Solutions of homework problems.
Math 113
Vera Serganova

12(4.5) If $f(x) = g(x)h(x)$ then $f(x+c) = g(x+c)h(x+c)$. Moreover, $\deg p(x) = \deg p(x+c)$ for any polynomial $p(x)$. Hence irreducibility of $f(x)$ is equivalent to irreducibility of $f(x+c)$.

13(4.5) The polynomial

$$f(x+1) = x^4 + 4x^3 + 6x^2 + 8x + 6$$

is irreducible by Eisenstein criterion with $p = 2$.

17(4.5) The number of polynomials of degree less or equal than k is n^k, the number of polynomial of degree less or equal than $k-1$ is n^{k-1}. Hence the number of polynomials of degree k equals $n^k - n^{k-1}$.

11 (5.1) Since $p(x)$ is not irreducible, then $p(x) = f(x)g(x)$ for some polynomial $f(x)$, $g(x)$ of degree less than the degree of $p(x)$. Then $f(x)g(x) \equiv 0_F \mod p(x)$ but both $f(x)$ and $g(x)$ are not congruent to 0_F modulo $p(x)$.

13 (5.1) Both graphs meet the y-axis at the same point, because $f(0) = g(0)$.

14(5.2) Answers:
(a)$[2x-3]^{-1} = [-2x-3]$
$(b)[x^2+x+1]^{-1} = [x]^{-1} = [-x]$
$(c)[x^2+x+1]^{-1} = [x^2]$

15(5.2) Let $r = [x]$, $s = [x+1]$. The polynomial is $x(x-1)(x-r)(x-s) = x^4 + x$.

1(5.3)
(a) Yes, the polynomial $x^3 + 2x^2 + x + 1$ is irreducible in $\mathbb{Z}_3[x]$, because it does not have a root.
(b) No, $2x^3 - 4x^2 + 2x + 1$ is reducible in $\mathbb{Z}_5[x]$, because 2 is a root.
(c) No, $x^4 + x^2 + 1$ is reducible in $\mathbb{Z}_2[x]$, because $(x^2+x+1)^2 = x^4 + x^2 + 1$.

7(5.3) Use induction on $n = \deg f(x)$. The case $n = 1$ is trivial. By Corollary 5.12 there exists an extension K of F which contains a root c_1 of $f(x)$. In $K[x]$ we have $f(x) = (x - c_1)h(x)$. By induction assumption there is an extension E of K such that $h(x) = c_0(x-c_2)\dots(x-c_n)$ for some $c_0, c_2, \dots c_n \in E$. Hence

$$f(x) = c_0(x-c_1)(x-c_2)\dots(x-c_n)$$

as required.

8 (5.3) Let $E = F[x]/(p(x))$. Then $(x - [x])$ divides $p(x)$ in $E[x]$. Therefore

$$p(x) = b(x - [x])(x - c)$$

for some $b, c \in E$. In particular c is the second root of $p(x)$.

10 (6.1) Let $(a_1, a_2), (b_1, b_2) \in I \times J$, then $a_1, b_1 \in I$ and $a_2, b_2 \in J$. Therefore

$$a_1 - b_1 \in I \text{ and } a_2 - b_2 \in J. \text{ Hence } (a_1, a_2) - (b_1, b_2) = (a_1 - b_1, a_2 - b_2) \in I \times J.$$

If $(r, s) \in R \times S$, then $ra_1 \in I$ and $sa_2 \in J$, and therefore $(r, s)(a_1, a_2) = (ra_1, sa_2) \in I \times J$. In the same way $(a_1, a_2)(r, s) \in I \times J$.

34 (6.1) If $x, y \in IJ$ then

$$x = a_1 b_1 + \cdots + a_n b_n,\ y = c_1 d_1 + \cdots + c_m d_m$$

for some $a_1, \ldots, a_n, c_1, \ldots, c_m \in I$, $b_1, \ldots, b_n, d_1, \ldots, d_m \in J$. Then

$$x - y = a_1 b_1 + \cdots + a_n b_n + (-c_1) d_1 + \cdots + (-c_m) d_m \in IJ,$$

because $-c_i \in I$. If $r \in R$, then

$$rx = (ra_1) b_1 + \cdots + (ra_n) b_n \in IJ,$$

$$xr = a_1 (b_1 r) + \cdots + a_n (b_n r) \in IJ$$

since $ra_i \in I$, $b_i r \in J$.

13 (6.2) Let $p : R[x] \to R$ defined by

$$p(a_0 + a_1 x + \cdots + a_n x^n) = a_0.$$

Then p is a surjective homomorphism, and the kernel of p consists of all polynomials with zero constant coefficients. In other words the kernel of p is (x). By the first isomorphism theorem R is isomorphic to $R[x]/(x)$.

18 (6.2) Let R/I be an integral domain. Then $(a + I)(b + I) = ab + I = 0 + I$ implies that $a + I = 0$ or $b + I = 0$. Hence $ab \in I$ implies $a \in I$ or $b \in I$.

Conversely, let $ab \in I$ implies $a \in I$ or $b \in I$. Then $(a + I)(b + I) = ab + I = 0 + I$ implies $ab \in I$. Therefore $a \in I$ or $b \in I$, and hence $a + I = 0 + I$ or $b + I = 0 + I$.

is not prime.

20 (6.2) Let $f : R \to S$ be a surjective homomorphism, so S is a homomorphic image. S is commutative, because $f(x) f(y) = f(xy) = f(yx) = f(y) f(x)$. Furthermore, $f(1_R)$ is the identity in S. Finally, if J is an ideal in S, then $f^{-1}(J) = \{r \in R \mid f(r) = j\}$ is an ideal in R, and $f^{-1}(J) = (c)$ for some $c \in R$. Then every element $b \in J$ can be written as $f(r)$ for some $r \in f^{-1}(J)$. But $r = xc$, so $b = f(r) = f(x) f(c)$. Thus $J = (f(c))$.

32 (6.2) Obviously $f(a) = a + J$ is a well-defined homomorphism $f : I \to (I + J)/J$. It is surjective since for any $a \in I, b \in J$, $a + b + J = f(a)$. The kernel of f consists of all $c \in I$ such that $c + J = 0 + J$, i.e. $c \in J$. Thus, $\operatorname{Ker} f = I \cap J$, and by the first isomorphism theorem $I/(I \cap J) \cong (I + J)/J$.

19 (7.1) Just check all properties of a group

$$(a \# b) \# c = c * (b * a) = (c * b) * a = a \# (b \# c),$$

$$a \# e = e * a = a = a * e = e \# a,\ a \# a^{-1} = a^{-1} * a = e = a * a^{-1} = a^{-1} \# a.$$

14 (7.2) If $|a| = n$, then the order a^k is equal to $\frac{n}{(n,k)}$. Indeed, $\left(a^k\right)^m = e$ if and only if n divides km. Let $r = \frac{k}{(n,k)}$, then $\frac{n}{(n,k)}$ divides rm. Since $\left(r, \frac{n}{(n,k)}\right) = 1$, we obtain $\frac{n}{(n,k)} | m$. The minimal possible $m = \frac{n}{(n,k)}$.

30 (7.2) Assume that G does not contain an element of order 2. Then if $g \in G$ and $g \neq e$, then $g^{-1} \neq g$. Thus, G is a disjoint union of $\{e\}$ and two-element sets $\{g, g^{-1}\}$. That implies $|G|$ is odd. Therefore if $|G|$ is even, G must have an element of order 2.

33 (7.2) Note that
$$ab^2 = b^4ab = b^8a = b^2a.$$
Therefore
$$ab = b^4a = b^2b^2a = ab^4,$$
and therefore
$$b^3 = e,\ ab = ba.$$

36 (7.2) Write
$$(ab)^k = a^kb^k,\ (ab)^{k+1} = a^{k+1}b^{k+1},\ (ab)^{k+2} = a^{k+2}b^{k+2}.$$
Then
$$ab = (ab)^{-k}(ab)^{k+1} = b^{-k}a^{-k}a^{k+1}b^{k+1} = b^{-k}ab^{k+1},$$
that implies $a = b^{-k}ab^k$. Similarly, $a = b^{-k-1}ab^{k+1}$. Therefore we get
$$a = b^{-k}ab^k = b^{-1}b^{-k}ab^kb = b^{-1}ab.$$
Therefore $ab = ba$.

31 (7.3) If $a, b \in x^{-1}Hx$, then $a = x^{-1}cx$, $b = x^{-1}dx$ for some $c, d \in H$. Therefore
$$ab = x^{-1}cxx^{-1}dx = x^{-1}cdx \in x^{-1}Hx,$$
$$a^{-1}\left(x^{-1}cx\right)^{-1} = x^{-1}c^{-1}x \in x^{-1}Hx,$$
since $cd, c^{-1} \in H$.

32 (7.3) The map $\varphi_x \colon H \to H$ given by $\varphi_x(h) = x^{-1}hx$ is a bijection, since $(\varphi_x)^{-1} = \varphi_{x^{-1}}$. Therefore φ_x is surjective and hence $x^{-1}Hx = \varphi_x(H) = H$.

21 (7.4) Let $(f(a))^k = e_H$. Since $(f(a))^k = f\left(a^k\right)$ and f is injective $a^k = e_G$. Thus, $|a|$ divides $|f(a)|$. On the other hand, if $a^m = e_G$, then $(f(a))^m = f(a^m) = e_H$. Therefore $|f(a)|$ divides $|a|$. Thus, $|f(a)| = |a|$.

24 (7.4) If f and g are two automorphisms of G. Then
$$f \circ g(ab) = f(g(ab)) = f(g(a)g(b)) = f(g(a))f(g(b) = f \circ g(a) f \circ g(b).$$
Therefore $f \circ g$ is a homomorphism. Since $f \circ g$ is bijective, $f \circ g \in \operatorname{Aut} G$. It is left to check that f^{-1} is a homomorphism.

Indeed, since f is bijective, for any $a, b \in G$ there exist unique $c, d \in G$ such that $a = f(c), b = f(d)$. Then
$$f^{-1}(ab) = f^{-1}(f(c)f(d)) = f^{-1}(f(cd)) = cd = f^{-1}(a)f^{-1}(b).$$