Solutions to final review sheet

Remember: our final is at 3.15 on Tuesday March 18!!!

1. (i) Let R be a ring. What is an *irreducible element* $x \in R$?
(ii) Determine which of the following polynomials in $\mathbb{Z}_2[x]$ are irreducible, explaining your method carefully. For the ones that are reducible, factor them into irreducibles.
(a) $x^2 + 1$;
(b) $x^3 + 1$;
(c) $x^3 + x + 1$;
(d) $x^3 + x^2 + 1$;
(e) $x^3 + x^2 + x + 1$;
(iii) Which of the following Gaussian integers are irreducible? For the ones that are reducible, factor them into irreducibles.
(a) 1;
(b) 11;
(c) 17;
(d) $1 + i$;
(e) $10 + 10i$.
Solution. (i) An irreducible element is a non-zero, non-unit x such that if $x = yz$ for $y, z \in R$, either y or z is a unit.
(ii) (a) $(x + 1)^2$; (b) $(x + 1)(x^2 + x + 1)$; (c) $x^3 + x + 1$ (irreducible as no roots); (d) $x^3 + x^2 + 1$ (irreducible as no roots); (e) $(x + 1)^3$.
(iii) (a) NO its a unit; (b) We know from class that primes congruent to 3 mod 4 are irreducible as Gaussian integers, so this is irreducible; (c) while this is reducible as its $(4 + i)(4 - i)$; (d) this is irreducible as $|1 + i|^2 = 2$ which is prime; (e) $10 + 10i$. It is $(1 + i)^2(1 - i)(1 + 2i)(1 - 2i)$. These factors are all irreducible as their degrees are prime.
2. (i) If R is a ring and $a \in R$, define what the notation (a) means. Prove that (a) is an *ideal* of R.
(ii) Now let R be the ring $F[x]/(x^4 + x^2 + 1)$. Suppose that

$$x^7 = a_3x^3 + a_2x^2 + a_1x + a_0$$

in R. Calculate the numbers a_0, a_1, a_2, a_3.
(iii) Factorize the polynomial $x^4 + x^2 + 1$ into irreducibles, working in the ring $\mathbb{Z}_3[x]$.
(iv) Is the factor ring $\mathbb{Z}_3[x]/(x^4 + x^2 + 1)$ a field? Explain.
Solution. (i) (a) denotes $\{ab \mid b \in R\}$. It is an ideal: it clearly contains 0 as $0 = a0$; it is closed under addition since $ab + ac = a(b + c)$; it is extra closed under multiply since $(ab)c = a(bc)$.
(ii) Divide $x^4 + x^2 + 1$ into x^7:

$$x^7 = (x^4 + x^2 + 1)(x^3 - x) + x$$

Reducing modulo $x^4 + x^2 + 1$ we see that $x^7 = x$ in R. Hence, $a_0 = a_2 = a_3 = 0$ and $a_1 = 1$.
(iii) $x^4 + x^2 + 1 = x^4 - 2x^2 + 1 = (x^2 - 1)^2 = (x - 1)^2(x + 1)^2 = (x + 1)^2(x + 2)^2$.
(iv) NO because $x^4 + x^2 + 1$ is not irreducible.
3. Let m, n be coprime positive integers. The Chinese remainder theorem says that $\mathbb{Z}_{mn} \cong Z_m \times \mathbb{Z}_n$.
(i) List *all* the elements of the ring $\mathbb{Z}_2 \times \mathbb{Z}_3$.
(ii) Compute the *multiplication table* of $\mathbb{Z}_2 \times \mathbb{Z}_3$.
(iii) Write down the isomorphism between $\mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_6$ coming from the proof of the Chinese Remainder Theorem explicitly (i.e. pair up the elements of $\mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_6$ according to the 1–1 correspondence of the isomorphism).
(iv) Prove or disprove: $\mathbb{Z}_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
Solution. (i) Let me write ab instead of the pair $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_3$. Then the elements are $00, 11, 01, 10, 02, 12$.

(ii) The multiplication table is:

	00	11	02	10	01	12
00	00	00	00	00	00	00
11	00	11	02	10	01	12
02	00	02	01	00	02	01
10	00	10	00	10	00	10
01	00	01	02	00	01	02
12	00	12	01	10	02	11

(iii) The isomorphism $\mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ is given by $0 \mapsto 00, 1 \mapsto 11, 2 \mapsto 02, 3 \mapsto 10, 4 \mapsto 01, 5 \mapsto 12$. You can really see the multiplicativity of this map explicitly as follows. Substitute 00 *by* 0, 11 *by* 1, 01 *by* 2, ... *in the above table. It becomes exactly the multiplication table in the ring $\mathbb{Z}_6$:*

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(iv) False. In $\mathbb{Z}_4$, $1 + 1 = 2 \neq 0$. In $\mathbb{Z}_2 \times \mathbb{Z}_2$, $(1, 1) + (1, 1) = (0, 0)$. So there is no way they could be isomorphic.

4. (i) Define an *integral domain.*
(ii) Determine whether the ring $\mathbb{Z}[x]/(x^4 - 16)$ is an integral domain, explaining your answer carefully.
Solution. (i) A ring such that $ab = 0$ implies either $a = 0$ or $b = 0$.
(ii) NO. The element $x^2 - 4 + (x^4 - 16)$ is a non-zero zero divisor. Multiply it by $x^2 + 4 + (x^4 - 16)$ and you get zero!

5. (i) State the Eisenstein criterion.
(ii) Determine which of the following polynomials in $\mathbb{Q}[x]$ are irreducible:
(a) $x^5 - 4x + 22$;
(b) $x^5 - 4x - 1$;
(c) $x^{11} - 6x^4 + 12x^3 + 36x - 6$.
Which of these are irreducible in $\mathbb{R}[x]$ instead?
(iii) Show that there are an infinite number of integers a such that $x^7 + 15x^2 - 30x + a$ is irreducible in $\mathbb{Q}[x]$.
(iv) Factor the polynomial $x^{24} - 1$ completely into irreducibles in $\mathbb{Q}[x]$.
Solution. (i) If $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ and there is a prime p such that $p|a_0, a_1, \ldots, a_{n-1}$ but $p^2 \nmid a_0$, then the polynomial is irreducible over $\mathbb{Q}$.
(ii) (a) irreducible by Eisenstein with $p = 2$; (b) $x = 1$ is a root, so it is reducible!; (c) irreducible by Eisenstein with $p = 2$ or $p = 3$! None of these polynomials are irreducible over $\mathbb{R}$: over $\mathbb{R}$ only linear polynomials and certain quadratics are irreducible, anything of degree > 2 is automatically reducible.
(iii) Just take $a = 2^k 5$ for $k \geq 1$. They are then all irreducible by Eisenstein with $p = 5$.

6. Let F be a field. Define the map

$$\phi : F[x] \to F[x], \qquad f(x) \mapsto f(x + 1).$$

So for example, $\phi(x) = x + 1, \phi(x^2) = (x + 1)^2 = x^2 + 2x + 1$, etc... Prove carefully that ϕ is an isomorphism.
Solution. This is more confusing than difficult. Let us just check the definition of homomorphism.

$\phi(1) = 1$ is clear because it is constant so nothing changes when we replace x by $x+1$.
$\phi(f(x)+g(x)) = f(x+1)+g(x+1) = \phi(f(x))+\phi(g(x))$ so it is additive.
Similarly, $\phi(f(x)g(x)) = f(x+1)g(x+1) = \phi(f(x))\phi(g(x))$ so it is multiplicative.
Hence it is a homomorphism.

7. Find a non-zero zero divisor in the ring $\mathbb{Z}[i]/(5+i)$.

Solution. It is isomorphic to $\mathbb{Z}_{26}$. So why not try $2+(5+i)$. It is not zero because 2 is obviously not a multiple of $5+i$ (e.g. the degree of 2 is 4 which is not a multiple of the degree 26 of $5+i$). It is a zero divisor because $2.13 = 26 = (5+i)(5-i)$ which is zero in $\mathbb{Z}[i]/(5+i)$ as it is a multiple of $5+i$.

8. Let R be a ring. Fix an element $a \in R$ and set

$$I_a = \{r \in R \mid r^2 a = 0\}.$$

Prove that I_a is an ideal of the ring R.

Solution. This question is FALSE! The thing is that although I_a contains zero and is extra closed under multiply (both of which are quite easy to see) it is not closed under addition.
A better question would be "Is I_a an ideal of the ring R"! So let me answer that instead: NO! For example, consider the ring $R = \mathbb{Z}[x,y]/(x^2,y^2)$. This is the ring $\mathbb{Z}[x,y]$ of polynomials in two variables factored out by the ideal generated by x^2 and by y^2. Elements in this quotient ring can be represented as $a+bx+cy+dxy$ for unique $a,b,c,d \in \mathbb{Z}$. The multiplication is like for polynomials but whenever you get x^2 or y^2 you can replace it by zero.
Now consider $a = 1$. The elements x and y both belong to I_1 because $x^2.1 = x^2 = 0$ and similarly for y. But $x+y$ does not belong to I_1 because $(x+y)^2.1 = x^2+2xy+y^2 = 2xy \neq 0$. Hence I_1 is not closed under addition.