Solutions to Exercises for Section 6

(Spring 2009) Exercises 4, 5 and 6 are the ones to try.

1. For what values of $a = 0, 1, 2, 3, 4$ is $\mathbb{Z}_5[X]/\langle X^2 + a\rangle$ a field?

Solution: Equivalently, for what values of $a = 0, 1, 2, 3, 4$ is $X^2 + a$ irreducible in $\mathbb{Z}_5[X]$? Equivalently, since the polynomial is quadratic, for what values of a does $X^2 + a$ have a root; equivalently, for what values of a is $-a$ a square in $\mathbb{Z}_5$? So we just compute the squares in $\mathbb{Z}_5$: $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 4$, $4^2 = 1$ (so, in fact in $\mathbb{Z}_5$, a is a square iff $-a$ is a square). So $\mathbb{Z}_5[X]/\langle X^2 + a\rangle$ is a field iff $a = 2$ or $a = 3$.

2. Find a canonical form for the elements of the ring $R = \mathbb{Z}_2[X]/\langle X^2+1\rangle$ (that is, write down all possible remainders with respect to $X^2 + 1$).
Noting that in $\mathbb{Z}_2[X]/\langle X^2 + 1\rangle$ we have $\alpha^2 = 1$ where $\alpha = X + \langle X^2 + 1\rangle$ is the image of $X \in \mathbb{Z}_2[X]$ in R, draw up the addition and multiplication tables for the ring R.

Is R a domain? a field?

Is $\langle X^2 + 1\rangle$ a prime ideal? a maximal ideal? if neither, what is its radical?

Solution: The possible remainders of polynomials when divided by X^2+1 are: 0, 1, X, $X+1$. So the factor ring $\mathbb{Z}_2[X]/\langle X^2+1\rangle$ has four elements - the images of these - which we may write as 0, 1, α, $\alpha + 1$ (having written α for the image $X + \langle X^2 + 1\rangle$). The addition and multiplication tables are as follows.

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\times$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	1	$\alpha+1$
$\alpha+1$	0	$\alpha+1$	$\alpha+1$	0

This ring R is not a domain (so certainly not a field) since it contains a zero-divisor, namely $\alpha + 1$. So, by 4.17, $\langle X^2 + 1\rangle$ is not a prime ideal (hence, by 4.18, not a maximal ideal). This reflects that fact that $X^2 + 1$ is reducible, being $(X + 1)^2$. Clearly $X + 1$ is in $\sqrt{\langle X^2 + 1\rangle}$ (since its square is in $\langle X^2 + 1\rangle$) and $\langle X + 1\rangle$ is a prime ideal so it follows that $\sqrt{\langle X^2 + 1\rangle} = \langle X + 1\rangle$.

3. Let $f = X^2 + X + 2 \in \mathbb{Z}_3[X]$. Check that f is irreducible, hence that $K = \mathbb{Z}_3[X]/\langle f\rangle$ is a field. Set $\alpha = X + \langle f\rangle$ and list all the elements of K. Identify each of α^{-2} and $(\alpha^2 + 1)(2\alpha + 1)$ as one of the elements on your list. Determine whether or not $Y^2 + 1 \in K[Y]$ is reducible or irreducible.

Solution: Since f has degree ≤ 3, it is enough to check for roots: $f(0) = 2$, $f(1) = 1$, $f(2) = 2$, so f has not root, hence is irreducible. By Kronecker's Theorem a basis for K over $\mathbb{Z}_3$ is $\{1, \alpha\}$ and so the elements of K are: 0, 1, 2, α, $\alpha + 1$, $\alpha + 2$, 2α, $2\alpha + 1$, $2\alpha + 2$.

We have $\alpha^2 + \alpha + 2 = 0$, so $\alpha(\alpha + 1) = 1$, hence $\alpha^{-1} = \alpha + 1$. Therefore $\alpha^{-2} = (\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = -\alpha - 2 + 2\alpha + 1 = \alpha - 1 = \alpha + 2$. We have $\alpha^2 = 2\alpha + 1$ and use this to simplify $(\alpha^2 + 1)(2\alpha + 1) = (2\alpha + 2)(2\alpha + 1) = \alpha^2 + 1 = 2\alpha$.

The last part is asking whether there is a root of $Y^2 + 1 = 0$ in K; that is, is there an element of K whose square is $-1(= 2)$? One possibility is just to start checking, squaring the elements of K in turn, to see if 2 is a square in K. Alternatively, take a typical element $a\alpha + b$, square it and rearrange, to get $(2a^2 + 2ab)\alpha + (a^2 + b^2)$ which, if equal to 2, gives $a(a + b) = 0$ and $a^2 + b^2 = 2$, so either $a = 0$ (since a, b come from the domain $\mathbb{Z}_3$) and then $b^2 = 1$ - which has no solution in $\mathbb{Z}_3$, or $a = 2b$ and then $2a^2 = 2$, giving $a = 1, b = 2$ or $a = 2, b = 1$, that is, $a\alpha + b = \alpha + 2$ or $2\alpha + 1$. We check $(Y - (\alpha + 2))(Y - (2\alpha + 1)) = \cdots = Y^2 + 1$, showing that $Y^2 + 1$ is reducible.

4. Write down a non-constant polynomial in $\mathbb{Z}_5[X]$ which has no root in $\mathbb{Z}_5$.

Solution: One possibility is to write down a polynomial of which every element is a root, so $X(X - 1)(X - 2)(X - 3)(X - 4)$, and then add 1: the value of each element of $\mathbb{Z}_5$ on $X(X - 1)(X - 2)(X - 3)(X - 4) + 1$ is $0 + 1 = 1$.

There are plenty of other examples. For instance, there is some quadratic polynomial in $\mathbb{Z}_5[X]$ with no root in $\mathbb{Z}_5$ (because there are 25 different polynomials of the form $X^2 + aX + b$ but there are only 5 linear polynomials $X - c$, hence only 15 different polynomials which are of the form $(X - c)(X - d)$ (10 with $c \neq d$ and 5 with $c = d$), leaving 10 monic irreducible quadratic monic polynomials. So just trying one at random will have a good chance of working (the most natural(?) one to try first, namely $X^2 + X + 1$, indeed has no root) and is certainly quicker than listing all 15 monic reducible quadratics then writing down one not on this list. An alternative is to make a little table with the 5 possible values of X and, underneath, the corresponding values of X^2 - that makes spotting a combination $X^2 + aX + b$ which never gives 0 quite easy.

5. Show that $\sqrt{2} - \sqrt{3}$ is an algebraic number by finding a non-zero polynomial with rational coefficients of which it is a root.

Solution: $(\sqrt{2} - \sqrt{3})^2 = 2 - 2\sqrt{2}\sqrt{3} + 3$ so, writing $a = \sqrt{2} - \sqrt{3}$, we have $a^2 = 5 - 2\sqrt{2}\sqrt{3}$, hence $a^2 - 5 = -2\sqrt{2}\sqrt{3}$, so $(a^2 - 5)^2 = 24$. Expanding, we obtain $a^4 - 10a^2 + 25 = 24$, so $\sqrt{2} - \sqrt{3}$ is a root of $X^4 - 10X^2 + 1$, hence is an algebraic number.

6. Show that each of (i) $1 + 2^{1/3}$ and (ii) $2^{1/3} + 3^{1/3}$ is an algebraic number by finding a non-zero polynomial with rational coefficients of which it is a root.

Solution: (i) Set $a = 1 + 2^{1/3}$; then $a^3 = 1 + 3 \cdot 2^{1/3} + 3 \cdot 2^{2/3} + 2$, giving $a^3 = 3 + 3(a - 1) + 3(a - 1)^2$. So $1 + 2^{1/3}$ is a root of $X^3 - X^2 + X - 1$, hence is an algebraic number.
(ii) Set $a = 1 + 2^{1/3}$; then $a^3 = 2 + 3 \cdot 2^{2/3}3^{1/3} + 3 \cdot 2^{1/3}3^{2/3} + 3 = 5 + 3(2^{1/3} + 3^{1/3})2^{1/3}3^{1/3}$, that is, $a^3 = 5 + 3a2^{1/3}3^{1/3}$. Rearrange and cube: $(a^3 - 5)^3 = 27a^36$ which you can simplify if you really want to. [This gives a degree 9 polynomial of which a is a root; perhaps there is one of lower degree but I didn't

check - and the question does not ask for the best/lowest-degree polynomial satisfied by a.]

7. Let $\mathbb{F}$ be the field with 4 elements which is obtained from $\mathbb{Z}_2$ by adding a root α of the polynomial X^2+X+1. How many monic irreducible polynomials of degree 2 are there in $\mathbb{F}[X]$? Find one of them.

Solution: A monic polynomial of degree 2 has the form $X^2 + aX + b$ where $a, b \in \{0, 1, \alpha, \alpha + 1\}$ (where, note, $\alpha^2 = \alpha + 1$). There are 4 choices of each of a, b, so 16 such polynomials in all. Those which are reducible must have the form $(X - c)(X - d)$: there are $4 \times 3/2 = 6$ of these with $c \neq d$ and 4 with $c = d$. So there are 10 reducible monic polynomials of degree 2, leaving 6 monic irreducible polynomials of degree 2.

To find one of these irreducible polynomials, you could compute the 10 reducible ones and then take a polynomial not on the list, but that looks a little tedious, so you could just choose one at random, and check (then take another if your first choice proves to be reducible, etc.). Or we can say: let's find values of a and b such that $X^2+aX+b = (X-c)(X-d)$ has no solution, that is, such that $a = c+d$, $b = cd$ has no solution. There are quite a few possibilities there, so let's make the guess that there is an irreducible polynomial with constant coefficient 1, that is $b = 1$, so $a = c + c^{-1}$. But the only values of $c + c^{-1}$ with $c \in L$ are: $1+1 = 0$, $\alpha+(\alpha+1) = 1$ - so that worked: choosing $b = 1$ and $a = \alpha$ (or $a = \alpha + 1$) gives the irreducible polynomial $X^2 + \alpha X + 1$ (which might well have been the first one you'd try under the "choose one at random" method).