SOLUTION FOR SAMPLE FINALS

1.

a) List all proper nontrivial subgroups in the group $\mathbb{Z}_3 \times \mathbb{Z}_3$;

b) List all proper nontrivial ideals in the ring $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Solution.

a) A proper non-trivial subgroup of $\mathbb{Z}_3 \times \mathbb{Z}_3$ has order 3 and therefore cyclic. Thus it has one generator. Hence there are the following subgroups

$$< (1,0) >=< (2,0) > ; \; < (0,1) >=< (0,2) > ; \; < (1,2) >=< (2,1) > ; \; < (1,1) >=< (2,2) > .$$

b) Every ideal is a subgroup with respect to addition. One can see immediately that the subgroups

$$I_1 =< (1,0) >=< (2,0) > \text{ and } I_2 =< (0,1) >=< (0,2) >;$$

are ideals, and two other subgroups are not since (1,1) and (1,2) are units.

2. Let U_{10} be the group of units in the ring $\mathbb{Z}_{10}$. Show that U_{10} is isomorphic to $\mathbb{Z}_4$. List all generators of U_{10}.

Solution. $U_{10} = \{1,3,7,9\} =< 3 >=< 7 >$.

3. List all group homomorphisms

a) of $\mathbb{Z}_6$ into $\mathbb{Z}_3$;

b) of S_3 into $\mathbb{Z}_3$.

Explain your answer.

Solution.

a) A homomorphism $f : \mathbb{Z}_6 \to \mathbb{Z}_3$ is defined by its value $f(1)$ on the generator. There are three possibilities

$$f(1) = 0, \text{ then } f(x) = 0;$$

$$f(1) = 1, \text{ then } f(x) = [x] \mod 3,$$

$$f(1) = 2, \text{ then } f(x) = [2x] \mod 3.$$

b) For any transposition $\tau \in S_3$, $2f(\tau) = f(\tau^2) = f(e) = 0$. Since $\mathbb{Z}_3$ does not have elements of order 2, $f(\tau) = 0$. Every permutation is a product of transpositions. Therefore $f(\sigma) = 0$ for any $\sigma \in S_3$.

4. Find all normal subgroups of S_4.

Solution. The only proper non-trivial normal subgroups of S_4 are the Klein subgroup

$$K_4 = \{e, (12)(34), (13)(24), (14)(23)\}$$

and A_4. Let us prove it. Suppose that N is a normal proper non-trivial subgroup of S_4. First note that N does not contain a transposition, because if one transposition τ lies in N, then N contains all transpositions, hence $N = S_4$. If N contains a 3-cycle, then N contains all 3-cycles (as they are all conjugate). Therefore $N = A_4$ (we have proven in class that 3-cycles generate A_4). If N contains a 4-cycle $(abcd)$, then it also contains its conjugate $(bacd)$, and the product

$$(bacd)(abcd) = (bdc).$$

If N contains a 3-cycle, we already have shown that it contains A_4. But N also contains an odd permutation. Hence $N = S_4$. Finally, if N does not contain a transposition, 3-cycle or 4-cycle, it must contain a disjoint product of two transpositions $(ab)(cd)$. Then $N = K_4$.

5. Factor the polynomial $x^2 + 3x - 1$ into a product of irreducibles in the ring
a) $\mathbb{Q}[x]$;
b) $\mathbb{Z}_{13}[x]$.
Solution.
a) Irreducible, there is no roots. To check use the rational root test.
b) $x^2 + 3x - 1 = (x-5)^2$.

6. Let $\phi_6 \colon \mathbb{Z}_{11}[x] \to \mathbb{Z}_{11}$ be the evaluation homomorphism, given by $\phi_6(p(x)) = p(6)$.
a) Find $\phi_6(x^{123} - x^{10} + 1)$;
b) Is $\mathrm{Ker}(\phi_6)$ a principal ideal? Explain your answer.
Solution.
a) Use Fermat's theorem to obtain

$$6^{10} \equiv 1 \mod 11,\ 6^{123} \equiv 6^3 \left(6^{10}\right)^{12} \equiv 6^3 \equiv 7 \mod 11,$$

and therefore $\phi_6(x^{123} - x^{10} + 1) = 6^{123} - 6^{10} + 1 = 7$.
b) Yes. In fact any ideal in a polynomial ring $F[x]$, where F is a field, is principal.

7. Determine which of the following rings are integral domains:
a) $\mathbb{Z}_{15}$;
b) $\mathbb{Z} \times \mathbb{Z}_5$;
c) $\mathbb{Z}_{11}[x]$.
Solution.
a) No, 3 is a zero divisor.
b) No, (1,0) is a zero divisor.
c) $\mathbb{Z}_{11}[x]$ is an integral domain. In fact every polynomial ring over a field is an integral domain..

8. Find the degree of $\mathbb{Q}\left(\sqrt{3}, \sqrt[5]{7}\right)$ over $\mathbb{Q}$ and write down a basis of $\mathbb{Q}\left(\sqrt{3}, \sqrt[5]{7}\right)$ over $\mathbb{Q}$.
Solution.

$$\left[\mathbb{Q}\left(\sqrt{3}, \sqrt[5]{7}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{3}, \sqrt[5]{7}\right) : \mathbb{Q}\left(\sqrt{3}\right)\right]\left[\mathbb{Q}\left(\sqrt{3}\right) : \mathbb{Q}\right] = 5 \times 2 = 10.$$

A basis: $1,\ \sqrt[5]{7},\ \left(\sqrt[5]{7}\right)^2,\ \left(\sqrt[5]{7}\right)^3,\ \left(\sqrt[5]{7}\right)^4,\ \sqrt{3},\ \sqrt{3}\sqrt[5]{7},\ \sqrt{3}\left(\sqrt[5]{7}\right)^2,\ \sqrt{3}\left(\sqrt[5]{7}\right)^3,\ \sqrt{3}\left(\sqrt[5]{7}\right)^4.$

9. Find the minimal polynomial of $\sqrt{5}+\sqrt{6}$ over $\mathbb{Q}$ and prove that your answer is correct.

Solution. Let $\alpha=\sqrt{5}+\sqrt{6}$, then $\alpha^2=11+2\sqrt{30}$, and

$$\left(\alpha^2-11\right)^2=\alpha^4-22\alpha^2+121=120.$$

The minimal polynomial of α is $p(x)=x^4-22x^2+1$. To prove it, note that $p(x)$ does not have a rational root, and $p(x)$ can not be factored into a product of two quadratic polynomials $(x^2+ax\pm 1)(x^2-ax\pm 1)$, since $-a^2\pm 2=-22$ does not have solution for rational a. Hence $p(x)$ is irreducible.

10. Find an abelian subgroup of maximal order in S_5.

Solution. An element of maximal order in S_5 is $(12)(345)$, it has order 6. Hence the cyclic subgroup generated by this element has order 6. We prove that it is an abelian subgroup of maximal order. Let A be an abelian subgroup of S_5. If 5 divides the order of A and $|A|>5$, then 2 or 3 divides the order of A. Then A must have an element of order 10 or 15, which is impossible since S_5 does not have such elements. Note that 8 does not divide $|A|$, because otherwise A must contain a Sylow subgroup of order 8 which is D_4 (not abelian). Thus, $|A|$ can be 6 or 12. On the other hand, A must have an element g of order 3, i.e. a 3 cycle. Since A is abelian, it is contained in the centralizer $C(g)$ which has 6 elements only.

1. Evaluate $2^{2007} \pmod{19}$.

Solution.

$$2^9=64\times 8\equiv 7\times 8\equiv -1 \pmod{19},\ 2^{2007}=\left(2^9\right)^{223}\equiv -1 \pmod{19}.$$

2. Determine if the polynomial x^5+3x+3 is irreducible

(a) Over $\mathbb{Q}$.

(b) Over $\mathbb{Z}_7$.

Solution.

a) Yes, by Eisenstein criterion $p=3$.

b) No, $x=1$ is a root in $\mathbb{Z}_7$.

3. Let $R=\mathbb{Z}[x]$.

(a) Show that R is an integral domain.

(b) Find all units of R.

Solution.

a) Note that $\mathbb{Z}[x]\subset\mathbb{Q}[x]$, contains 1. Since $\mathbb{Q}[x]$ is an integral domain, $\mathbb{Z}[x]$ is an integral domain.

b) All units are ± 1. Indeed, if $p(x)$ has inverse $q(x)$, then $p(x)q(x)=1$, which imply that the degree of $p(x)$ and $q(x)$ is zero, *i. e.* $p(x)=c\in\mathbb{Z}$, $q(x)=c^{-1}\in\mathbb{Z}$. The latter implies $c=\pm 1$.

4. Let p be an odd prime number. Show that the equation

$$x^2=-1$$

has a solution in $\mathbb{Z}_p$ if and only if $p \equiv 1 \pmod 4$. (Hint: use the fact that the group of units is cyclic.)

Solution. If $x = b$ is a solution, then b is an element of order 4 in $U_p \cong \mathbb{Z}_{p-1}$. $\mathbb{Z}_{p-1}$ has an element of order 4 if and only if $4|p-1$.

5. Show that the groups D_6 and A_4 are not isomorphic.

Solution. The groups are not isomorphic because D_6 has an element of order 6, for instance the rotation on $60°$, but A_4 has only elements of order 2 (products of disjoint transpositions) and order 3 (a 3-cycle).

6. Show that the quotient ring $\mathbb{Z}_{25}/(5)$ is isomorphic to $\mathbb{Z}_5$.

Solution. The homomorphism $f(x) = [x]_{\text{mod } 5}$, is surjective as clear from the formula and $\operatorname{Ker} f = (5)$. Therefore by the first isomorphism theorem $\mathbb{Z}_{25}/(5)$ is isomorphic to $\mathbb{Z}_5$.

7. Show that the rings $\mathbb{Z}_{25}$ and $\mathbb{Z}_5[x]/(x^2)$ have the same number of elements but not isomorphic.

Solution. Elements of $\mathbb{Z}_5[x]/(x^2)$ are of the form $[ax+b]$ where $a, b \in \mathbb{Z}_5$. Hence $\mathbb{Z}_5[x]/(x^2)$ has 25 elements. But $5a = 0$ for any $a \in \mathbb{Z}_5[x]/(x^2)$, and this is not so in $\mathbb{Z}_{25}$.

8. How many Sylow 5-subgroups does the group A_5 have? Write down one Sylow subgroup and its normalizer.

Solution. The number of Sylow 5-subgroups is 6. As an example one can take a subgroup generated by (12345). The normalizer is generated by (12345) and (15)(24), it has 10 elements and one can check that it is isomorphic to D_5.

9. Show that every group of order 51 is cyclic.

Solution. Denote a group by G. There is only one Sylow 3-subgroup K and only one Sylow 17-subgroup H. So K and H are normal, $K \cap H = \{e\}$, and by counting elements $G = KH$. Then G is a direct product of $H \cong \mathbb{Z}_{17}$ and $K \cong \mathbb{Z}_3$, hence isomorphic to $\mathbb{Z}_{51}$.

10. Show that $\mathbb{Q}[x]/(x^2+x+1)$ and $\mathbb{Q}[x]/(x^2+3)$ are isomorphic. (Hint: show that $\mathbb{Q}[x]/(x^2+3)$ contains a root of x^2+x+1.)

Solution. Define a homomorphism $f\colon \mathbb{Q}[x] \to \mathbb{Q}\left(\sqrt{-3}\right)$ by

$$f(p(x)) = p\left(\frac{-1+\sqrt{-3}}{2}\right).$$

Clearly, f is surjective and the kernel of f is (x^2+x+1) since x^2+x+1 is the minimal polynomial of $\frac{-1+\sqrt{-3}}{2}$. Now the isomorphism follows from the first isomorphism theorem.