrix}1,1\\1,0\end{bmatrix}, \begin{bmatrix}0,1\\1,1\end{bmatrix}.$$

This gives us all 2 by 2 invertible matrices with entries in $\mathbb{Z}/2\mathbb{Z}$. So $GL_2(\mathbb{Z}/2\mathbb{Z})$ has cardinality 6.

Now each 2 by 2 matrix acts by matrix multiplication on the set of column vectors (2 by 1) with entries in $\mathbb{Z}/2\mathbb{Z}$, namely the set

$$\{\begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\1\end{bmatrix}\}$$

Further if the matrix is invertible, then it fixes the first vector and permutes the other three. We use this idea to define a group isomorphim from $GL_2(\mathbb{Z}/2\mathbb{Z})$ to $S_3$.

Label the four vectors above $\{0,1,2,3\}$ and define a map $\phi : GL_2\mathbb{Z}/2\mathbb{Z} \to S_3$ by letting $\phi(A)$to be the permutation on $\{1,2,3\}$ given by the action of $A$ on the vectors $1,2$ and 3.

It is clear that if $A$ fixes all three vectors (in fact even if it only fixes the first two, then it automatically fixes the third which is the sum of the other two) then $A$ is the identity matrix.

The group operation on both sides is just composition of maps and hence $\phi$ respects the operation and so is a group homomorphism which is injective by the previous paragraph.

Now an injective map of finite sets is surjective if and only if the sets have the same cardinality. In this case both $GL_2$ and $S_3$ have 6 elements and so $\phi$ is also surjective and hence gives and isomorphism of groups.

**(8)** To prove that $H$ is normal in $G$ we need to show that for every $g \in G$ $gH = Hg$.

$H$ has index 2 in $G$, so the number of left cosets (which equals the number of right cosets) of $H$ in $G$ is 2. Since $G$ is the disjoint union of all the left cosets (or the right cosets) we have

$$G = H \sqcup aH$$

for some $a \in G$ such that $aH \neq H$ or equivalently $a \notin H$.

Now for this $a$, $H$ and $Ha$ give two right cosets of $H$ in $G$. Since $a \notin H$ these two right cosets are distinct (hence disjoint) and since we only have two distinct right cosets $\{H, Ha\}$ gives the set of all right cosets of $H$ in $G$. So we have

$$G = H \sqcup Ha.$$

This proves that $aH = Ha$ and for any $h \in H$ in particular, we have $ah \in aH = Ha$ and so $ah = h'a$ for some $h' \in H$.

Now for $g \in G$, if $g \in H$ then we have

$$gH = H = Hg.$$

And if $g \in G$ but $g \notin H$ then $g \in aH$ and so $g = ah$ for some $h \in H$ and we have

$$gH = ahH = aH = Ha = Hh'a = Hah = Hg,$$

as desired, where $h' \in H$ is such that $ah = h'a$.

This proves that $H$ is normal in $G$.

**(9)** Firstly, the intersection of any two subgroups is a subgroup, so $N \cap H$ is a subgroup of G that is included in $H$ and so is a subgroup of $H$. Now we show it is normal in $H$;

For any element $n \in N \cap H$ and $h \in H$ we want to prove that $hnh^{-1} \in N \cap H$.

- $h \in H$ and $n \in H$ so $hnh^{-1} \in H$, as $H$ is a subgroup.
- $h \in G$ and $n \in N$ so $hnh^{-1} \in N$ as $N$ is normal in $G$.

This shows that $hnh^{-1} \in H \cap N$. Hence $H \cap N$ is normal in $H$.

**(10)** We know that for any group homomorphism $f : G \to G', Ker(f)$ is a normal subgroup of $G$. So since $G$ is assumed to be simple, $Ker(f)$ is either $\{e\}$ or the whole group.

If, further, the homomorphism is non-trivial, $Ker(f) \neq G$, and so we should have $Ker(f) = \{e\}$. This implies that any such $f$ is injective, as desired.